Διαπανεπιστημιακό Πρόγραμμα
Μεταπτυχιακών Σπουδών
στη Λογική και Θεωρία Αλγορίθμων
και Υπολογισμού
«Μ.Π.Λ.Α.»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μη-Μεταθετική Κρυπτογραφία

- Κωνσταντίνος Ι. Καραθάνος -

Επιβλέπων Καθηγητής:
Ευάγγελος Ράπτης
Αθήνα, 2016

Αφιερωμένο
στην Οικογένεια,
στους Φίλους,
στους Συνεργάτες
& Συναδέρφους

The noblest pleasure is the joy of understanding.

¤ Leonardo da Vinci

Για να γίνει κανείς ικανός σ' οποιοδήποτε επάγγελμα
τρία πράγματα χρειάζονται:
φύση, μελέτη και πρακτική εξάσκηση.

¤ Αριστοτέλης

ΠΡΟΛΟΓΟΣ

Η εκπόνηση της συγκεκριμένης διπλωματικής εργασίας έλαβε χώρο στα πλαίσια της ολοκλήρωσης της φοίτησής μου στο Μεταπτυχιακό Πρόγραμμα στη Λογική και Θεωρία Αλγορίθμων και Υπολογισμού, ευρέως γνωστό ως Μ.Π.Λ.Α.

Αρχικώς θα ήθελα να ευχαριστήσω όλο το Διδακτικό προσωπικό που είχα την τύχη να γνωρίσω κατά τη διάρκεια της φοίτησης μου στο προαναφερθέν πρόγραμμα και να εκφράσω την ευγνωμοσύνη μου για την διαπροσωπική επικοινωνία που αναπτύχθηκε με αρκετές αναγνωρισμένες και αξιοσέβαστες προσωπικότητες των Θεωρητικών Μαθηματικών και της Αλγοριθμικής Πληροφορικής.

Ιδιαιτέρως θα ήθελα να εκφράσω την ευγνωμοσύνη μου για τον επιβλέποντα καθηγητή, κ. Ευάγγελο Ράπτη, για την εμπιστοσύνη που έδειξε στο πρόσωπό μου και στην ολοκλήρωση της παρούσας εργασίας. Οι αναμνήσεις που έχω από τη διδασκαλία του, με ταξιδεύουν πίσω στα Προπτυχιακά μου χρόνια, στο Μαθηματικό Τμήμα. Έκτοτε έτρεφα ιδιαίτερη εκτίμηση και αισθάνομαι ευτυχής που είχα την ευκαιρία να συνεργαστούμε στη Διπλωματική εργασία.

Επιπροσθέτως, θα ήθελα να ευχαριστήσω και τους κ. Βάρσο και κ. Λάππα, που αποδέχθηκαν να συμπεριληφθούν στην τριμελή επιτροπή που συγκροτήθηκε για την εποπτεία και αξιολόγηση της όλης προσπάθειας. Όντας προπτυχιακός φοιτητής του Τμήματος Μαθηματικών, δε θα μπορούσα να μην έχω πληθώρα αναμνήσεων μαζί τους, από τις διάφορες Ακαδημαϊκές Δραστηριότητες, είτε επρόκειτο για εκπαιδευτικές, είτε για κοινωνικές. Και είναι ευνόητη η εκτίμηση που τρέφω στο πρόσωπό τους.

Θα μπορούσα να αναφέρω πολλούς ακόμη αξιόλογους ανθρώπους που γνώρισα κατά το όμορφο ταξίδι που έζησα ως μέλος της κοινότητας του Μ.Π.Λ.Α., είτε ήταν συνάδερφοι, είτε ήταν δάσκαλοι, όμως θα προτιμήσω να μην πλατειάσω.

Ολοκληρώνοντας, θα ήθελα να ευχαριστήσω την οικογένειά μου, τους φίλους μου και τους συνεργάτες μου, για την αγαστή συμπαράσταση και κατανόηση που έδειξαν όλα αυτά τα χρόνια.

Κωνσταντίνος Καραθάνος,
Αθήνα, 28 Αυγούστου 2016

ΠΕΡΙΛΗΨΗ

Στην παρούσα διπλωματική εργασία έχουμε την ευκαιρία να ταξιδέψουμε στον όμορφο κόσμο της Άλγεβρας και της Θεωρίας Ομάδων, κάνοντας μια ευχάριστη στάση στα θαυμαστά μυστήρια που κρύβει η Κρυπτογραφία σε όλο της το χρονικό φάσμα, από την Αρχαιότητα έως και σήμερα.

Θα εμβαθύνουμε ιδιαιτέρως σε επί μέρους προβλήματα που συναντάμε στη Θεωρία Ομάδων, με κυρίαρχα αυτά της συζυγίας, της λέξης και του ισομορφισμού. Θα θυμηθούμε εδραιωμένα πρωτόκολλα κρυπτογραφίας και ψηφιακών υπογραφών και θα σκαλίσουμε αδύναμες πτυχές τους.

Αυτό θα μας οδηγήσει στην ανάγκη εύρεσης και μελέτης εναλλακτικών οδών για τη διασφάλιση της επικοινωνίας από κακόβουλες ενέργειες, μέσω εργαλείων που μας χαρίζει ο κόσμος των Ομάδων, όπως η ιδιάζουσα κατηγορία των Πλεξίδων. Εκεί, θα μας δοθεί η ευκαιρία να γνωρίσουμε καλύτερα μορφές όπως των Dehorney και Garside, αλλά και περιπτώσεις όπως οι Ομάδες Πινάκων, Thompson, Artin και ο Αλγόριθμος του Dehn.

Για να καταλήξουμε στη μορφή της Μη-Μεταθετικής Κρυπτογραφίας, σε μια σειρά πρωτοκόλλων που θα αναλύσουμε, με κυρίαρχο αυτό των Anshel-Anshel-Goldfeld και σε πολλά παρεμφερή προβλήματα και σχέσεις που αναπτύσσονται μεταξύ τους.

Τέλος, το ταξίδι μας ολοκληρώνεται με μια προσπέλαση μέσα από διάφορα προβλήματα απόφασης και την Κρυπτογραφία Δημοσίου Κλειδιού, όπου θα επικρατήσουν οι μορφές των Shpilrain, Zapata και Tietze.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ Ι

ΑΛΓΕΒΡΙΚΕΣ ΔΟΜΕΣ & ΚΡΥΠΤΟΓΡΑΦΙΑ

Ι.1
Αλγεβρικές Δομές, Ορισμοί και Βασικές Έννοιες

Ι.1.1. Ομάδες

α. Ομάδες, Υποομάδες & Ιδιότητες

Σύνολο

Ορισμός Ι.1
Ένα σύνολο S αποτελείται από στοιχεία κι αν α ένα από αυτά τα στοιχεία, τότε θα ορίσουμε και θα λέμε πως $\alpha \in S$. □

Ιδιότητες συνόλου

Υπάρχει ένα ακριβώς σύνολο που δεν περιέχει στοιχεία και θα το ονομάσουμε κενό σύνολο. Το σύνολο αυτό θα το συμβολίζουμε με $\emptyset$.

Ένα σύνολο μπορούμε να το περιγράψουμε με το να χαρακτηρίσουμε μια ιδιότητά των στοιχείων του, όπως «$το\ σύνολο\ των\ Νομών\ της\ χώρας$» ή με το να εκθέσουμε το σύνολο των στοιχείων του. Ο συνήθης τρόπος παρουσίασης των στοιχείων ενός συνόλου είναι να τα βάλουμε μέσα σε αγκύλες και να τα διαχωρίσουμε με κόμμα, δηλαδή έτσι $\{3, 7, 9\}$. Από την άλλη, εάν το σύνολο το περιγράφουμε με κάποια χαρακτηριστική ιδιότητα $P(x)$ των στοιχείων του x, θα χρησιμοποιήσουμε τη μορφή: $\{x|P(x)\}$ το οποίο και θα διαβάσουμε ως «το σύνολο όλων των στοιχείων x για τα οποία η ιδιότητα $P(x)$ για τα x είναι αληθής». Ένα παράδειγμα θα μπορούσε να είναι το εξής:

Παράδειγμα Ι.1

$$\{2, 4, 6, 8\} = \{x \mid x\ είναι\ ένας\ ζυγός\ αριθμός\ \leq 8\}$$
$$= \{2x \mid x = 1, 2, 3, 4\}$$

□

Ένα σύνολο S είναι καλώς ορισμένο όταν για κάποιο στοιχείο α, ισχύει ότι το α είναι στοιχείο του S και εκφράζεται ως $\alpha \in S$ ή ότι το α δεν ανήκει στο S και τότε θα πούμε $\alpha \notin S$. Δηλαδή δε μπορούμε να επικαλεστούμε το σύνολο «κάποιων θετικών αριθμών», γιατί σε αυτήν την περίπτωση δε θα γνωρίζουμε εάν το $2 \in S$ ή το $2 \notin S$. Δηλαδή αυτό το σύνολο δε θεωρείται καλώς ορισμένο.

Υποσύνολα και καρτεσιανά γινόμενα

Ορισμός Ι.2
Ένα σύνολο B αποτελεί υποσύνολο ενός συνόλου A, και θα το συμβολίζουμε ως $B \subseteq A$ ή $A \supseteq B$, εάν κάθε στοιχείο του B βρίσκεται στο A. Οι εκφράσεις $B \subset A$ ή $A \supset B$ θα χρησιμοποιούνται για $B \subseteq A$, αλλά $B \neq A$. □

Όπως είναι πρόδηλες από τον ορισμό του υποσυνόλου, θα ισχύει επίσης ότι για κάθε σύνολο A, το ίδιο το A και το $\emptyset$ θα είναι και τα δύο υποσύνολα του A.

Έστω δύο σύνολα A και B. Το σύνολο $A\ x\ B = \{(\alpha, \beta) \mid \alpha \in A\ και\ b \in B\}$ αποτελεί το καρτεσιανό γινόμενο των A και B.

Παράδειγμα Ι.2
Για παράδειγμα, αν έχουμε τα σύνολα $A = \{1,2,3\}$ και $B = \{3,4\}$, τότε το καρτεσιανό γινόμενό τους θα είναι:

$$A\ x\ B = \{(1,3), (1,4), (2,3), (2,4), (3,3), (3,4)\}$$

□

Σχέσεις συνόλων και Πληθικότητα

Ορισμός Ι.3
Μια σχέση μεταξύ των συνόλων A και B είναι ένα υποσύνολο $\mathfrak{G}$ του $A\ x\ B$. Θα διαβάζουμε $(\alpha, b) \in \mathfrak{G}$ ως «το α σχετίζεται με το b» και γράφουμε $\alpha\ \mathfrak{G}\ b$. □

Ορισμός Ι.4
Μια συνάρτηση ϕ που αντιστοιχεί το X στο Y είναι μια σχέση μεταξύ των X και Y με την ιδιότητα ότι κάθε $x \in X$ εμφανίζεται ως το πρώτο μέλος ακριβώς ενός ταξινομημένου ζεύγους (x, y) στην ϕ. Μια τέτοια συνάρτηση καλείται επίσης «αντιστοίχιση» του X στο Y. Θα γράφουμε $\phi : X \longrightarrow Y$ και θα εκφράζουμε το $(x, y) \in \phi$ ως $\phi(x) = y$. □

Ορισμός Ι.5
Το σύνολο των στοιχείων ενός συνόλου X ονομάζεται ως η «Πληθικότητα» του X και συμβολίζεται με $|X|$. □

Για παράδειγμα ισχύει $|\{2,5,7\}| = 3$. Γενικά θα μας είναι χρήσιμο να γνωρίζουμε πότε δύο σύνολα έχουν την ίδια Πληθικότητα. Για πεπερασμένα σύνολα, αυτό είναι γενικά εύκολο. Για άπειρα όμως σύνολα, το ζήτημα δυσκολεύει και πολλές φορές ίσως η εφαρμογή κάποιων τεχνασμάτων να μας δώσουν προσεγγιστικές απαντήσεις.

Αλλά σε γενικές γραμμές, δύο σύνολα έχουν την ίδια Πληθικότητα, εάν υπάρχει $1-1$ συνάρτηση αντιστοίχισης από το X στο Y, δηλαδή εάν υπάρχει $1-1$ αντιστοίχιση μεταξύ των X και Y.

Ορισμός Ομάδας

Ορισμός Ι.6
Μια ομάδα $\langle G,* \rangle$ είναι ένα σύνολο G, κλειστό ως προς μια δυαδική πράξη $*$, δηλαδή είναι ένα σύνολο G εφοδιασμένο με μια πράξη $G\ x\ G \longrightarrow G$, $(\alpha, b) \mapsto a \cdot b$ έτσι ώστε τα ακόλουθα αξιώματα να ικανοποιούνται:

(i) $\mathfrak{G}_1$: Για κάθε $\alpha, b, c \in G$, θα έχουμε ότι $(\alpha * b) * c = a * (b * c)$. Η ιδιότητα αυτή ονομάζεται προσεταιριστική.
(ii) $\mathfrak{G}_2$: Υπάρχει ένα στοιχείο e που ανήκει στο G, τέτοιο ώστε για όλα τα $x \in G$, ισχύει $e * x = x * e = x$. Το στοιχείο e ονομάζεται ταυτοτικό στοιχείο.
(iii) $\mathfrak{G}_3$: Για κάθε $\alpha \in G$, υπάρχει ένα στοιχείο α' στο G τέτοιο ώστε $\alpha * \alpha' = \alpha' * \alpha = e$. Το α' λέγεται το αντίστροφο του α.

□

Έστω μια ομάδα G και η πράξη $*$, τότε ισχύει πως $\alpha * b = a * c \Rightarrow b = c$, και $b * a = c * a \Rightarrow b = c$ για κάθε $\alpha, b, c \in G$.

Έστω μια ομάδα G, τότε με $|G|$ θα συμβολίζουμε τον αριθμό των στοιχείων της G.

Αβελιανές Ομάδες

Ορισμός Ι.7
Μια ομάδα G είναι αβελιανή, εάν ισχύει η Μεταθετική ιδιότητα, δηλαδή εάν για δύο στοιχεία $\alpha, b \in G$ ισχύει ότι $\alpha \cdot b = b \cdot a$. □

Υποομάδες

Ορισμός Ι.8
Εάν ένα υποσύνολο H μιας ομάδας G είναι κλειστό ως προς την δυαδική πράξη του G και εάν το υποσύνολο H με την παραγόμενη πράξη στο G είναι από μόνο του ομάδα, τότε το H καλείται υποομάδα του G. Δηλαδή με άλλα λόγια, ένα υποσύνολο H μιας ομάδας G θα λέγεται υποομάδα της G, αν το H είναι ομάδα ως προς την πράξη που ορίζεται στη G. □

Τότε και θα συμβολίζουμε $H \leq G$ ή $G \geq H$, που σημαίνει ότι το H είναι υποομάδα του G και $H < G$ ή $G > H$ όταν θα ισχύει η σχέση $H \leq G$, αλλά $H \neq G$.

Παράδειγμα Ι.3
Για τον λόγο αυτόν, ισχύει ότι $\langle \mathbb{Z}, + \rangle < \langle \mathbb{R}, + \rangle$ αλλά το $\langle \mathbb{Q}^+, \cdot \rangle$ δεν είναι υποομάδα του $\langle \mathbb{R}, + \rangle$, παρ' όλο που σε επίπεδο συνόλων ισχύει $\mathbb{Q}^+ \subset \mathbb{R}$. □

Εδώ θα πρέπει να επισημάνουμε ότι κάθε ομάδα G έχει ως υποομάδα τον εαυτό της, δηλαδή τη G. και το ταυτοτικό στοιχείο που θα το ονομάσουμε και συμβολίσουμε με $\{e\}$.

Όμως ας δούμε και πιο συγκεκριμένα τι ισχύει:

i. Το ουδέτερο στοιχείο 1 μιας ομάδας G είναι το ουδέτερο στοιχείο κάθε υποομάδας.
   Το κενό υποσύνολο $\emptyset$ δεν είναι υποομάδα.
   Το μόνο μονοσύνολο που είναι υποομάδα της G είναι το μονοσύνολο $\{1\}$.
   Επειδή η τομή όλων των υποομάδων της G είναι αυτό το μονοσύνολο, δηλαδή το $\{1\}$, αυτήν την υποομάδα θα τη λέμε και «τετριμμένη υποομάδα» της G.

ii. Κάθε ομάδα G έχει τουλάχιστον δύο υποομάδες, τον ίδιο τον εαυτό της G και την τετριμμένη που αναφέραμε πιο πάνω στο (i). Αυτές θα ονομάζονται και απλές ομάδες. Κάθε άλλη υποομάδα H της G θα την ονομάσουμε ως γνήσια υποομάδα και τότε θα ισχύει $1 < H < G$. Όμως υπάρχουν και ομάδες που ενδεχομένως να μην έχουν γνήσιες υποομάδες.

iii. Οι σχέσεις $\leq$ και $\geq$ μεταξύ των υποομάδων μιας ομάδας είναι μεταβατικές. Δηλαδή αν $H_1 \leq H_2$ και $H_2 \leq H_3$, τότε θα ισχύει $H_1 \leq H_3$.

iv. Όταν θέλουμε να δείξουμε αν ένα υποσύνολο H μιας ομάδας G είναι υποομάδα δε χρειάζεται να εξετάζουμε αν ισχύει η προσεταιριστική ιδιότητα για την H. Αυτή ισχύει για όλη τη G.

Έστω H ένα μη κενό υποσύνολο μιας ομάδας G, τότε όλα τα κάτωθι είναι ισοδύναμα:

i. Το υποσύνολο H είναι υποομάδα.

ii. Εάν για κάθε δύο στοιχεία h_1 και h_2 της G ισχύει ότι ανήκουν στο H, τότε το στοιχείο $h_1{h_2}^{-1}$ ανήκει στην υποομάδα H.

iii. Αν για δύο στοιχεία h_1 και h_2 της G ισχύει ότι ανήκουν στο H, τότε ισχύει πως και το $h_1h_2 \in H$. Δηλαδή το H είναι κλειστό ως προς την πράξη της G.

Αν όμως το στοιχείο h της G ανήκει στο υποσύνολο H, τότε και το αντίστροφο αυτού h^{-1} πρέπει να είναι στοιχείο του H.

Παραγόμενη Υποομάδα και Γεννήτορες

Έστω ότι έχουμε μια ομάδα G κι ένα υποσύνολο X. Τότε η τομή όλων των υποομάδων που περιέχουν το X είναι η μικρότερη υποομάδα μ' αυτήν την ιδιότητα.

Έστω τώρα ένα τέτοιο X ως μη κενό υποσύνολο μιας ομάδας G. Επιπλέον θα πάρουμε και το υποσύνολο X^{-1} που ορίζεται ως $X^{-1} = \{x^{-1} | x \in X\}$.

Στη συνέχεια θα πάρουμε όλα τα δυνατά πεπερασμένα γινόμενα της μορφής:

$$x_1x_2 \dots x_n, \qquad n = 0,1,2,3, \dots$$

όπου τα x_i είναι οποιαδήποτε (όχι κατ' ανάγκη διακεκριμένα) στοιχεία της ένωσης $X \cup X^{-1}$ και τα οποία θα απαρτίσουν το σύνολο H. Τότε λέμε πως το σύνολο H είναι υποομάδα της G. Επιπροσθέτως, αυτή η υποομάδα H είναι η τομή όλων των υποομάδων της G, έστω των S, που περιέχουν το X, δηλαδή είναι η μικρότερη υποομάδα που περιέχει το X:

$$H = \bigcap \{ S : S \leq G, \qquad X \subseteq S \}$$

Είναι προφανές ότι η υποομάδα H των στοιχείων της G, μπορεί να εκφραστεί ως πεπερασμένο γινόμενο στοιχείων και αντιστρόφων στοιχείων από το συνόλο X, δηλαδή:

$$H = \left\{ x_{i_1}^{e_1} \dots x_{i_n}^{e_n} : x_{i_j} \in X, e_j \in \{-1,1\}, \qquad j = 1, \dots, n, \qquad n \in \mathbb{N} \right\}$$

Ορισμός Ι.9

Έστω ότι ισχύει η ισότητα $H = G$, δηλαδή η υποομάδα H είναι ίση με την ομάδα G. Τότε επειδή η υποομάδα H παράγεται από το σύνολο X, θα παράγεται και η ομάδα G από το σύνολο X, και τα στοιχεία του X λέγονται γεννήτορες της G, ενώ αυτή η υποομάδα συμβολίζεται με $\langle X \rangle$. □

Ορισμός Ι.10

Μια ομάδα G θα λέγεται πεπερασμένα παραγόμενη αν για ένα πεπερασμένο υποσύνολο X της ομάδας G, ισχύει η σχέση $G = \langle S \rangle$. □

β. Κυκλικές Ομάδες, Ελεύθερες Ομάδες και Λέξεις

Κυκλικές Ομάδες

Ορισμός Ι.11

Έστω το μονοσύνολο $X = \{x\}$. Τότε η υποομάδα $\langle X \rangle = \langle x \rangle$ που παράγεται από αυτό το μονοσύνολο είναι η κυκλική ομάδα με γεννήτορα το στοιχείο $x \in X$.

Πιο συγκεκριμένα, μια ομάδα G καλείται κυκλική (cyclic), αν υπάρχει ένα στοιχείο της x ώστε κάθε άλλο στοιχείο της να είναι δύναμη ή άθροισμα αυτού, $y = x^k$ ή $y = xk$ για κάποιον ακέραιο k. Τότε κι ο x θα καλείται γεννήτορας όπως είδαμε και πιο πάνω και γράφουμε $G = < x > = \{x^k \mid με\ k\ ακέραιο\}$. □

Μια κυκλική ομάδα θα καλείται πεπερασμένης τάξης αν έχει πεπερασμένο πλήθος στοιχείων και καλείται άπειρη σε αντίθετη περίπτωση.

Μερικές από τις ιδιότητες που ισχύουν στις κυκλικές ομάδες είναι:

Έστω μια κυκλική ομάδα G και x κάποιο στοιχείο της. Τότε με k, s ακεραίους, ισχύει:

i. $x^k x^s = x^{k+s}$ (Από την προσεταιριστική ιδιότητα και της σχέση $xx^{-1} = 1$)

ii. $(x^{-1})^k = x^{-k} = (x^k)^{-1}$
(Βασιζόμαστε στο προηγούμενο όπου $x^k x^{-k} = 1$ κτλ.)

iii. $(x^k)^s = x^{ks}(x^s)^k$ (Για $s > 0$, χρησιμοποιούμε s φορές της σχέση (i). Αν $s < 0$, τότε χρησιμοποιούμε πρώτα τη σχέση (ii) και μετά τη σχέση (i).

Θέλουμε να δείξουμε ότι οι κυκλικές ομάδες είναι και αβελιανές. Έτσι έστω μια κυκλική ομάδα G για την οποία θέλουμε να δείξουμε το πιο πάνω και έστω ότι κάθε στοιχείο της γράφεται x^k για κάποιον ακέραιο k. Τότε αν πάρουμε δύο στοιχεία της, μπορούμε να δείξουμε ότι αυτά μετατίθενται και αποδεικνύουμε το ζητούμενο:

$$x^k x^s = x^{k+s} = x^{s+k} = x^s x^k$$

Το αντίστροφο όμως δεν ισχύει, δηλαδή μια αβελιανή ομάδα δεν είναι κατ' ανάγκη κυκλική. Ένα τέτοιο παράδειγμα είναι η αβελιανή ομάδα $(\mathbb{Q}, +)$ που δεν είναι κυκλική.

Ελεύθερες Ομάδες και Λέξεις

Όπως προαναφέραμε, σε μια ομάδα G παραγόμενη από ένα σύνολο X, κάθε στοιχείο της ομάδας θα εκφραστεί με μη μοναδικό τρόπο ως γινόμενο των στοιχείων και των αντίστροφων στοιχείων του X. Τέτοιο παράδειγμα είναι η Αβελιανή ομάδα στην οποία έχουμε $ab = ba$, αλλά και περιπτώσεις σχέσεων όπως $x^{-1}x = xx^{-1} = 1, x \in X$.

Σε μια ομάδα G, οι σχέσεις μεταξύ των στοιχείων του X αποτελούν ισότητες μεταξύ γινομένων στοιχείων και αντιστρόφων στοιχείων του X. Εδώ όμως υπεισέρχεται η έννοια της Αναγωγής. Δηλαδή, του τρόπου με τον οποίον τα προαναφερθέντα γινόμενα μπορούν να αναχθούν ύστερα από διαγραφή γινομένων που εμφανίζονται με τη μορφή $x^{-1}x$ ή xx^{-1}.

Για να το κάνουμε αυτό θα πρέπει να πάρουμε μια $1-1$ απεικόνιση από ένα σύνολο X σε ένα άλλο ισοπληθικό και ξένο ως προς το X, έστω το X^{-1}. Με τον ίδιο τρόπο ορίζεται και η αντίστροφη απεικόνιση, δηλαδή από το σύνολο X^{-1} στο σύνολο X. Όπως είναι αυτονόητο, στην πρώτη περίπτωση θα έχουμε $(x)^{-1} = x^{-1}$ ενώ στη δεύτερη θα έχουμε $(x^{-1})^{-1} = x$ όπου x^{-1} είναι το αντίστροφο στοιχείο του x.

Ορισμός Ι.12
Έστω τώρα ότι παίρνουμε ένα τυχαίο σύνολο X που θα το ονομάσουμε αλφάβητο. Θα ονομάσουμε λέξη w στο X μια πεπερασμένη ακολουθία

στοιχείων (που θα μπορούσε να είναι και κενή) την οποία συμβολίζουμε με $w = y_1 \dots y_n,\ y_i \in X$. □

Ο αριθμός n πιο πάνω ονομάζεται μήκος της λέξης w και θα συμβολίζεται με $|n|$. Μαρτυρά το πλήθος των στοιχείων της ακολουθίας.

Η κενή λέξη συμβολίζεται με ε, έχει μηδενικό (κενό) αριθμό στοιχείων και το μήκος της είναι $|\varepsilon| = 0$.

Έστω τώρα το σύνολο $X^{-1} = \{x^{-1} | x \in X\}$, με το x^{-1} να είναι η έκφραση που παίρνουμε από τα x και -1. Τώρα, εάν $x \in X$, τα σύμβολα x και x^{-1} ονομάζονται μεταβλητές στο X. Το σύνολο όλων των μεταβλητών στο X εκφράζεται ως $X^{\pm 1} = X \cup X^{-1}$.

Ορισμός Ι.13
Μια έκφραση της μορφής

$$w = x_{i_i}^{\varepsilon_1} \dots x_{i_n}^{\varepsilon_n}, \text{ όπου } x_{i_j} \in X,\ \varepsilon_j \in \{1, -1\}$$

ονομάζεται λέξη σε μια ομάδα στο X. Κατά συνέπεια μια λέξη σε μια ομάδα στο X είναι μια λέξη στο αλφάβητο $X^{\pm 1}$. □

Ανηγμένες Λέξεις

Ορισμός Ι.14
Μια λέξη $w = y_1 \dots y_n$ είναι ανηγμένη αν για κάθε $i = i, \dots, n-1$, ισχύει $y_i \neq y_{i+1}^{-1}$, που σημαίνει ότι η λέξη w δεν συμπεριλαμβάνει κάποια υποακολουθία της μορφής yy^{-1} για κάποια μεταβλητή $y \in X^{\pm 1}$. □

Εάν $X \subseteq G$, τότε κάθε λέξη $w = x_{i_1}^{\varepsilon_1} \dots x_{i_n}^{\varepsilon_n}$ στο X προσδιορίζει ένα μοναδικό στοιχείο στο G που είναι ίσο με το γινόμενο $x_{i_1}^{\varepsilon_1} \dots x_{i_n}^{\varepsilon_n}$ των στοιχείων $x_{i_j}^{\varepsilon_j} \in G$.

Από τα πιο πάνω, προκύπτει ότι οι κενές λέξεις αλλά και εκείνες που έχουν μόνον ένα στοιχείο, δεν έχουν διαδοχικά γράμματα στην παράστασή τους και κατά συνέπεια είναι ανηγμένες. Ιδιαίτερα η κενή λέξη ε προσδιορίζει το ταυτοτικό 1 του G.

Το μήκος μιας ανηγμένης λέξης w θα το ονομάσουμε ανηγμένο μήκος.

Στην περίπτωση των ανηγμένων λέξεων μας χρειάζεται η έννοια της αναγωγής που μελετήσαμε πιο πάνω. Κατά προφανή λόγο, η όλη διαδικασία έγκειται στη

διαγραφή τυχόν υπακολουθιών που έχουν τη μορφή (y_i, y_i^{-1}) έτσι ώστε να προκύψει η προαναφερθείσα ανηγμένη λέξη.

Ας δούμε λίγο αναλυτικότερα πως λειτουργεί η διαδικασία της αναγωγής μέχρι να φτάσουμε στην τελική ανηγμένη μορφή. Έτσι, θεωρούμε τη λέξη $w = (y_1, \dots, y_n)$ όπου $y_{i+1} = y_i^{-1}$. Έστω ότι παίρνουμε την αναγωγή της σε μια άλλη λέξη $z = (y_1, \dots, y_{i-1}, y_{i+1}, \dots, y_n)$ με $1 \leq i \leq n$ και τη συμβολίζουμε $w \overset{k}{\to} z$ όπου στη συγκεκριμένη περίπτωση ισχύει $k = 1$, επειδή η αναγωγή πραγματοποιείται σε ένα βήμα. Γενικότερα όμως, για αναγωγές της μορφής $w \overset{k}{\to} z$ με $k \geq 0$, ισχύει ότι η μετάβαση από μια λέξη w σε μια τελική ανηγμένη μορφή z μπορεί να γίνει σε k βήματα (αναγωγές), δηλαδή:

$$w \overset{1}{\to} w^{(1)} \overset{2}{\to} w^{(2)} \overset{3}{\to} w^{(3)} \to \cdots \overset{k}{\to} w^{(k)} = z.$$

Έτσι προκύπτει πως αν υπάρχει $k \geq 0$ τέτοιο ώστε $w \overset{k}{\to} z$, θα λέμε ότι έχουμε αναγωγή της λέξης w στη λέξη z και θα τη συμβολίζουμε με $w \to z$.

Αν όμως η λέξη w είναι ήδη ανηγμένη, τότε $k = 0$, δηλαδή δεν υπάρχει κάποιο βήμα (μεταβατική λέξη) που θα μας οδηγήσει σε κάποια επιθυμητή ανηγμένη μορφή, επειδή η λέξη w είναι ήδη ανηγμένη κι ακόμη κι αν υφίσταται η σχέση $w \to z$, τότε θα ισχύει $w = z$.

Έστω ότι πάρουμε μια λέξη w από το σύνολο των W των λέξεων, που είναι εφοδιασμένο με την πράξη της συνένωσης των λέξεων, και θέλουμε να δείξουμε ότι υφίσταται η αναγωγή της $w \to z$ που θα μας δώσει μια ανηγμένη μορφή z.

Όπως είδαμε πιο πάνω, αν η λέξη που διαλέξουμε είναι ήδη ανηγμένη, τότε θα ισχύει $w = z$. Αν όμως δεν είναι, τότε έστω ότι υπάρχει μια ενδιάμεση λέξη (αναγωγή/βήμα) s έτσι ώστε να έχουμε $w \overset{1}{\to} s$ και μετά $s \overset{2}{\to} z$, με την z να είναι η ανηγμένη λέξη στο αρχικό μας σύνολο. Τώρα, παίρνοντας το μήκος των λέξεων όπως το είδαμε πιο πάνω, μπορούμε να ισχυριστούμε ότι η s έχει μικρότερο μήκος από τη w και κατά συνέπεια έχουμε $w \to z$. Η ανηγμένη λέξη z που βρίσκουμε είναι μοναδική και για να το αποδείξουμε θα πάρουμε τις αναγωγές $w \to z$ και $w \to b$ με τις λέξεις z, b να είναι ανηγμένες. Τότε υπάρχει λέξη p τέτοια ώστε $z \to p$ και $b \to p \Longrightarrow z = b = p$.

Αυτό το ισχυριζόμαστε γιατί γνωρίζουμε τις κάτωθι δύο ιδιότητες που ισχύουν για τις ανηγμένες λέξεις:

i. Έστω ότι έχουμε τις αναγωγές $w \to z$ και $w \to b$. Τότε θα πρέπει να υπάρχει λέξη p τέτοια ώστε $z \to p$ και $b \to p \Longrightarrow z = b = p$.

ii. Εάν έχουμε $w \overset{1}{\to} z$ και $w \overset{1}{\to} b \neq z$, τότε και θα υπάρχει λέξη $p \in W$, τέτοια ώστε $z \overset{1}{\to} p$ και $b \overset{1}{\to} p$.

Αν πάρουμε το σύνολο των ανηγμένων λέξεων στο X, έστω S_X, αυτό θα είναι ομάδα με πράξη την $\cdot$, δηλαδή $w \cdot z = αναγ(wz)$, όπου με $αναγ(wz)$ συμβολίζουμε την αναγωγή από τη λέξη w στη z, δηλαδή $w \to z$.

Για το δείξουμε αυτό, θα πρέπει να πάρουμε $w \overset{1}{\to} z$. Για κάθε λέξη $b \in W$, θα έχουμε $wb \overset{1}{\to} zb$ και $bw \overset{1}{\to} bz$. Άρα και αν $w \to z \Longrightarrow wb \to zb$ και $bw \to bz$ για κάθε λέξη $b \in W$.

Αν οι λέξεις $w, z, b \in W$ είναι ανηγμένες, τότε θα έχουμε:

$$wz \to w \cdot z \text{ και } zb \to z \cdot b \Longrightarrow wzb \longrightarrow (w \cdot z)b \longrightarrow (w \cdot z) \cdot b$$
$$\text{και } wzb \longrightarrow w(z \cdot b) \longrightarrow w \cdot (z \cdot b).$$

Η πράξη $\cdot$ είναι προσεταιριστική και κατά συνέπεια έχουμε:

$$(w \cdot z) \cdot b = w \cdot (z \cdot b).$$

Έστω τώρα η κενή λέξη ε που είναι ανηγμένη και θα αποτελεί το μοναδιαίο στοιχείο της S_X.

Αν και η $w \in W$ είναι ανηγμένη λέξη, τότε $\varepsilon \cdot w = αναγ(\varepsilon w) = αναγ(w) = w$ και $w \cdot \varepsilon = αναγ(w\varepsilon) = αναγ(w) = w$.

Τώρα, παίρνοντας την αντίστροφη της ανηγμένης λέξης w, αυτή θα είναι $w^{-1} = (w_n^{-1}, \dots, w_1^{-1})$. Παρατηρούμε ότι και η w^{-1} είναι ανηγμένη επειδή ισχύει $w_i^{-1} \neq (w_{i-1}^{-1})^{-1}$ για κάθε $i > 1$ και $ww^{-1} \longrightarrow \varepsilon, w^{-1}w \longrightarrow \varepsilon$.

Οπότε συμπεραίνουμε πως η S_X είναι μια ομάδα με πράξη την $\cdot$.

Στην περίπτωση του μονοσύνολου (λέξη με ένα γράμμα), έστω (x), το αντίστροφό του είναι (x^{-1}).

Ορισμός Ι.15

Μια ομάδα G θα ονομάζεται ελεύθερη ομάδα εάν υπάρχει ένα σύνολο γεννητόρων X του G, τέτοιο ώστε κάθε μη κενή ανηγμένη λέξη στο X ορίζει ένα τετριμμένο στοιχείο του G. □

Σε μια τέτοια περίπτωση, το X ονομάζεται ελεύθερη βάση του G και το G ονομάζεται ελεύθερη ομάδα πάνω στο X, ή αλλιώς μια ομάδα που προκύπτει ελεύθερα από τους γεννήτορες X. Κατά συνέπεια, η ελεύθερη ομάδα επί του X, είναι η ομάδα S_X που αποτελείται από τις ανηγμένες λέξεις επί του X. Αυτό συνεπάγεται κι ότι διαφορετικές ανηγμένες λέξεις στο X προσδιορίζουν διαφορετικά στοιχεία του G.

Ορισμός Ι.16
Μια αβελιανή ομάδα S λέμε ότι είναι ελεύθερη μήκους n αν είναι ευθύ άθροισμα n αντιτύπων της άπειρης κυκλικής $\mathbb{Z}$.
Δηλαδή, υπάρχουν $x_1 \in S, i = 1,2, \dots, n$ με:

$$S = \langle x_1 \rangle \oplus \langle x_2 \rangle \oplus \dots \oplus \langle x_n \rangle \text{ και } \langle x_1 \rangle \simeq \mathbb{Z} \text{ για κάθε } i.$$

□

Ορισμός Ι.17
Το $\{x_1, x_2, \dots, x_n\}$ λέγεται βάση της S και λέμε ότι η S είναι ελεύθερη επί του $\{x_1, x_2, \dots, x_n\}$. □

Οπότε προκύπτει ότι αν S ελεύθερη αβελιανή ομάδα μήκους n, τότε:

$$S = \mathbb{Z} \oplus \mathbb{Z} \oplus \dots \oplus \mathbb{Z}, \text{ με } n \text{ αριθμό } \mathbb{Z}$$

και

$$2S = 2\mathbb{Z} \oplus 2\mathbb{Z} \oplus \dots \oplus 2\mathbb{Z}$$

Οπότε και έχουμε:

$$S/2S = S/2\mathbb{Z} \oplus S/2\mathbb{Z} \oplus \dots \oplus S/2\mathbb{Z} = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \dots \oplus \mathbb{Z}_2$$

$$\Longrightarrow |S/2S| = 2^n$$

Γνωρίζουμε πως αν S_1 και S_2 είναι ελεύθερες αβελιανές ομάδες διαστάσεων n_1 και n_2 αντίστοιχα, θα έχουμε και $S_1 \simeq S_2$ αν και μόνον αν $n_1 = n_2$.

γ. Κανονικές Μορφές

Εισαγωγή

Ορισμός Ι.18
Γενικότερα, στη θεωρία ομάδων, μια κανονική μορφή για μια ομάδα G με ένα σύνολο γεννητόρων X, είναι η επιλογή μιας ανηγμένης λέξης από το X για κάθε στοιχείο της G. Μερικά παραδείγματα είναι τα εξής:

- Το σύνολο των ανηγμένων λέξεων από το X είναι μια κανονική μορφή της ελεύθερης ομάδας πάνω στο X.
- Το σύνολο των λέξεων της μορφής $w^m z^n$ με $m, n \in Z$ είναι μια κανονική μορφή από το γινόμενο των κυκλικών ομάδων $\langle x \rangle$ και $\langle y \rangle$.

□

Κανονικές Υποομάδες

Ειδικότερα, ας δούμε τι σημαίνει κανονική υποομάδα.

Ορισμός Ι.19
Έτσι, έστω G μια ομάδα και $H \leq G$. Η υποομάδα H λέγεται κανονική ή αναλλοίωτη (normal) αν ισχύει:

$$gH = Hg, \text{ για κάθε } g \in G$$

Ή ισοδύναμα αν ισχύει:

$$H = gHg^{-1}, \text{ για κάθε } g \in G$$

Και θα συμβολίζεται με $H \trianglelefteq G$ ή $H \lhd G$ όταν είναι σαφές πως $H \subsetneq G$. □

Ας κάνουμε σε αυτό το σημείο και δύο παρατηρήσεις:

(i) Η σχέση $gH = Hg$ σημαίνει ότι τα δύο σύνολα είναι ίσα και όχι ότι το στοιχείο g αντιμετατίθεται με κάθε στοιχείο της H. Έτσι αν έχουμε $h \in H$, τότε το $gh \in Hg$. Άρα θα υπάρχει $h' \in H$ ώστε $gh = h'g$. Φυσικά από τη σχέση αυτή δε μπορούμε να συμπεράνουμε ότι $h = h'$.

(ii) Από τον ορισμό της κανονικής υποομάδας, προκύπτει αμέσως ότι $H \trianglelefteq G$ αν και μόνον αν η H ταυτίζεται με όλες τις συζυγείς υποομάδες της.

Έστω ομάδα G και $H \leq G$. Τα ακόλουθα θα είναι ισοδύναμα:

a. $H \lhd G$.

b. $gH = Hg$, για κάθε $g \in G$.

c. $gHg^{-1} \subseteq H$, για κάθε $g \in G$.

d. $ghg^{-1} \in H$, για κάθε $g \in G$ και για κάθε $h \in H$.

Από τα πιο πάνω, τα a, b και c, d είναι κατά προφανή τρόπο ισοδύναμα.

Άρα για να αποδειχθούν όλα τους, αρκεί να δείξουμε ότι από το a όπου έχουμε ισότητα θα πάρουμε τον εγκλεισμό που απαιτείται στην c. Αντιστρόφως, αν $gHg^{-1} \subseteq H$, για κάθε $g \in G$, τότε $H \subseteq g^{-1}Hg$, για κάθε $g \in G$. Ενώ για $g = g^{-1}$ θα πάρουμε $H \subseteq gHg^{-1}$. Οπότε:

$$\Longrightarrow gHg^{-1} = H$$

Παράδειγμα Ι.4
Παραδείγματα κανονικής υποομάδας:

1. Έστω ομάδα G. Τότε ισχύουν τα εξής: $\{1\} \lhd G$ και $G \lhd G$.

2. Κάθε υποομάδα μιας αβελιανής ομάδας είναι κανονική υποομάδα. Το αντίστροφο δεν ισχύει.

3. Η τομή κανονικών υποομάδων (και απείρου πλήθους) είναι κανονική υποομάδα.

□

Ιδιότητες Κανονικών Μορφών

Όμως, Κανονικές Μορφές υπάρχουν και στα Στοιχεία Ομάδων, και αποτελούν τους κύριους μηχανισμούς απόκρυψης για τα Κρυπτογραφικά πρωτόκολλα.

Μια κανονική μορφή θα πρέπει να έχει δύο σημαντικές ιδιότητες:

1. Κάθε αντικείμενο προς συζήτηση θα πρέπει να έχει ακριβώς μια κανονική μορφή.

2. Δύο αντικείμενα που έχουν την ίδια κανονική μορφή, θα πρέπει να παραμείνουν το ίδιο μέχρι κάποια συνθήκη ισορροπίας. Η συνθήκη μοναδικότητας που ορίζεται στο σημείο (1) πιο πάνω, μερικές φορές μπορεί να είναι πιο χαλαρή, επιτρέποντας την κανονικότητα να είναι μοναδική μέχρι κάποια απλή συνθήκη ισορροπίας.

Παράδειγμα Ι.5
Οι προαναφερθείσες κανονικές μορφές μπορούν να είναι απλές και αυτονόητες, αλλά μπορεί να είναι και πιο σύνθετες. Μερικά τέτοια παραδείγματα είναι:

i. Στην προσθετική ομάδα ακεραίων, συναντάμε πολλές αυτονόητες κανονικές μορφές, όπως οι δεκαδικές, οι δυαδικές κτλ. Αυτές είναι πολύ χρήσιμες όταν θέλουμε να κρύψουμε παράγοντες σε ένα γινόμενο, όπως στο γινόμενο $3 \cdot 7 = 21$, όπου δε μπορούμε να δούμε το 3 ή το 7. Στο σημείο αυτό μπορούμε να κάνουμε μια επιπλέον επισήμανση που είναι σημαντική από τη σκοπιά της κρυπτογραφίας. Εάν υπάρχουν αρκετές διαφορετικές κανονικές μορφές των στοιχείων μιας δεδομένης ομάδας, τότε μια κανονική μορφή μπορεί να αποκαλύψει αυτό που μια άλλη προσπαθεί να κρύψει. Ένα τέτοιο παράδειγμα θα μπορούσε να είναι ο αριθμός 48, ο οποίος στην δεκαδική του μορφή φαίνεται ένας τυχαίος αριθμός, ενώ στη δυαδική του μορφή γίνεται πιο συγκεκριμένος και προσδιορίζεται καλύτερα 00110000.
Υπάρχουν κι άλλες μοναδικές κανονικές μορφές που σχετίζονται με τους ακεραίους. Ένα τέτοιο πρόβλημα παραγοντοποίησης είναι το πρόβλημα στο οποίο ζητάμε κάθε ακέραιος να γραφτεί με τη μορφή του γινομένου πρώτων αριθμών που βρίσκονται σε αύξουσα σειρά.

ii. Σε μια ομάδα πινάκων σε ένα Δακτύλιο R, κάθε πίνακας είναι μια κανονική μορφή του εαυτού του. Αυτή η κανονική μορφή θα είναι μοναδική μέχρι να έχουμε ισότητα ως προς τις καταχωρήσεις στο Δακτύλιο R.

iii. Σε κάποιες ομάδες που παίρνουμε από γεννήτορες και ορίζουσες σχέσεις, υπάρχουν συστήματα επανεγγραφής, δηλαδή διαδικασίες που παίρνουν ως καταχώρηση (στην είσοδο) μια λέξη σε ένα συγκεκριμένο αλφάβητο και τη μετατρέπουν σε μια άλλη λέξη στο ίδιο αλφάβητο, χρησιμοποιώντας τις ορίζουσες σχέσεις. Η όλη διαδικασία τερματίζεται με την κανονική μορφή του στοιχείου της ομάδας που αναπαρίσταται από την λέξη της εισόδου.
Σε άλλες πάλι περιπτώσεις ομάδων που παίρνουμε από γεννήτορες και ορίζουσες σχέσεις, οι κανονικές μορφές μπορεί να βασίζονται σε κάποιες ειδικές (τοπολογικές, γεωμετρικές ή άλλες) ιδιότητες μιας δεδομένης ομάδας και όχι απλά σε ένα σύστημα επανεγγραφής. Ένα τέτοιο παράδειγμα μπορούμε να συναντήσουμε και στις Ομάδες Πλεξίδων. Υπάρχουν πάρα πολλές διαφορετικές κανονικές μορφές για τα στοιχεία μιας Ομάδας Πλεξίδων, με την κλασσική μορφή, που είναι γνωστή ως Κανονική Μορφή Garside, να μην είναι καν λέξη στους γεννήτορες της ομάδας.

□

δ. Ομομορφισμοί και Ισομορφισμοί

Εισαγωγή

Έστω ότι έχουμε δύο ομάδες G και G'. Αυτό που μας ενδιαφέρει να μελετήσουμε είναι οι απεικονίσεις (αντιστοιχίσεις) από την ομάδα G στην G', που συσχετίζουν τη δομή της ομάδας G με τη δομή της ομάδας G'. Μια τέτοια απεικόνιση μπορεί να μας δώσει πληροφορίες για μια ομάδα, από τις δομικές ιδιότητες μιας άλλης. Μια τέτοια περίπτωση απεικόνισης (συσχέτισης δομικών ιδιοτήτων) είναι ο ισομορφισμός, έστω $\varphi : G \longrightarrow G'$. Δηλαδή με απλά λόγια, αν γνωρίζουμε τα πάντα για την ομάδα G και επίσης γνωρίζουμε ότι η φ είναι ισομορφισμός , τότε θα γνωρίζουμε τα πάντα και για τις δομικές ιδιότητες της ομάδας G', επειδή αυτή αποτελεί ένα αντίγραφο της G.

Ας δούμε όμως πιο συγκεκριμένα τι είναι ομομορφισμός και ισομορφισμός.

Ορισμός Ι.20
Έτσι, μια απεικόνιση φ από μια ομάδα G σε μια άλλη ομάδα G'. Αυτή θα είναι ομομορφισμός εάν ισχύει η ιδιότητα του ομομορφισμού για όλα τα $w, z \in G$, δηλαδή η:

$$\varphi(wz) = \varphi(w)\,\varphi(z)$$

Στην πιο πάνω εξίσωση, το γινόμενο wz στο αριστερό μέλος προέρχεται από την ομάδα G, ενώ το γινόμενο $\varphi(w)\,\varphi(z)$ στο δεξιό μέλος προέρχεται από την ομάδα G'. Κατά συνέπεια η εξίσωση αυτή μας δίνει μια σχέση ανάμεσα σε δυαδικές πράξεις και επομένως και μεταξύ των δομών των δύο ομάδων. □

Ανάμεσα σε δύο ομάδες G και G' υπάρχει πάντα τουλάχιστον ένας ομομορφισμός $\varphi : G \longrightarrow G'$, που θα τον ονομάσουμε τετριμμένο ομομορφισμό και ορίζεται από τη σχέση $\varphi\,(g) = e'$, για όλα τα $g \in G$, όπου e' είναι το ταυτοτικό στοιχείο της G'. Η εξίσωση αυτή μπορεί να αναχθεί στην αληθή εξίσωση $e' = e'e'$. Όμως από τον τετριμμένο ομομορφισμό δε μπορούμε να πάρουμε πληροφορίες για τη δομή μιας εκ των ομάδων G ή G' από την άλλη.

Ορισμός Ι.21
Ο ομομορφισμός φ θα ονομαστεί μονομορφισμός αν είναι $1-1$ και επιμορφισμός αν είναι *επί*.

Ενώ στην περίπτωση που ένας ομομορφισμός είναι $1-1$ και *επί*, τότε θα ονομάζεται ισομορφισμός. Σε μια τέτοια περίπτωση θα ονομάζουμε τις ομάδες G και G' ισόμορφες και θα συμβολίζουμε $G \simeq G'$.

Τέλος, ενδομορφισμό θα καλούμε έναν ομομορφισμό $G \to G$ και αυτομορφισμό ένα ισομορφισμό $G \to G$. □

Ιδιότητες Ομομορφισμών & Ισομορφισμών

Ας δούμε μερικές παρατηρήσεις στα πιο πάνω:

(i) Αν $\varphi: G \to G'$ ομομορφισμός ομάδων, τότε $\varphi(1_G) = 1_{G'}$.
Αυτό προκύπτει από
$\varphi(1_G) = \varphi(1_G \cdot 1_G) = \varphi(1_G)\varphi(1_G) \Rightarrow \varphi(1_G) = 1_{G'}$.

(ii) Αν $\varphi: G \to G'$ ομομορφισμός ομάδων, τότε $\varphi(w^{-1}) = (\varphi(w))^{-1}$ για κάθε $w \in G$.
Αυτό προκύπτει από $1_{G'} = \varphi(1_G) = \varphi(ww^{-1}) = \varphi(w)\varphi(w^{-1})$.
Άρα $\varphi(w^{-1}) = (\varphi(w))^{-1}$.

(iii) Ορισμός Ι.22
Έστω $\varphi: G \to G'$ ένας ομομορφισμός ομάδων.
Τότε θα ορίσουμε ως εικόνα του φ:

$$im\varphi = \{\varphi(w) : w \in G\} = \varphi(G)$$

Η εικόνα του φ είναι υποομάδα της G'. □

(iv) Ορισμός Ι.23
Θα ορίσουμε τον πυρήνα του φ:

$$ker\varphi = \{w \in G : \varphi(w) = 1_{G'}\} = \varphi^{-1}(1_{G'})$$

Ο πυρήνας του φ είναι κανονική υποομάδα της G. □

(v) Αν $w \in ker\varphi$ και $z \in G$, τότε $\varphi(zwz^{-1}) = \varphi(z)\varphi(w)\varphi(z^{-1}) = 1_{G'}$

(vi) Έστω $\varphi: G \to G'$ ομομορφισμός ομάδων. Τότε ο φ είναι $1-1$ αν και μόνον αν $ker\varphi = \{1\}$.
Αυτό προκύπτει από το γεγονός αν ο φ είναι $1-1$, τότε $ker\varphi = \{1\}$.
Ενώ αντιστρόφως, αν $ker\varphi = \{1\}$ και $\varphi(w) = \varphi(z)$, τότε:
$\varphi(wz^{-1}) = 1 \Longrightarrow wz^{-1} \in ker\varphi = \{1\}$. Οπότε και παίρνουμε $w = z$.

Παράδειγμα Ι.6
Εδώ μπορούμε να δώσουμε κι ένα παράδειγμα. Έτσι, έστω ένας ομομορφισμός ομάδας $\varphi : G \longrightarrow G'$ από την ομάδα G στην ομάδα G'. Ισχυριζόμαστε ότι αν η

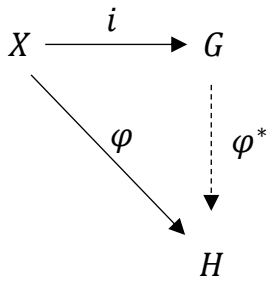
ομάδα G είναι αβελιανή, τότε και η ομάδα G' πρέπει να είναι αβελιανή. Έστω τώρα $w', z' \in G'$. Αυτό που πρέπει να δείξουμε είναι ότι $w'z' = z'w'$. Όμως καθότι η φ αποτελεί απεικόνιση στο G', τότε θα πρέπει να υπάρχουν $w, z \in G$ τέτοια ώστε να έχουμε $\varphi(w) = w'$ και $\varphi(z) = z'$. Όμως η G είναι αβελιανή, οπότε $wz = zw$. Από την πιο πάνω σχέση, όπου $\varphi(wz) = \varphi(w)\,\varphi(z)$, θα έχουμε $w'z' = \varphi(w)\varphi(z) = \varphi(wz) = \varphi(zw) = \varphi(z)\varphi(w) = z'w'$, οπότε και G' είναι αβελιανή. □

Οπότε είναι προφανές ότι μέσω του ισομορφισμού $\varphi : G \longrightarrow G'$ μπορούμε να πάρουμε πληροφορίες για την ομάδα G από την ομάδα G'.

Αν θέλουμε να δούμε και διαγραμματικά την πιο πάνω σχέση, θα μελετήσουμε πιο κάτω την καθολική ιδιότητα των ελεύθερων ομάδων. Έτσι, έστω μια ομάδα G που παράγεται από ένα σύνολο X, όπου $X \subseteq G$. Τότε κάθε απεικόνιση $\varphi : X \longrightarrow H$ από το X στην ομάδα H μπορεί να επεκταθεί στον πιο κάτω μοναδικό ομομορφισμό:

$$\varphi^* : G \longrightarrow H$$

που σημαίνει ότι το πιο κάτω διάγραμμα είναι μεταθετικό:



Σχήμα Ι.1

Από το πιο πάνω διάγραμμα είναι προφανές ότι έχουμε έναν ομομορφισμό $\varphi^* : G \longrightarrow H$ τέτοιο ώστε $\varphi = \varphi^* \circ i$.

<u>Απόδειξη Ι.1</u>

Για να το αποδείξουμε, πρώτα πρέπει να δείξουμε τη μοναδικότητα. Θα πάρουμε τον ομομορφισμό $\varphi^* : G \longrightarrow H$ ώστε $\varphi = \varphi^* \circ i$. Τώρα θα επεκτείνουμε την φ στο X^{-1} έτσι ώστε $\varphi(x^{-1}) = \varphi(x)^{-1}$ για κάθε $x \in X$ και θα πάρουμε:

$$\varphi^*\big(i(x)\big) = \varphi(x) \text{ και } \varphi^*\big(i(x^{-1})\big) = \varphi^*(i(x)^{-1}) = \varphi(x)^{-1} = \varphi(x^{-1})$$

Εφ' όσων η φ^* είναι ομομορφισμός, αν η $w = (w_1, \dots, w_n)$ είναι ανηγμένη λέξη, τότε:

$$\varphi^*(w) = \varphi^*\big(i(w_1) \dots i(w_n)\big) = \varphi(w_1) \dots \varphi(w_n)$$

Οπότε δείξαμε τη μοναδικότητα. Τώρα πρέπει να δείξουμε τον ομομορφισμό.

Θα πάρουμε την απεικόνιση $\varphi^* : G \longrightarrow H$, όπου $\varphi^*(w) = \varphi(w_1) \dots \varphi(w_n)$ με $w = (w_1, \dots, w_n)$ ανηγμένη λέξη. Χρησιμοποιώντας τον τύπο αυτόν για κάθε λέξη (ακόμη κι αν δεν είναι ανηγμένη) θα προβούμε σε επέκταση της φ^* στη συνένωση λέξεων που είδαμε και πιο πριν, τη W.

Έτσι προκύπτει ότι: $\varphi^*(wz) = \varphi^*(w)\varphi^*(z)$, για κάθε $w, z \in W$.

Αν όμως $w \overset{1}{\rightarrow} z \Longrightarrow \varphi^*(w) = \varphi^*(z)$. Αυτό προκύπτει από τα $w = (w_1, \dots, w_n)$ όπου $w_{i+1} = w_i^{-1}$ και $z = (z_1, \dots, z_{i-1}, z_{i+2}, \dots, z_n)$, με $1 \leq i \leq n$. Άρα παίρνουμε:

$$\varphi(w_{i+1}) = \varphi(w_i)^{-1}$$

$$\begin{aligned} \varphi^*(w) &= \varphi(w_1) \dots \varphi(w_{i-1})\varphi(w_i)\varphi(w_{i+1})\varphi(w_{i+2}) \dots \varphi(w_n) \\ &= \varphi(w_1) \dots \varphi(w_{i-1})\varphi(w_{i+2}) \dots \varphi(w_n) \\ &= \varphi^*(z) \end{aligned}$$

Άρα $w \longrightarrow z \Rightarrow \varphi^*(w) = \varphi^*(z)$

Όμως όταν οι λέξεις w, z είναι ανηγμένες, θα έχουμε:

$$\varphi^*(w \cdot z) = \varphi^*(wz) = \varphi^*(w)\varphi^*(z)$$

κάτι που μας οδηγεί στο ασφαλές συμπέρασμα ότι η φ είναι ομομορφισμός ομάδων. □

Θεωρήματα Ισομορφισμών

Στη συνέχεια ας δούμε μερικά θεωρήματα ισομορφισμών:

Σύμπλοκα:

Ορισμός Ι.24
Έστω ομάδα G και $H \leq G$. Τότε θα ορίσουμε αριστερό σύμπλοκο ένα σύνολο της μορφής $gH = \{gh : h \in H\}$ και δεξιό σύμπλοκο ένα σύνολο της μορφής $Hg = \{hg : h \in H\}$. □

Κανονική Υποομάδα (Ορίστηκε πλήρως στην προηγούμενη ενότητα):

Ορισμός Ι.25
Έστω μια ομάδα G και $H \leq G$. Η H λέγεται κανονική υποομάδα της G, και γράφουμε $H \lhd G$, αν $gHg^{-1} = H$ για κάθε $g \in G$. □

Ομάδα Πηλίκο:

Ορισμός Ι.26
Έστω μια ομάδα G, και H μια κανονική υποομάδα της G. Και έστω G/H το σύνολο των αριστερών συμπλόκων της H στη G. Το σύνολο G/H εφοδιασμένο με την πράξη πολλαπλασιασμού που ορίζεται ως $g_1H \cdot g_2H = g_1g_2H$ για κάθε $g_1, g_2 \in G$, αποκτά τη δομή ομάδας και ονομάζεται ομάδα πηλίκο. □

Έστω ομάδα G, $H \lhd G$ και G/N η αντίστοιχη ομάδα πηλίκο. Τότε η απεικόνιση:

$$\pi: G \longrightarrow G/N, \qquad g \mapsto gN$$

Είναι επιμορφισμός και ονομάζεται φυσικός (ή κανονικός) επιμορφισμός.

1ο Θεώρημα Ισομορφισμών

Θεώρημα Ι.1
Έστω ομάδα G και $\varphi : G \to H$ ένας ομομορφισμός ομάδων. Τότε ο φ επάγει ισομορφισμό ομάδων:

$$\varphi' : G/ker\varphi \ \to im\varphi$$

Οπότε προκύπτει πως κάθε επιμορφική εικόνα της G είναι (ως προς τον ισομορφισμό) ομάδα πηλίκο της G.

Και έτσι όταν G πεπερασμένη ομάδα και $\varphi : G \to H$ ένας ομομορφισμός ομάδων, τότε:

$$|G| = |ker\varphi| \cdot |im\varphi|$$

□

2ο Θεώρημα Ισομορφισμών

Θεώρημα Ι.2
Έστω ομάδα G, $H \lhd G$ και $H \leq G$. Τότε θα έχουμε:

$$H \cap N \lhd H, HN \leq G \text{ και } H/H \cap N \simeq HN/N$$

□

3ο Θεώρημα Ισομορφισμών

Θεώρημα Ι.3
Έστω ομάδα G, $N \lhd H \lhd G$ και $N \lhd G$. Τότε θα έχουμε:

$$G/H \simeq (G/N) \,/\, (H/N)$$

□

Θεώρημα της Αντιστοιχίας

Θεώρημα Ι.4
Έστω $\varphi : G \longrightarrow G'$ επιμορφισμός ομάδων και $K = ker\varphi$. Τότε ο φ επάγει μια $1-1$ και $επί$ αντιστοιχία φ', μεταξύ της οικογένειας A των υποομάδων της G που περιέχουν τον πυρήνα K και της οικογένειας B των υποομάδων της G' ως εξής:

Αν $H \in A$, τότε $\varphi'(H) = \varphi(H) = H'$ και αν $H' \in B$, τότε $\varphi'^{-1} : H' \mapsto \varphi^{-1}(H')$.

Κι επιπλέον για $H, H_1 \in A$ έχουμε:

(i) $\varphi(H_1) \subseteq \varphi(H) \Leftrightarrow H_1 \subseteq H$, στην οποία περίπτωση

$$[H : H_1] = [\varphi(H) : \varphi(H_1)].$$

(ii) $\varphi(H) \lhd \varphi(G) \Leftrightarrow H \lhd G$ και σε αυτή την περίπτωση

$$G/H \simeq \varphi(G)/\varphi(H).$$

□

ε. Απεικονίσεις & Παραστάσεις Ομάδων

Η παράσταση μιας ομάδας μας βοηθάει στον ορισμός της. Έτσι κάποιος μπορεί να προσδιορίσει ένα σύνολο X από γεννήτορες έτσι ώστε κάθε στοιχείο της ομάδας να μπορεί να γραφτεί ως γινόμενο δυνάμεων κάποιων εκ των γεννητόρων κι ένα σύνολο R από σχέσεις, εκ των γεννητόρων και πάλι. Τότε λέμε ότι η G έχει την παράσταση:

$$\langle X \mid R \rangle$$

Μιλώντας πιο ελεύθερα, η G έχει την πιο πάνω παράσταση εάν είναι η «πιο ελεύθερη ομάδα» που παράγεται από το σύνολο X και υπόκειται μόνον στις σχέσεις R.

Σε έναν πιο αυστηρό ορισμό, η ομάδα G θα έχει την πιο πάνω παράσταση, εάν είναι ισομορφική προς το πηλίκο μια ελεύθερης ομάδας στο X, με την κανονική υποομάδα να παράγεται από τις σχέσεις R.

Ένα απλό παράδειγμα αποτελεί η κυκλική ομάδα μήκους n που έχει ως παράσταση:

$$\langle w \mid w^n = 1 \rangle$$

Με το 1 να αποτελεί την ταυτοτική ομάδα. Οπότε αυτό θα μπορούσε να γραφτεί κατά ισοδύναμο τρόπο και:

$$\langle w \mid w^n \rangle$$

με τους όρους που δεν περιέχουν κάποιο σύμβολο ισότητας να θεωρούνται ίσοι ως προς την ταυτοτική ομάδα. Ένας τέτοιος όρος καλείται ορίζουσα σχέση έτσι ώστε να την ξεχωρίσουμε από τις σχέσεις που περιέχουν την ισότητα.

Κάθε ομάδα έχει πολλές και διάφορες παραστάσεις. Συνήθως, η παράσταση είναι ο πιο σύντομος τρόπος για να περιγράψεις τη δομή μιας ομάδας.

Η καθολική ιδιότητα των ελεύθερων ομάδων μας δίνει τη δυνατότητα να περιγράψουμε τυχαίες ομάδες με βάσει τους γεννήτορες και τις ορίζουσες σχέσεις.

Έτσι, έστω μια ομάδα G με ένα σύνολο γεννητόρων X. Από την καθολική ιδιότητα των ελεύθερων ομάδων θα πρέπει να υπάρχει ένας ομομορφισμός $y : S(X) \longrightarrow G$ τέτοιο ώστε $y(x) = x$ με $x \in X$.

Προκύπτει ότι η y είναι $επί$ κι έτσι από το πρώτο θεώρημα ισομορφισμού θα έχουμε:

$$G \simeq {S(X)}\Big/{\ker(y)}$$

Αν θα θέλαμε να το δούμε λίγο πιο απλά, θα μπορούσαμε να πούμε ότι η καθολική ιδιότητα που είδαμε πιο πάνω, μας πληροφορεί πως κάθε απεικόνιση φ του X σε μια ομάδα G μπορεί να επεκταθεί κατά μοναδικό τρόπο σε έναν ομομορφισμό $y : S(X) \longrightarrow G$.

Αν έχουμε $X \subseteq G$, τότε η y θα αποτελεί απεικόνιση ενός στοιχείου της $S(X)$, που θα είναι γινόμενο στοιχείων και αντιστρόφων στοιχείων του X, σε ένα ίδιο γινόμενο υπολογισμένο στην ομάδα G. Ο πυρήνας $kery$ του ομομορφισμού y μπορεί να είναι και μη τετριμμένος. Τότε είναι που θα έχουμε ανηγμένη λέξη $w \in S(X)$ τέτοια ώστε $y(w) = 1$.

Όμως τότε, από το 1ο Θεώρημα Ισομορφισμών που είδαμε πιο πάνω θα έχουμε:

$$imy \simeq S(X)/\ker(y)$$

Όμως αν $G = \langle X \rangle$, τότε η y είναι επιμορφισμός και επομένως:

$$S(X)/\ker(y) \simeq G$$

που σημαίνει ότι η G είναι πηλίκο της ελεύθερης ομάδας $S(X)$.

Τώρα θα πάρουμε μια ομάδα G κι ένα σύνολο X τέτοιο ώστε $G = \langle S \rangle$. Έστω $S(X)$ η ελεύθερη ομάδα επί του X και έστω y ο μοναδικός ομομορφισμός της $S(X)$ στην G. Τότε η G θα είναι ισόμορφη ως προς το πηλίκο $S(X)/kery$. Όμως, καθότι $kery \lhd S(X)$, θα υπάρχει $R \subseteq S(X)$ τέτοιο ώστε να ισχύει το πιο κάτω που μας δείχνει ότι η G εξαρτάται πλήρως από το σύνολο των γεννητόρων X και το σύνολο R:

$$kery = \langle R \rangle^{S(X)} = \bigcap \{H : H \lhd S(X) \; και \; R \subseteq H\}$$

Ορισμός Ι.27

Το R όμως δε μας είναι τελείως άγνωστο. Το είδαμε και πιο πάνω. Και πιο συγκεκριμένα θα μπορούσαμε να το ορίσουμε μαζί με την ιδιότητα $kery = \langle R \rangle^{S(X)}$ ως το σύνολο των οριζουσών σχέσεων της G και κάθε στοιχείο του R θα καλείται ορίζουσα σχέση για την G. □

Έτσι και μια ομάδα G θα μπορεί να συμβολιστεί από την παράστασή της, δηλαδή το ζεύγος $\langle X \mid R \rangle$.

Προς την αντίστροφη κατεύθυνση, όταν έχουμε ένα σύνολο X και ένα $R \subseteq S(X)$, τότε μαζί και τα δύο μας δίνουν την παράσταση μιας ομάδας $\langle X \mid R \rangle$.

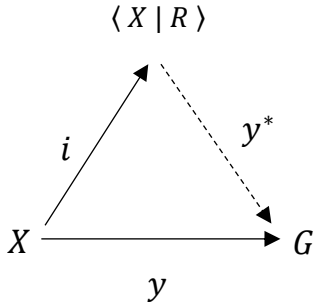
Αν πάρουμε τις απεικονίσεις $i : X \to S(X)$ και $k : S(X) \to S(X)/\langle R \rangle^{S(X)}$ και στη συνέχεια τη σύνθεσή τους, δηλαδή την $f : k \circ i \Rightarrow f : X \to \langle X \mid R \rangle$, θα πάρουμε στο τέλος τη ζητούμενη ομάδα.

Καθολική Ιδιότητα του Von Dyck:

Θεώρημα Ι.5
Έστω μια ελεύθερη αβελιανή ομάδα $\langle X \mid R \rangle$ (όπου X σύνολο και R σύνολο σχέσεων μεταξύ των στοιχείων του X) με βάση $\{x_1, x_2, \dots, x_n\}$. Τότε για κάθε αβελιανή ομάδα G και απεικόνιση $y : X = \{x_1, x_2, \dots, x_n\} \to G$, θα υπάρχει μοναδικός ομομορφισμός $y^* : \langle X \mid R \rangle \to G$ που μας επεκτείνει την y. Δηλαδή $y = y^* \circ i$ με i να είναι η απεικόνιση $i : X \to \langle X \mid R \rangle$. □

Στην ιδιαίτερη περίπτωση που η εικόνα $y(X)$ παράγει τη G, θα έχουμε ότι η y^* είναι επιμορφισμός.

Διαγραμματικά μπορούμε να αποδώσουμε το πιο πάνω ως εξής:



Σχήμα Ι.2

Η y^*είναι μοναδική γιατί καθορίζεται πλήρως από τα $y(x_i)$ κι οπότε το παραπάνω διάγραμμα είναι μεταθετικό.

Το συμπέρασμα που προκύπτει είναι ότι αν μια ομάδα G παράγεται από ένα σύνολο X και κάθε ορίζουσα σχέση του R ισχύει στην G, τότε θα έχουμε και επιμορφισμό ομάδων $\langle X \mid R \rangle \to G$ άρα και η G είναι ισόμορφη με μία ομάδα πηλίκο της $\langle X \mid R \rangle$.

Εδώ θα πρέπει να επισημάνουμε ότι παρ' όλο που μια ομάδα G ορίζεται μοναδικά από ένα ζεύγος (X, R), το ζεύγος (X, R) που ορίζει την προαναφερθείσα ομάδα G δεν είναι απαραίτητο ότι είναι μοναδικό.

Από τα πιο πάνω προκύπτει και μια ιδιότητα σύμφωνα με την οποία αν έχουμε ένα σύνολο X και $R_1, R_2 \subseteq S(X)$ με τα $R_1 \subseteq R_2$, τότε θα πρέπει και η ομάδα με παράσταση $\langle X \mid R_2 \rangle$ να είναι πηλίκο της ομάδας με παράσταση $\langle X \mid R_1 \rangle$.

Ι.1.2. Αλγοριθμικά Προβλήματα σε Ομάδες

Εισαγωγή

Τα αλγοριθμικά προβλήματα που θα δούμε πιο κάτω, θα μπορούσαμε να τα διακρίνουμε σε δύο κατηγορίες, στα Προβλήματα Απόφασης και στα Προβλήματα Αναζήτησης.

Πιο συγκεκριμένα:

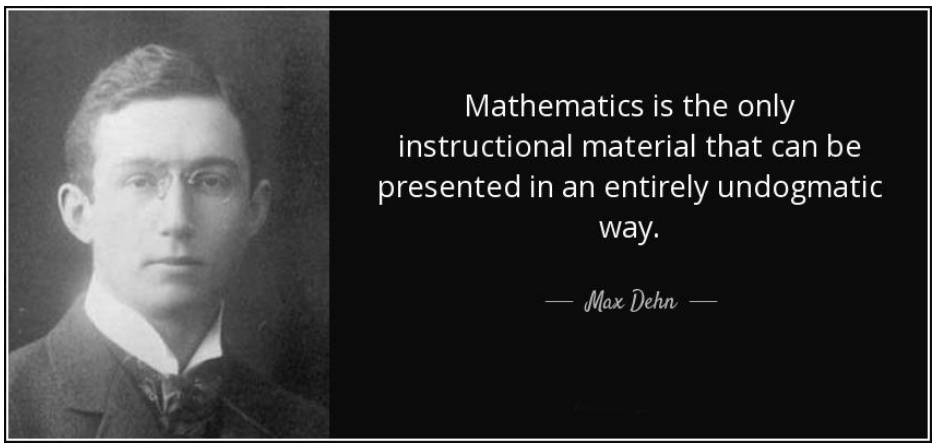
Προβλήματα Απόφασης
Ορισμός Ι.28
Αφορούν προβλήματα της ακόλουθης μορφής, όπου έχουμε μια ιδιότητα $\wp$ κι ένα αντικείμενο $\mathbb{O}$ και θα θέλαμε να βρούμε αν το αντικείμενο $\mathbb{O}$ έχει ή δεν έχει την ιδιότητα $\wp$.□

Προβλήματα Αναζήτησης
Ορισμός Ι.29
Αφορούν προβλήματα της ακόλουθης μορφής, όπου έχουμε μια ιδιότητα $\wp$ και γνωρίζουμε ότι υπάρχουν αντικείμενα με την ιδιότητα $\wp$ και θέλουμε να βρούμε τουλάχιστον ένα αντικείμενο με την ιδιότητα $\wp$.□

Ας δούμε τώρα πιο συγκεκριμένα μερικά αλγοριθμικά προβλήματα της θεωρίας ομάδων που έχουν χρησιμοποιηθεί στην κρυπτογραφία.

α. Το πρόβλημα της συζυγίας

Το πρόβλημα αποδόθηκε αρχικά από τον Max Dehn το 1911 και θεωρείται ένα από τα πλέον σημαντικά προβλήματα απόφασης στη θεωρία ομάδων. Ο ίδιος, το 1912, έδωσε έναν αλγόριθμο που επίλυε το πρόβλημα συζυγίας και την ειδική του περίπτωση, το πρόβλημα της λέξης.



Φωτογραφία Ι.1

Θα αναλύσουμε τώρα δύο μορφές του προβλήματος.

Ορισμός Ι.28
Το πρόβλημα συζυγίας (ή αλλιώς πρόβλημα μετασχηματισμού) υφίσταται όταν έχουμε μια αναδρομική παράσταση μιας ομάδας G και δύο στοιχεία $g, h \in G$, και πρέπει να βρούμε αν υπάρχει ή όχι κάποιο στοιχείο $x \in G$, τέτοιο ώστε $x^{-1}gx = h$. □

Με άλλα λόγια, όταν έχουμε μια ομάδα G με συγκεκριμένη παράσταση και δύο στοιχεία της $g, h \in G$, το πρόβλημα μας θα μπορέσει να επιλυθεί για την G εάν βρούμε τρόπο να απαντήσουμε ως προς την ύπαρξη ή μη κάποιου στοιχείου $x \in G$, τέτοιο ώστε $x^{-1}gx = h$.

Το πρόβλημα της συζυγίας περιέχει τις απαντήσεις «ΝΑΙ» και «ΟΧΙ», με το «ΝΑΙ» να είναι πάντα αναδρομικό γιατί κάποιος μπορεί πάντα να απαριθμήσει όλες τις συζυγίες ενός δεδομένου στοιχείου.

Το πρόβλημα αναζήτησης συζυγίας υφίσταται όταν έχουμε την αναδρομική παράσταση μιας ομάδας G και δύο συζυγή στοιχεία $g, h \in G$ και πρέπει να βρούμε ένα συγκεκριμένο στοιχείο $x \in G$, τέτοιο ώστε $x^{-1}gx = h$.

Είναι προφανές ότι το πρόβλημα της αναζήτησης συζυγίας έχει πάντα μια αναδρομική λύση, γιατί κάποιος μπορεί να απαριθμήσει αναδρομικά όλες τις

συζυγίες ενός δεδομένου στοιχείου. Όμως, μια τέτοια λύση ενδέχεται να είναι υπερβολικά δύσκολη.

Πλέον γνωρίζουμε ότι για αρκετές κλάσεις ομάδων δε μπορούμε να αποφανθούμε για το αν το πιο πάνω πρόβλημα επιλύεται, ενώ για κάποιες άλλες κλάσεις παραστάσεων ομάδων, γνωρίζουμε ότι είναι επιλύσιμο, όπως οι Ομάδες Πλεξίδων, Ομάδες Κόμβων, Ελεύθερες Ομάδες (χωρίς τον ορισμό ορίζουσών σχέσεων), Οι πεπερασμένα παραγόμενες αβελιανές ομάδες, κτλ.

Μια ειδική περίπτωση του προβλήματος αποτελεί το πρόβλημα της λέξης, που θα δούμε και πιο κάτω αναλυτικά, στο οποίο έστω ότι έχουμε τις λέξεις w και z με τα γράμματά τους από ένα σύνολο γεννητόρων και θέλουμε να αποφανθούμε για το αν ταυτίζονται. Δηλαδή να εξετάσουμε αν η λέξη wz^{-1} είναι συζυγής ως προς το μοναδιαίο στοιχείο, δηλαδή αν ισούται με αυτό.

β. Το πρόβλημα της διάσπασης

Ορισμός Ι.29
Μια διαφορετική εκδοχή του προβλήματος αναζήτησης συζυγίας είναι το πρόβλημα της διάσπασης που σχετίζεται με τις υποομάδες. Στο πρόβλημα αυτό έχουμε την αναδρομική παράσταση μιας ομάδας G, δύο αναδρομικώς παραγόμενες υποομάδες $A, B \leq G$ και δύο στοιχεία $g, h \in G$ και πρέπει να βρούμε δύο στοιχεία $x \in A$ και $y \in B$, που θα ικανοποιούσαν τη σχέση $x \cdot g \cdot y = h$, δεδομένου ότι τουλάχιστον ένα τέτοιο ζευγάρι υπάρχει. □

Το αντίστοιχο πρόβλημα απόφασης δεν έχει εφαρμογές στην Κρυπτογραφία και κατά συνέπεια δεν κάνουμε σχετική αναφορά.

Αν παρατηρήσουμε λίγο καλύτερα το πιο πάνω πρόβλημα, θα διαπιστώσουμε ότι υπάρχουν πάντα κάποια x και y που ικανοποιούν τη σχέση $x \cdot g \cdot y = h$. Μια τέτοια περίπτωση είναι το ζεύγος $x = 1, y = g^{-1}h$. Οπότε το ζητούμενο που μένει και μας ενδιαφέρει είναι να ελέγξουμε αν τα οποιαδήποτε x, y θα ικανοποιούν και τις συνθήκες $x \in A$ και $y \in B$.

Δύο γνωστά παραδείγματα του προβλήματος διάσπασης είναι το πρόβλημα διπλού συμπλόκου και το πρόβλημα της παραγοντοποίησης.

Ορισμός Ι.30
Πιο συγκεκριμένα, για $A = B$, θα έχουμε την περίπτωση του προβλήματος του διπλού συμπλόκου. □

Ορισμός Ι.31
Ενώ όταν έχουμε $g = 1$, πρόκειται για το πρόβλημα της παραγοντοποίησης, που μπορεί να επιμεριστεί στο πρόβλημα απόφασης και στο πρόβλημα αναζήτησης. Έτσι:

Στο πρόβλημα απόφασης της παραγοντοποίησης, έχουμε ένα στοιχείο w μιας αναδρομικώς παριστάμενης ομάδας G και δύο υποομάδες $A, B \leq G$ και πρέπει να βρούμε αν υπάρχουν ή όχι δύο στοιχεία $\alpha \in A$ και $b \in B$ τέτοια ώστε $\alpha \cdot b = w$. □

Ορισμός Ι.32
Ενώ στο πρόβλημα αναζήτησης της παραγοντοποίησης, έχουμε ένα στοιχείο w μιας αναδρομικώς παριστάμενης ομάδας G και δύο αναδρομικώς παραγόμενες υποομάδες $A, B \leq G$ και πρέπει να βρούμε δύο στοιχεία $\alpha \in A$ και $b \in B$ που να ικανοποιούν τη σχέση $\alpha \cdot b = w$, δεδομένου ότι τουλάχιστον ένα τέτοιο ζεύγος στοιχείων υπάρχει. □

γ. Το πρόβλημα της λέξης

Ορισμός Ι.33
Ένα από τα πλέον γνωστά αλγοριθμικά προβλήματα αυτής της κατηγορίας είναι το πρόβλημα της λέξης. Σε αυτό το πρόβλημα έχουμε την αναδρομική παράσταση μιας ομάδας G κι ένα στοιχείο $g \in G$ και ψάχνουμε να βρούμε αν ισχύει $g = 1$ στο G. □

Εάν θα θέλαμε να το προσεγγίσουμε από τη σκοπιά των γεννητόρων και οριζουσών σχέσεων, θα παίρνουμε μια ομάδα G, και στη συνέχεια δύο σύνολα. Το σύνολο των γεννητόρων $X = \{x_1, \dots, x_n\}$ και το σύνολο των οριζουσών σχέσεων $R = \{r_1, \dots, r_n\}$, με τις σχέσεις να είναι λέξεις με γράμματα εκ των στοιχείων ${x_i}^{\pm 1}$.

Μελετώντας την επιλυσιμότητα του πιο πάνω προβλήματος, μπορούμε να αποφανθούμε θετικά εάν και μόνον καταλήξουμε στην ανάπτυξη αλγορίθμου που δεδομένου μιας λέξης w με γράμματα από το σύνολο των γεννητόρων, μπορεί να μας απαντήσει στο ερώτημα αν το $w = 1$ στο G. Θα πρέπει δηλαδή η προαναφερθείσα λέξη w να εμπεριέχεται στην παραγόμενη εκ του συνόλου R, κανονική υποομάδα, εντός της ελεύθερης ομάδας $S(X)$.

Είναι προφανές ότι πρόκειται για πρόβλημα απόφασης και κατά συνέπεια επιδέχεται δύο απαντήσεις, «ΝΑΙ» και «ΟΧΙ». Εάν έχουμε να κάνουμε με μια ομάδα που προκύπτει από μια αναδρομική παράσταση γεννητόρων και οριζουσών σχέσεων, τότε η απάντηση «ΝΑΙ» θα έχει αναδρομική επίλυση.

Εύλογα προκύπτει το συμπέρασμα ότι το πρόβλημα της λέξης δεν εξαρτάται από τις εκάστοτε παραστάσεις. Όμως για να είναι επιλύσιμο για κάποια ομάδα, θα πρέπει να είναι επιλύσιμο και για κάποια παράσταση της ομάδας αυτής.

Θεώρημα Ι.6
Έστω τώρα ότι παίρνουμε μια ομάδα G, και στη συνέχεια το σύνολο των γεννητόρων $X = \{x_1, \dots, x_n\}$ και το σύνολο των οριζουσών σχέσεων $R = \{r_1, \dots, r_n\}$. Θα ορίσουμε με $\langle X \mid R \rangle$ την αναδρομική παράσταση της ομάδας G. Τότε το σύνολο όλων των λέξεων $g \in G$, τέτοιων ώστε $g = 1$, είναι αναδρομικά αριθμήσιμο. □

Απόδειξη Ι.2
Μια πρώτη προσέγγιση μερικής απόδειξης του πιο πάνω προβλήματος λέξης, είναι και η εξής:

Έστω μια ομάδα G και μια αναδρομική της παράστασή $\langle X \mid R \rangle$.

Τότε θα ορίσουμε:

$$Q = \{\langle u, v\rangle : u \text{ και } v \text{ λέξεις στο } X \text{ και } u = v \text{ στην } G\}$$

Τότε έχουμε μια μερικώς αναδρομική συνάρτηση $f_{\langle X \mid R \rangle}$, τέτοια ώστε:

$$f_{\langle X \mid R \rangle}(\langle u, v\rangle) = \begin{cases} 0 & \text{αν } \langle u, v\rangle \in Q \\ \text{δεν ορίζεται / δεν κάνει παύση} & \text{αν } \langle u, v\rangle \notin Q \end{cases}$$

Οπότε για να επιλύσουμε το ζητούμενο πρόβλημα για την παράσταση $\langle X \mid R \rangle$, είναι αρκετό να κατασκευάσουμε μια αναδρομική συνάρτηση g τέτοια ώστε:

$$g(\langle u, v\rangle) = \begin{cases} 0 & \text{αν } \langle u, v\rangle \notin Q \\ \text{δεν ορίζεται / δεν κάνει παύση} & \text{αν } \langle u, v\rangle \in Q \end{cases}$$

Όμως, $u = v$ στην G, αν και μόνον αν $uv^{-1} = 1$ στην G. Κατά εύλογη συνέπεια προκύπτει ότι για να επιλύσουμε το πρόβλημα της λέξης για $\langle X \mid R \rangle$, είναι αρκετό να κατασκευάσουμε μια αναδρομική συνάρτηση h τέτοια ώστε:

$$h(x) = \begin{cases} 0 & \text{αν } x \neq 1 \text{ στο } G \\ \text{δεν ορίζεται / δεν κάνει παύση} & \text{αν } x = 1 \text{ στο } G \end{cases}$$

□

Το πρόβλημα αναζήτησης της λέξης (Πρόβλημα Αναζήτησης), προκύπτει όταν έχουμε μια αναδρομική παράσταση της ομάδας G κι ένα στοιχείο $g = 1$ στην G και πρέπει να βρούμε μια παράσταση του g ως γινόμενο συζεύξεων των οριζουσών σχέσεων και των αντιστρόφων τους.

Διαπιστώνουμε ότι μπορούμε να αριθμήσουμε αναδρομικώς όλα τα γινόμενα τον οριζουσών σχέσεων, των αντιστρόφων τους και των συζεύξεων. Κατά συνέπεια μπορούμε να πούμε ότι το πρόβλημα αναζήτησης της λέξης θα έχει πάντα κάποια αναδρομική λύση. Παρ' όλα αυτά, σε ένα τέτοιο γινόμενο, ο αριθμός των παραγόντων που απαιτείται για την αναπαράσταση μιας λέξης μήκους n, που είναι ίση με 1 στην G, μπορεί να είναι αρκετά μεγάλη συγκριτικά με το n. Για παράδειγμα, υπάρχουν ομάδες G με το πρόβλημα λέξης να επιλύεται αποδοτικά και λέξεις w μήκους n ίσο με 1 στην G, τέτοιες ώστε ο αριθμός των παραγόντων σε οποιαδήποτε παραγοντοποίηση της w σε γινόμενο των οριζουσών σχέσεων, των αντιστρόφων τους και των συζεύξεών τους να μην είναι φραγμένο εκθετικά στο n.

Επιπροσθέτως, εάν σε μια ομάδα G το πρόβλημα της λέξης είναι αναδρομικά μη επιλύσιμο, τότε το μήκος της απόδειξης που μας επιβεβαιώνει ότι

$w = 1$ στην G δεν είναι φραγμένο από κάποια αναδρομική συνάρτηση του μήκους της w.

Μέχρι στιγμής, έχουμε δει τρία αλγοριθμικά προβλήματα και παρακάτω παραθέτουμε κάποιες σχέσεις που γνωρίζουμε ότι υπάρχουν μεταξύ τους:

1. Εάν το πρόβλημα συζυγίας στο G είναι επιλύσιμο, τότε το πρόβλημα της λέξης είναι επίσης επιλύσιμο.

2. Εάν το πρόβλημα αναζήτησης της συζυγίας στο G είναι επιλύσιμο, τότε το πρόβλημα της διάσπασης είναι επιλύσιμο για μεταθετικές υποομάδες $A, B \leq G$, όπως $ab = ba$ για όλα τα $a \in A$, $b \in B$.

3. Εάν το πρόβλημα αναζήτησης της συζυγίας στο G είναι επιλύσιμο, τότε το πρόβλημα αναζήτησης της παραγοντοποίησης είναι επιλύσιμο για μεταθετικές υποομάδες $A, B \leq G$.

δ. Το πρόβλημα του μέλους

Το πρόβλημα του μέλους, αποτελεί μια άλλη κατηγορία προβλημάτων, λίγο διαφορετική από τα τρία προηγούμενα. Πιο συγκεκριμένα, το πρόβλημα ορίζεται ως εξής:

Ορισμός Ι.34
Εάν έχουμε μια αναδρομικώς παριστάμενη ομάδα G, μια υποομάδα $H \leq G$ παραγόμενη από τα $h_1, \dots, h_k$ κι ένα στοιχείο $g \in G$, θα πρέπει να βρούμε εάν $g \in H$. □

Ξανά έχουμε να κάνουμε με ένα πρόβλημα απόφασης και δύο πιθανές απαντήσεις, «ΝΑΙ» και «ΟΧΙ». Η θετική απόφανση είναι πάντα αναδρομική επειδή κάποιος μπορεί να αριθμήσει αναδρομικώς όλα τα στοιχεία μιας υποομάδας με πεπερασμένο σύνολο γεννητόρων.

Το πρόβλημα του μέλους είναι επίσης γνωστό και με ένα άλλο όνομα, λιγότερο περιγραφικό, ως το «γενικευμένο πρόβλημα της λέξης».

Φυσικά, κι αυτό το πρόβλημα μπορεί να εκφραστεί ως πρόβλημα αναζήτησης. Σε αυτήν την περίπτωση λέμε ότι έχουμε μια αναδρομικώς παριστάμενη ομάδα G, μια υποομάδα $H \leq G$ παραγόμενη από τα $h_1, \dots, h_k$ κι ένα στοιχείο $h \in G$ και θα πρέπει να βρούμε μια έκφραση (απόδοση) της h που να χρησιμοποιεί τα $h_1, \dots, h_k$.

ε. Το πρόβλημα του ισομορφισμού

Ορισμός Ι.35
Τέλος, θα θέλαμε να κάνουμε και μια απλή αναφορά σε ένα επιπλέον πρόβλημα, που είναι γνωστό ως το πρόβλημα του ισομορφισμού. Σε αυτό έχουμε δύο πεπερασμένα παριστάμενες ομάδες G_1 και G_2 και θέλουμε να βρούμε αν είναι ισόμορφες ή όχι. □

Εδώ μπορούμε να αναφέρουμε ότι η μέθοδος επίλυσης του Tietze μας παρέχει μια αναδρομική αρίθμηση όλων των πεπερασμένα παριστάμενων ομάδων που είναι ισόμορφες ως προς μια πεπερασμένα παριστάμενη ομάδα, κάτι που υποδηλώνει πως η θετική απόφανση του πιο πάνω προβλήματος είναι πάντα αναδρομική.

Όμως το πρόβλημα του ισομορφισμού και των προσεγγίσεών του, ξεφεύγουν από τα πλαίσια ενδιαφέροντος της παρούσας εργασίας και κατά συνέπεια δε θα γίνει κάποια περαιτέρω ανάπτυξη.

Ι.2
Στοιχεία Κρυπτογραφίας

Ι.2.1. Σύντομη Ιστορική Αναδρομή

Ετυμολογία

Η λέξη κρυπτογραφία προέρχεται από τις ελληνικές λέξεις «κρύπτω» και «γράφω». Η Κρυπτογραφία είναι η μελέτη των «κρυμμένων» κειμένων, ή αλλιώς μπορούμε να πούμε ότι είναι η επιστήμη της κρυπτογράφησης και αποκρυπτογράφησης κειμένου και μηνυμάτων.

Προέλευση

Ένα μεγάλο μέρος της παγκόσμιας κοινότητας πιστεύει ότι το παλαιότερο γνωστό κείμενο που φαίνεται να περιέχει σημαίνοντα στοιχεία κρυπτογραφίας είναι η παραλλαγή ενός κειμένου που χρονολογείται 4.000 χρόνια παλαιότερα, στην Αιγυπτιακή πόλη Menet Khufu. Πιο συγκεκριμένα, στον τάφο ενός εκ των ευγενών της εποχής, του Khnumhotep II, οι ιερογλυφικές επιγραφές βρέθηκαν εμπλουτισμένες με ένα σύνολο ασυνήθιστων συμβόλων που είχαν ως σκοπό να μπερδέψουν και κατά συνέπεια να αποκρύψουν το μήνυμα των επιγραφών.

Φωτογραφία Ι.2

Γύρω στο 5 π.Χ., οι Σπαρτιάτες που ήταν μια από τις πιο γνωστές πολεμικές κοινότητες και οι οποίοι φημίζονταν για τον λιτό τρόπο ζωής τους, τη γενναιότητά τους και τις πολεμικές τους δεξιοτεχνίες, φαίνεται να ανέπτυξαν

μια κρυπτογραφική συσκευή ικανή να στέλνει και να λαμβάνει κρυφά κείμενα. Η συσκευή αυτή, κυλινδρική στο σχήμα και ευρέως γνωστή με το όνομα Σκυτάλη, θα έπρεπε να βρισκόταν στην κατοχή και των δύο πλευρών, δηλαδή του αποστολέα αλλά και του παραλήπτη του μηνύματος. Για την προετοιμασία του μηνύματος, παίρνανε μια στενή λωρίδα περγαμηνής ή δέρματος, κάτι παραπλήσιο με τη σημερινή κόλλα χαρτί, και στη συνέχεια, αφού την τύλιγαν γύρω από τη σκυτάλη, έγραφαν το μήνυμα επάνω. Όταν το υλικό (περγαμηνή ή δέρμα) ξετυλίγονταν ώστε να μεταφερθεί στον παραλήπτη, έφερε επάνω του μια φαινομενικά ακατανόητη ακολουθία γραμμάτων. Προκειμένου κάποιος να διάβαζε το μήνυμα, θα έπρεπε εκ νέου να τυλίξει την περγαμηνή σε μια Σκυτάλη που θα έφερε ακριβώς την ίδια διάμετρο. Ο κώδικας που πρόκυπτε από το ξετύλιγμα του υλικού, ήταν ένας μέσο κρυπτογραφικής μεταφοράς, στο οποίο όλα τα γράμματα παραμένουν ακριβώς το ίδιο, απλά αλλάζει η σειρά τους. Μια τεχνική που εξακολουθεί να αποτελεί τη βάση και για αρκετές σύγχρονες δημοφιλείς μεθόδους.

Φωτογραφία Ι.3

Αυτό όμως που κυρίως διαφοροποιεί τις σύγχρονες δημοφιλείς τεχνικές κρυπτογράφησης είναι ο εμπλουτισμός τους και με δύο επιπλέον μεθόδους,

αυτήν της Πρόσθεσης κι αυτήν της Υποκατάστασης στοιχείων. Παρ' όλο που η πρώτη αναφορά σε κρυπτογραφία με υποκατάσταση στοιχείων γίνεται από τον Έλληνα συγγραφέα Πολύβιο, η πρώτη καταγεγραμμένη χρήση της είναι αυτή από τον Ιούλιο Καίσαρα. Όλα τα μηνύματα κρυπτογραφούνταν με την υποκατάσταση του κάθε γράμματος του κειμένου, με κάποιο που βρίσκεται ακριβώς 3 θέσεις δεξιότερα στο αλφάβητο, δηλαδή το Α γινόταν Δ, το Κ γινόταν Ν κτλ. Ακόμη δεν έχει απαντηθεί το ερώτημα γιατί επιλέχθηκε να είναι η 3η θέση εκ δεξιών κι όχι κάποια άλλη.

Σε ένα δοκίμιο που χρονολογείται από το 1466, ένα Ιταλός γνωστός με το όνομα Leon Battista Alberti, που κάποιες φορές αποκαλείτε κι ως ο «πατέρας της Δυτικής Κρυπτογραφίας», περιέγραψε την κατασκευή ενός δίσκου κρυπτογράφησης, κι έτσι θεμελίωσε την έννοια του «πολυαλφαβητικού» μοντέλου κρυπτογράφησης. Αν και αυτή του η κίνηση αποτελεί την πιο σημαντική εξέλιξη στον Τομέα της Κρυπτογραφίας για τα τελευταία τουλάχιστον 500 χρόνια, ποτέ του δεν προχώρησε στην υλοποίηση της. Η δόξα αυτή έμεινε για άλλους, με τον πιο γνωστό να είναι ο Γάλλος κρυπτογράφος Blaise de Vigenere, ο οποίος επινόησε ένα πρακτικό «πολυαλφαβητικό» σύστημα που φέρει το όνομά του και είναι γνωστό ως «Τετράγωνο Vigenere».

Blaise de Vigenere

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Φωτογραφία Ι.4

Εκείνη την εποχή, και για το σεβαστό χρονικό διάστημα που ακολούθησε, πίστευαν ότι η τεχνική αυτή ήταν απαραβίαστη. Όμως, αγνοούσαν την έλευση μιας μορφής επίθεσης που θα αναπτυσσόταν αργότερα και θα μπορούσε να σπάσει αυτήν την τεχνική κρυπτογράφησης. Η επίθεση αυτή έγινε γνωστή ως «Στατιστική Επίθεση».

Κλασσική Κρυπτογραφία

Η παλαιότερη γνωστή χρήση υποτυπώδους απόπειρας κρυπτογραφίας εντοπίζεται σε πρόχειρα ιερογλυφικά που βρέθηκαν σκαλισμένα σε μνημεία από την εποχή του Παλαιού Βασιλείου της Αιγύπτου (4.500 χρόνια πριν). Δε θεωρούνται όμως ως σοβαρό δείγμα κρυπτογραφικής εργασίας αλλά ως ένας τρόπος να δημιουργηθεί κάποια σύγχυση και να μπερδευτεί ο αναγνώστης.

Σε έναν ύστερο χρόνο, αποδίδονται κάποιοι πήλινοι πίνακες από τη Μεσοποταμία, στους οποίου έχει εντοπισθεί προσπάθεια απόκρυψης του περιεχομένου, που για την ακρίβεια είναι κάποιες συνταγές προφανώς εμπορικής αξίας. Αργότερα, κάποιοι Εβραίοι μελετητές έκαναν χρήση μιας απλής «μονοαλφαβητικής» μεθόδου κρυπτογράφησης με υποκατάσταση, όπως το γνωστό Σύστημα Atbash, που χρονολογείται γύρω στο 500-600 π.Χ.

Άλλες μορφές κρυπτογράφησης και συμβολισμού συναντώνται μέσα στις θρησκείες. Ένα χαρακτηριστικό παράδειγμα αποτελεί ο αριθμός «666», γνωστός κι ως ο αριθμός της Διαβόλου, ο οποίος ενδέχεται να έχει αλληγορική έννοια και να παραπέμπει σε κάτι άλλο που ήταν γνωστό κατά τους Ρωμαϊκούς Χρόνους, αλλά μπορούσε να ερμηνευτεί μόνον από τους μυημένους. Πιστεύεται ότι μπορεί να ήταν κι ο συμβολισμός για τον ίδιο τον Νέρωνα, Αυτοκράτορα της Ρώμης.

Στην Ινδία, η κρυπτογραφημένη μέθοδος επικοινωνίας ήταν ευρέως διαδεδομένη και συναντάται ακόμη και στο Kama Sutra, όπου δίνονται οδηγίες για το πώς οι εραστές μπορούν να επικοινωνούν κρυφά.

Μεσαιωνική Κρυπτογραφία

Το 800 μ.Χ., στην πρώτη σελίδα του χειρόγραφου του al-Kindi που σχετίζεται με την αποκρυπτογράφηση κρυπτογραφικών μηνυμάτων, περιλαμβάνονται οι πρώτες περιγραφές κάποιας μορφής κρυπτανάλυσης και στατιστικής επίθεσης. Προφανώς, το κίνητρο της απόπειρας ήταν θρησκευτικό και αποσκοπούσε στην ανάλυση του κειμένου του Κορανίου. Όμως, οδήγησε στην ανάπτυξη της στατιστικής επίθεσης για το σπάσιμο «μονοαλφαβητικών» αλγορίθμων κρυπτογράφησης με υποκατάσταση. Πρόκειται για την πιο σημαντική μορφή κρυπτανάλυσης πριν τον Β’ Παγκόσμιο Πόλεμο.

al-Kindi

Φωτογραφία Ι.5

Έτσι, όλα τα «μονοαλφαβητικά» συστήματα παρέμειναν ευάλωτα σε αυτήν την επίθεση, μέχρι που το 1465 ο Leone Battista Alberti (που είδαμε πιο πάνω), ανέπτυξε την ιδέα των «πολυαλφαβητικών» συστημάτων. Να σημειώσουμε ότι κάποιες τελευταίες ανακαλύψεις, προσδιορίζουν την πρώτη χρήση των γνωστών ως «πολυαλφαβητικών» συστημάτων, κάπου στον Αραβικό κόσμο, 500 χρόνια νωρίτερα από την αρχική εκτίμηση. Πιο συγκεκριμένα, φαίνεται να έχει γίνει αναφορά από τον μαθηματικό al-Kindi σε κάποιες πρωταρχικές μορφές «πολυαλφαβητικών» συστημάτων. Και γενικότερα παρατηρούμε την εποχή αυτήν μια έξαρση από τους Άραβες επιστήμονες, οι οποίοι δώσανε αρκετή γνώση και ευρηματικότητα τόσο στα μοντέλα κρυπτογράφησης, όσο και στην κρυπτανάλυση. Άλλα γνωστά ονόματα της εποχής ήταν οι Ahmad al-Qalqashandi (1355-1418), Taj ad-Din Ali ibn ad-Duraihim ben Muhammad ath-Tha ‘alibi al-Mausili (1312-1362).

Στον Ευρωπαϊκό χώρο, η κρυπτογραφία απέκτησε ιδιάζουσα σημασία, ως αποτέλεσμα του πολιτικού ανταγωνισμού και της θρησκευτικής επανάστασης. Πριν και μετά την Αναγέννηση, πολίτες από τις διάφορες πολιτείες της Ιταλίας, προσπαθούσαν να σπάσουν τα διάφορα κρυπτογραφικά μοντέλα που αναπτύσσονταν τότε για την μετάδοση μιας πληροφορίας. Αυτό οδήγησε στην συνεχή ανάπτυξη «πολυαλφαβητικών» μοντέλων, που φαίνονταν να ήταν σύντομα σε ζωή.

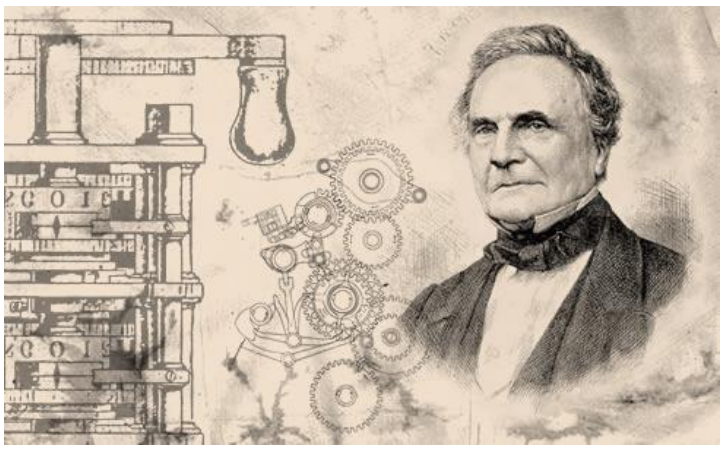
Εκτός Ευρωπαϊκού χώρου, μετά το τέλος της Χρυσής Εποχής των Μουσουλμάνων, όταν αυτοί πέρασαν υπό την κυριαρχία των Μογγόλων, η Κρυπτογραφία έπαψε να αναπτύσσεται. Στην Ιαπωνία εν αντιθέτου, παρουσιάζεται η Κρυπτογραφία για πρώτη φορά το 1510, ενώ οι πιο αναπτυγμένες τεχνικές εμφανίστηκαν μετά το άνοιγμα της χώρας στον Δυτικό Πολιτισμό, δηλαδή στις αρχές του 1860. Το 1920, οι Πολωνοί ναυτικοί

βοήθησαν τους Ιάπωνες αξιωματούχους στην ανάπτυξη κάποιου κώδικα και μιας υποτυπώδους κρυπτογράφησης.

Η Κρυπτογραφία από το 1800 ως τον 'Β Παγκόσμιο Πόλεμο

Τον 19ο αιώνα, οι κρυπτογράφοι σταμάτησαν να φτιάχνουν κρυπτογραφικά μοντέλα με συγκεκριμένη χρηστικότητα και θέλησαν να κάνουν κάτι πιο ευρύ. Τέτοια παραδείγματα μας έρχονται από έγγραφα όπως ο Πόλεμο της Κριμαίας (Charles Babbage), από κείμενα του Auguste Kerckhoff, του Edgar Allan Poe, κτλ. Ο τελευταίος έγραψε κι ένα δοκίμιο σχετικά με τις μεθόδους κρυπτογράφησης που φάνηκε χρήσιμο ως εισαγωγικό εγχειρίδιο για τους Βρετανούς κρυπταναλυτές, που προσπαθούσαν να σπάσουν τους Γερμανικούς κώδικες και τα κρυπτογραφημένα μηνύματα κατά τη διάρκεια του Α΄ Παγκοσμίου Πολέμου.

Το 1854 ο Charles Babbage ανέπτυξε τη μέθοδο της στατιστικής ανάλυσης με την οποία κατάφερε να αποκρυπτογραφήσει επιτυχώς μηνύματα που είχαν κρυπτογραφηθεί με το τετράγωνο Vigenere. Δυστυχώς όμως, το έργο του έγινε γνωστό κατά τη διάρκεια του 20ου αιώνα, είτε γιατί ο Babbage ποτέ δεν ολοκλήρωνε τα έργα του, είτε γιατί δεν ήθελε να διαρρεύσει η μέθοδός του και να δώσει έτσι στους Βρεττανούς τη δυνατότητα να σπάσουν τα μηνύματα που στέλνοντας στην Κριμαία. Έτσι ο φόρος τιμής για την Στατιστική Επίθεση και το Σπάσιμο του τετραγώνου Vigenere δόθηκε στον Πρώσο Kasiski το 1863 και η μέθοδος του έγινε γνωστή ως το «Τεστ Kasiski».



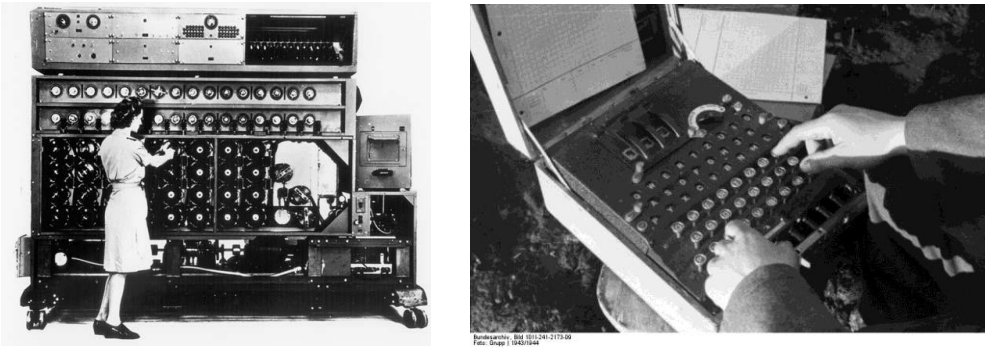
Charles Babbage

Φωτογραφία Ι.6

Το 1917 ο Gilbert Vernam πρότεινε έναν τηλέτυπο τρόπο κρυπτογράφησης.

Κατά τη διάρκεια του Β' Παγκοσμίου Πολέμου, η μηχανή Enigma της Ναζιστικής Γερμανίας αλλά και η κρυπτανάλυσή της από τις Συμμαχικές

Δυνάμεις, μονοπώλησε το ενδιαφέρον της εποχής. Σε γενικές γραμμές όμως, η ανάπτυξη κρυπτογραφικών μοντέλων και συστημάτων κρυπτανάλυσης ήταν κεντρικό σημείο και των δύο πλευρών κατά τη διάρκεια του Πολέμου.



Μηχανή Enigma

Φωτογραφία Ι.7

Οι Γερμανοί έκαναν εκτενή χρήση υπό διαφορετικές μορφές, μιας ηλεκτρομηχανολογικής μηχανής, γνωστή ως Enigma. Ο Μαθηματικός Marian Rejewski κατάφερε να μειώσει την πολυπλοκότητα στη δομή της Enigma, τον Δεκέμβριο του 1932. Για να το πετύχει αυτό έκανε χρήση μαθηματικών μοντέλων και ένα περιορισμένο υλικό που του πρόσφερε ο Gustave Bertrand των Γαλλικών μυστικών υπηρεσιών. Επρόκειτο για τη μεγαλύτερη επιτυχία των τελευταίων χιλίων χρόνων στην κρυπτογραφία.

Marian Rejewski

Φωτογραφία Ι.8

Όμως, όταν τον Σεπτέμβριο του 1939 ξέσπασε ο Β' Παγκόσμιος Πόλεμος και οι Σοβιετικοί εισήρθαν στην Πολωνία, όλη η επιστημονική ομάδα που ήταν υπεύθυνη για την ανάλυση της Enigma φυγαδεύτηκε στην Ρουμανία κι από κει στο Παρίσι και στη συνέχεια συνεργάστηκαν με την αντίστοιχη ομάδα κρυπταναλυτών που είχε συστηθεί στη Βρετανία από Μαθηματικούς και

Σκακιστές. Ξεχωρίζουν τα ονόματα των Gordon Welchman, Max Newman και Alan Turing, του Πατέρα της Πληροφορικής, οι οποίοι σταδιακά ανέπτυξαν κι άλλο την τεχνολογία κρυπτανάλυσης και τελικά κατάφεραν να σπάσουν εντελώς την Enigma.

Alan Turing


Gordon Welchman


Max Newman

Φωτογραφία Ι.9

Αντίστοιχες επιθέσεις συνεχίστηκαν κι απέναντι σε άλλα κρυπτογραφικά εργαλεία όπως αυτά των Ιαπώνων. Την ίδια στιγμή, οι συμμαχικές δυνάμεις είχαν αναπτύξει τα δικά τους κρυπτογραφικά μοντέλα, με πρωτοπόρο την Αμερική.

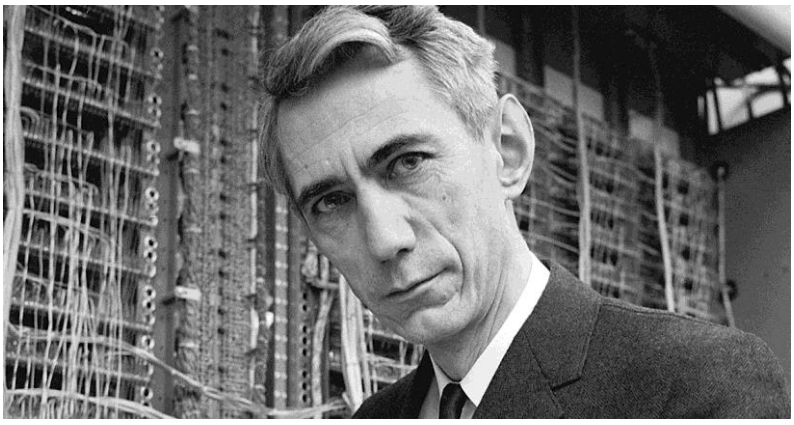
Ι.2.2. Σύγχρονη Κρυπτογραφία

Γενικά Χαρακτηριστικά

Μέχρι το 1970, η ασφαλής κρυπτογραφία ήταν αντικείμενο ενδιαφέροντος μόνον για τους κυβερνητικούς μηχανισμούς. Έκτοτε, δύο σημεία σταθμοί ήταν αυτά που οδήγησαν την κρυπτογραφία να είναι αναγκαία και προσιτή στο ευρύ κοινό:

- Η κατασκευή δημόσιων κρυπτογραφικών προτύπων (DES) και
- Η εφεύρεση της Κρυπτογραφίας Δημόσιου Κλειδιού.

Η ακμή της μοντέρνας κρυπτογραφίας εντοπίζεται την εποχή του Claude Shannon, γνωστού κι ως ο «πατέρας» της μαθηματικής κρυπτογραφίας. Ο Shannon, είναι ιδιαίτερα γνωστός για το έργο του πάνω στην ασφάλεια των επικοινωνιών, κατά την περίοδο του Β' Παγκοσμίου Πολέμου. Το 1949, εκδίδει το έργο «Communication Theory of Secrecy Systems» στο Bell System Technical Journal και λίγο αργότερα, μαζί με τον Warren Weaver, το βιβλίο «Mathematical Theory of Communication». Και τα δύο του έργα, περιλαμβάνουν μέρος της δουλειάς που είχε αναπτύξει κατά τον Β' Παγκόσμιο Πόλεμο. Επιπροσθέτως, μαζί με την εργασία του πάνω στη θεωρία της πληροφορίας και της επικοινωνίας, κατάφερε να θεμελιώσει μια στέρεη θεωρητική βάση για την κρυπτογραφία και την κρυπτανάλυση. Μπορούμε να πούμε ότι εκείνη την περίοδο, η κρυπτογραφία μονοπωλούσε το ενδιαφέρον των μυστικών κυβερνητικών οργανώσεων όπως οι NSA, GCHQ κα. Από τότε και μέχρι τα μέσα του 1970 που άλλαξαν τα πάντα, πολύ λίγα πράγματα έχουν γνωστοποιηθεί.



Claude Shannon

Φωτογραφία Ι.10

Στις σύγχρονες πλέον μορφές της, η Κρυπτογραφία αντλεί στοιχειώδη εργαλεία από τα Μαθηματικά και κυρίως από τους τομείς της Στατιστικής, των Πιθανοτήτων, της Συνδυαστικής, της Θεωρίας Αριθμών, των Διακριτών Μαθηματικών, της Λογικής και Υπολογιστικής Πολυπλοκότητας, της Θεωρίας Καμπυλών, της Θεωρίας Ομάδων κα.

Κάθε κρυπτογραφικό μοντέλο θα πρέπει να χαρακτηρίζεται από τέσσερα βασικά στοιχεία:

1. Την Ακεραιότητα των δεδομένων, δηλαδή η πληροφορία προς μετάδοση να μη δεχθεί αλλοιώσεις.

2. Την Εμπιστευτικότητα, δηλαδή την απόκρυψη της μεταδιδόμενης πληροφορίας από εκείνους που δεν πρέπει να τη λάβουν/διαβάσουν (που δεν έχουν εξουσιοδότηση).

3. Την Πιστοποίηση μερών, δηλαδή την ταυτοποίηση ενός προσώπου, μηχανήματος κτλ. που συμμετέχει σε μια αντίστοιχη περίπτωση ανταλλαγής κρυπτογραφημένης πληροφορίας.

4. Την Επικύρωση της Προέλευσης, δηλαδή την ταυτοποίηση και δέσμευση του αποστολέα του κρυπτογραφημένου μηνύματος.

Ένα κρυπτογραφικό πρότυπο

Στα μέσα του 1970, είχαμε δύο σημαντικές εξελίξεις που είδαν το φως της δημοσιότητας. Η πρώτη αφορούσε την έκδοση του προσχέδιου με το όνομα Data Encryption Standard στις Η.Π.Α., στις 17 Μαρτίου 1975. Το προτεινόμενο πρότυπο (γνωστό κι ως DES) πρωτοπαρουσιάστηκε από μια ερευνητική ομάδα της IBM, ύστερα από πρόσκληση του Εθνικού Φορέα Προτύπων (πλέον NIST). Ο στόχος ήταν η ανάπτυξη υποδομών ασφαλούς ηλεκτρονικής επικοινωνίας για φορείς όπως οι τράπεζες και οι υπόλοιπες μεγάλες οικονομικές οργανώσεις. Το 1977, με την καθοδήγηση της NSA που λειτουργούσε παρασκηνιακά, και τη σχετική τροποποίηση που ακολούθησε, το πρότυπο υιοθετήθηκε και δημοσιεύθηκε ως Federal Information Processing Standard Publication (πλέον FIPS 46-3). Το πρότυπο DES αποτελεί και το πρώτο κρυπτογραφικό μοντέλο που έπαιξε τόσο σημαντικό ρόλο στην NSA. Στη συνέχεια, η δημοσιοποίηση των προδιαγραφών του από την NBS οδήγησε σε μια έκρηξη ενδιαφέροντος για την κρυπτογραφία, εκ μέρους της δημόσιας και ακαδημαϊκής κοινότητας.

Στη συνέχεια, το 2001, όταν το DES είχε πλέον παλαιώσει, αντικαταστάθηκε και επίσημα από το πρότυπο Advanced Encryption Standard (AES). Ύστερα από έναν ανοιχτό διαγωνισμό που ακολούθησε, η NIST επέλεξε το Rijndael να αποτελέσει το AES. Παρ' όλα αυτά, το DES και διάφορες ασφαλείς παραλλαγές του (όπως το τριπλό DES), εξακολουθούν να χρησιμοποιούνται μέχρι και σήμερα, όντας μέρος πολλών εθνικών και θεσμικών προτύπων. Θα πρέπει εδώ να σημειωθεί ότι το 56-bit κλειδί του DES, είναι ευάλωτο σε brute force επιθέσεις. Μια τέτοια επίθεση κατάφερε να σπάσει ένα πρότυπο DES σε 56 ώρες. Ως αποτέλεσμα, η χρήση του DES αποφεύγεται πλέον στα νέα κρυπτογραφικά μοντέλα που αναπτύσσονται. Όμως, όλα τα μηνύματα που είχαν κρυπτογραφηθεί με το DES, από το 1976 και ύστερα, διατρέχουν τον κίνδυνο της αποκρυπτογράφησης. Επιπλέον, πιστεύεται ότι οι κυβερνητικές αρχές είχαν την υπολογιστική ισχύ να σπάσουν τον DES πολύ νωρίτερα από ότι γνωρίζουμε.

Μοντέρνα Κρυπτανάλυση

Η ανάπτυξη της κρυπτογραφίας έγινε παράλληλα με την αντίστοιχη ανάπτυξη της κρυπτανάλυσης, δηλαδή του σπασίματος των κωδίκων και κρυφών μηνυμάτων. Η ανακάλυψη και εφαρμογή της στατιστικής μελέτης στα κρυπτογραφικά μοντέλα επικοινωνίας, άλλαξαν τη ροή της ιστορίας. Έτσι είχαμε την πρόκληση από την Zimmermann Telegramm να ενταχθούν οι Η.Π.Α. στον Α' Παγκόσμιο Πόλεμο αλλά και να καταφέρουν οι Συμμαχικές Δυνάμεις να διαβάσουν τα κρυπτογραφημένα μηνύματα της Ναζιστικής Γερμανίας κατά τη διάρκεια του Β' Παγκοσμίου Πολέμου, μειώνοντας τη διάρκεια του κατά δύο χρόνια (σύμφωνα με κάποιες εκτιμήσεις).

Μερικά αξιοσημείωτα παραδείγματα σπασμένων κρυπτογραφικών μοντέλων είναι το DES, το πρώτο είδος κρυπτογραφικού μοντέλου για Wi-Fi (WEP), το Content Scrambling System που χρησιμοποιήθηκε για την κρυπτογράφηση και τη διαχείριση των DVD, τα A5/1 και A5/2 μοντέλα που χρησιμοποιήθηκαν στα GSM κινητά τηλέφωνα, το μοντέλο CRYPTO1 που χρησιμοποιήθηκε ευρέως σε διάφορες έξυπνες κάρτες, κα. Όμως όλα τα πιο πάνω είμαι συμμετρικά μοντέλα. Μέχρι στιγμής, καμία μαθηματική προτυποποίηση που έχει χρησιμοποιηθεί στην κρυπτογραφία δημοσίου κλειδιού δεν έχει αποδειχθεί να είναι «ανίκητη» και κατά συνέπεια, μια πιθανή μελλοντική πρόοδο σε κάποια μαθηματικά μοντέλα ενδέχεται να καταστήσει και πολλά άλλα συστήματα να θεωρούνται ευάλωτα. Αν και το τελευταίο είναι κάτι που προς το παρόν λίγοι θεωρούν πιθανό, η ασφάλεια των κρυπτογραφικών μοντέλων δημοσίου κλειδιού συνεχώς αυξάνει το μέγεθος του κλειδιού, επειδή η τεχνολογία γίνεται όλο και φθηνότερη με αποτέλεσμα ο καθένας να μπορεί να την

αγοράσει και κατά συνέπεια να γίνει απειλητικός με το να καταφέρει κάποιο ανεπιθύμητο «σπάσιμο».

Το 1996 σημειώθηκε και προτάθηκε για πρώτη φορά κάποια πρόοδο στη χρήση κβαντικών υπολογιστών που βασίζεται στα NTRUEncrypt πλέγματα. Τυποποιήθηκε το 2008, με το Πρότυπο IEEE 1363.1. Όπως όλα δείχνουν, ίσως αυτό να είναι και το πρότυπο του μέλλοντος, μόλις το RSA και η Κρυπτογραφία Ελλειπτικών Καμπυλών θα πρέπει να αποσυρθούν ως μη αξιόπιστα. Οι παραλληλισμοί και η ιδέα των τεχνικών κβαντικής κρυπτογραφίας στηρίχτηκε στην τεράστια υπολογιστική και έντονη θερμοδυναμική μοντελοποίηση όπως αυτή εκφράζεται στο βιβλίο του George G Szpiro.

Ι.2.3. Κρυπτογραφία Δημόσιου Κλειδιού

Συστήματα Δημόσιου Κλειδιού

Το 1976, η δεύτερη πρόοδος που ακολούθησε, ήταν ίσως και η πιο σημαντική. Ήταν αυτή που άλλαξε τον τρόπο λειτουργίας των κρυπτοσυστημάτων. Η πρόοδος αυτή σημειώθηκε με τη δημοσίευση του paper «New Directions in Cryptography» από τους Whitfield Diffie και Martin Hellman. Όπως θα δούμε πιο κάτω, αργότερα αποδόθηκαν εύσημα και στον Ralph Merkle. Στην ουσία, μας εισήγαγε σε έναν τελείως διαφορετικό τρόπο διαμοιρασμού των δημοσίων κλειδιών και κατάφερε να λύσει ένα από τα θεμελιώδη προβλήματα της κρυπτογραφίας, αυτό της ανταλλαγής κλειδιών. Η προαναφερθείσα μέθοδος είναι γνωστή ως Μέθοδος Ανταλλαγής Κλειδιών Diffie-Hellman. Στη συνέχεια οδηγηθήκαμε στην ανάπτυξη μιας καινούριας κατηγορίας αλγορίθμων, γνωστών και ως αλγόριθμοι ασύμμετρου κλειδιού.

Από αριστερά: Ralph Merkle, Martin Hellman και Whitfield Diffie (1977)

Φωτογραφία Ι.11

Whitfield Diffie & Martin Hellman

Whitfield Diffie & Martin Hellman & Ralph Merkle

Φωτογραφία Ι.12

Μέχρι τότε, όλοι οι σύγχρονοι κρυπτογραφικοί αλγόριθμοι χρησιμοποιούσαν συμμετρικά κλειδιά, δηλαδή τόσο ο αποστολέας όσο κι ο παραλήπτης είχαν ακριβώς το ίδιο κρυπτογραφικό κλειδί που έπρεπε να κρατάνε μυστικό και στη συνέχεια χρησιμοποιούσαν τους απαραίτητους αλγορίθμους επικοινωνίας. Η λογική αυτή είχε εφαρμοστεί σε όλα τα κρυπτογραφικά μοντέλα πριν τα ασύμμετρα κλειδιά, συμπεριλαμβανομένου την Αρχαιότητα, το Μεσαίωνα και τον Β' Παγκόσμιο Πόλεμο.

Στη μέθοδο που αναφέραμε πιο πάνω, πριν προχωρήσουμε στην ανταλλαγή της οποιαδήποτε πληροφορίας, θα πρέπει οι δύο πλευρές να ανταλλάξουν το σχετικό κλειδί μέσω της ασφάλειας ενός προστατευμένου καναλιού. Μπορεί να φαντάζει ως μια απλή διαδικασία, όμως επιφέρει αρκετές δυσκολίες όπως όταν ο αριθμός των μερών που επικοινωνούν συνεχώς αυξάνεται, όπως όταν πλέον έχουν εξαντληθεί όλα τα διαθέσιμα ασφαλή κανάλια επικοινωνίας ή όταν για λόγους διατήρησης του επιπέδου ασφαλείας, πρέπει να προβούμε σε αλλαγές και αντικατάσταση των κλειδιών που χρησιμοποιούμε. Είναι προφανές ότι αν επιθυμούμε κάθε μήνυμα να είναι καλά φυλαγμένο από τρίτους, τότε θα χρειαζόμαστε ένα κλειδί για κάθε πιθανό ζεύγος χρηστών. Το όλο σύστημα που αναλύουμε χρησιμοποιεί ένα κρυφό κλειδί και είναι ευρέως γνωστό με το όνομα «Κρυπτοσύστημα Συμμετρικού Κλειδιού».

Η μέθοδος ανταλλαγής κλειδιών των Diffie-Hellman, (κι όλες οι βελτιώσεις και παραλλαγές που ακολούθησαν) έκαναν τη χρήση όλων αυτών των συστημάτων πολύ ευκολότερη και σαφέστατα πολύ ασφαλέστερη από εκείνη που η ανθρωπότητα είχε συνηθίσει καθ' όλη τη διάρκεια της ιστορίας της.

Αντιθέτως με τα πιο πάνω, η κρυπτογραφία ασύμμετρου κλειδιού χρησιμοποιεί ένα ζεύγος κλειδιών που συσχετίζονται στη βάση των μαθηματικών και το κάθε ένα αποκρυπτογραφεί την κρυπτογράφηση που έκανε το άλλο. Μερικοί μάλιστα από τους σχετικούς αλγορίθμους έχουν την ιδιότητα να προστατεύουν το ζεύγος κλειδιών κι έτσι να είναι αδύνατο να προσδιοριστεί το ένα κλειδί, εάν γνωρίζουμε το δεύτερο, παρά μόνον αν κάνουμε όλες τις δυνατές προσπάθειες μέχρι να το βρούμε. Ένας τέτοιος αλγόριθμος είναι γνωστός ως σύστημα δημοσίου ή ασύμμετρου κλειδιού.

Χρησιμοποιώντας έναν τέτοιο αλγόριθμο, χρειαζόμαστε μόνον ένα ζεύγος κλειδιών ανά χρήστη. Τότε θα ονομάσουμε το ένα από τα δύο κλειδιά ως ιδιωτικό (που παραμένει πάντα κρυφό) και το άλλο ως δημόσιο (που συχνά είναι ευρέως διαθέσιμο) και στη συνέχεια η ανταλλαγή μπορεί να γίνει χωρίς της ανάγκη κάποιου ασφαλούς καναλιού. Έτσι, όσο διατηρούμε το ιδιωτικό κλειδί κρυφό, το δημόσιο κλειδί μπορεί να δημοσιοποιείται ελεύθερα χωρίς να διακυβεύεται η ασφάλεια, δίνοντάς μας τη δυνατότητα να χρησιμοποιούμε το ζεύγος τους απείρως.

Στην περίπτωση που έχουμε δύο χρήστες που προσπαθούν να επικοινωνήσουνε με αλγόριθμο ασύμμετρου κλειδιού μέσω ενός μη ασφαλούς καναλιού, τότε ο καθένας τους θα πρέπει να γνωρίζει το ιδιωτικό και δημόσιο κλειδί του καθώς και το δημόσιο κλειδί του άλλου. Έχουμε συναντήσει πολλές φορές το βασικό σενάριο επικοινωνίας που θα μπορούσε να είναι όπως το ακόλουθο:

- Η Alice κι ο Bob έχουν ένα ζεύγος κλειδιών που το χρησιμοποιούν εδώ και χρόνια με αρκετούς άλλους χρήστες.
- Στην αρχή, ανταλλάσσουν τα δημόσια κλειδιά τους, χωρίς κάποια κρυπτογράφηση, μέσω ενός μη ασφαλούς καναλιού.
- Στη συνέχεια η Alice κρυπτογραφεί ένα μήνυμα χρησιμοποιώντας το ιδιωτικό της κλειδί και στη συνέχεια το παίρνει το αποτέλεσμα και το κρυπτογραφεί και πάλι χρησιμοποιώντας το δημόσιο κλειδί του Bob. Το διπλο-κρυπτογραφημένο μήνυμα μεταδίδεται ψηφιακά από την Alice στον Bob μέσω ενός μη ασφαλούς καναλιού.
- Ο Bob λαμβάνει την ψηφιακή ακολουθία και την αποκρυπτογραφεί χρησιμοποιώντας το ιδιωτικό του κλειδί και στη συνέχεια, αυτό που θα πάρει το αποκρυπτογραφεί χρησιμοποιώντας το δημόσιο κλειδί της Alice.
- Εάν το τελικό αποτέλεσμα που θα πάρει μπορεί να γίνει αποδεκτό ως μήνυμα, τότε κι ο Bob μπορεί να είναι σίγουρος ότι το μήνυμα που έλαβε είναι σίγουρα από κάποιον που γνωρίζει το ιδιωτικό κλειδί της Alice και είναι προφανές ότι για να υποκλέψει ένας τρίτος το μήνυμα θα έπρεπε να γνωρίζει το ιδιωτικό κλειδί του Bob.

Οι ασύμμετροι αλγόριθμοι στηρίζουν την φερεγγυότητά τους σε μια κλάση μαθηματικών προβλημάτων που είναι γνωστά κι ως συναρτήσεις μιας κατεύθυνσης και τα οποία απαιτούν αμελητέα υπολογιστική ισχύ να εκτελεστούν προς τη μια κατεύθυνση αλλά απίστευτα μεγάλη υπολογιστική ισχύ για να έχουμε την αντιστροφή τους. Μάλιστα, σε αρκετές περιπτώσεις, αυτό δεν είναι καθόλου εφικτό. Ένα κλασσικό παράδειγμα συνάρτησης μια κατεύθυνσης είναι ο πολλαπλασιασμός πολύ μεγάλων πρώτων αριθμών. Είναι εφικτό να πολλαπλασιάσουμε σχετικά εύκολα δύο πολύ μεγάλους πρώτους αριθμούς, αλλά πρακτικά αδύνατο να βρούμε τους δύο πρώτους αριθμούς από το γινόμενό τους. Λόγω του μαθηματικού υπόβαθρου των συναρτήσεων μιας κατεύθυνσης, τα περισσότερα πιθανά κλειδιά θα πρέπει να τα απορρίπτουμε ως κακές επιλογές. Μόνον ένα μικρό τμήμα των πιθανών κλειδιών, δεδομένου μήκους, είναι κατάλληλα για να χρησιμοποιηθούν. Κατά συνέπεια οι ασύμμετροι αλγόριθμοι απαιτούν κλειδιά πολύ μεγάλου μήκους ώστε να επιφέρουν την ίδια ασφάλεια που οι συμμετρικοί αλγόριθμοι εξασφαλίζουν με κλειδιά πολύ μικρότερου μήκους. Η ανάγκη δημιουργίας των ζευγών από κλειδιά και η διαδικασία κρυπτογράφησης και

αποκρυπτογράφησης καθιστούν τους ασύμμετρους αλγόριθμους να έχουν μεγαλύτερο υπολογιστικό κόστος έναντι των περισσότερων συμμετρικών αλγορίθμων. Οι συμμετρικοί αλγόριθμοι μπορούν συχνά να χρησιμοποιούν ένα εύρος ψηφίων ενός κλειδιού. Αυτό μας δίνει τη δυνατότητα να παράγουμε πολύ γρήγορα πρόχειρα κλειδιά που να έχουν μια σύντομη χρηστική αξία. Κατά συνέπεια, είναι συνηθισμένη πρακτική να χρησιμοποιούμε ένα μεγάλο ασύμμετρο κλειδί για να ανταλλάξουμε ένα διαθέσιμο αλλά αρκετά πιο μικρό (χωρίς να στερούμαστε σε ασφάλεια) συμμετρικό κλειδί. Έτσι, έχουμε ως αποτέλεσμα τον αργό ασύμμετρο αλγόριθμο να στέλνει με ασφάλεια ένα συμμετρικό κλειδί και στη συνέχεια ο κατά πολύ πιο γρήγορος συμμετρικός αλγόριθμος να συνεχίσει τις όποιες διεργασίες πάνω στο μήνυμα.

Η Κρυπτογραφία Ασύμμετρου Κλειδιού, η Ανταλλαγή Κλειδιών Diffie-Hellman και οι καλύτεροι γνωστοί αλγόριθμοι δημόσιου/ιδιωτικού κλειδιού (όπως ο πολύ γνωστός αλγόριθμος RSA που θα δούμε παρακάτω), φαίνεται να είχαν αναπτυχθεί σε ανεξάρτητη βάση από τις μυστικές υπηρεσίες της Μεγάλης Βρετανίας, πριν από τη δημόσια κοινοποίηση που έγινε από τους Diffie και Hellman το 1976. Στελέχη της GCHQ έχουν δημοσιοποιήσει έγγραφα με τα οποία ισχυρίζονται ότι είχαν αναπτύξει την κρυπτογραφία δημοσίου κλειδιού, πριν από τη σχετική δημοσίευση του paper των Diffie και Hellman. Πολλά ήταν τα απόρρητα έγγραφα (papers) που είχαν συνταχθεί στην GCHQ τις δεκαετίες 1960 και 1970 και οδήγησαν σε συστήματα παρόμοια με το RSA και την Ανταλλαγή Κλειδιών των Diffie και Hellman (1973 και 1974). Μερικά από αυτά έχουν πλέον δημοσιευθεί και οι εμπνευστές τους (James H. Ellis, Clifford Cocks και Malcolm Williamson) φρόντισαν να γνωστοποιηθούν μόνον επίλεκτα σημεία του έργου τους.

Ας δούμε όμως λίγο πιο αναλυτικά το πώς δουλεύει η λογική της κρυπτογραφίας δημοσίου κλειδιού. Όπως είπαμε, ένα από τα πιο σημαντικά στοιχεία της κρυπτογραφίας δημοσίου κλειδιού είναι η αδυναμία μας να αντιστρέψουμε τις συναρτήσεις μιας κατεύθυνσης. Για παράδειγμα, στο Κρυπτοσύστημα RSA, ενώ δεν είναι δύσκολο να υπολογίσουμε το γινόμενο δύο μεγάλων πρώτων αριθμών, είναι σχεδόν αδύνατο να βρούμε ποιοι είναι οι δύο μεγάλοι πρώτοι αριθμοί με παραγοντοποίηση του γινομένου τους. Ένα άλλο, ακόμη πιο προφανές παράδειγμα της αδυναμίας μας αντιστρέψουμε τέτοιες συναρτήσεις είναι αυτό της συνάρτησης $f(x) = x^2$. Όπως βλέπουμε είναι σχετικά εύκολο να υπολογίσουμε το τετράγωνο στην περίπτωση αρκετών (ημί)ομάδων, ενώ δεν είναι τόσο εύκολο όταν καλούμαστε να υπολογίσουμε μια ρίζα, έστω τη $\sqrt{x}$. Η παρατήρηση αυτή αξιοποιείται στο Κρυπτοσύστημα του Rabin με την πολλαπλασιαστική ημιομάδα των $\mathbb{Z}_n$ με το n να είναι σύνθετος.

Κρυπτογραφία εγκατάστασης κλειδιού

Για να καταλάβουμε λίγο τη μέθοδο που θέλουμε να αναδείξουμε, θα πάρουμε και πάλι το αγαπημένο και ευρέως γνωστό μας ζευγάρι, δηλαδή την Alice και το Bob.

Έτσι, έστω ότι η Alice και ο Bob μοιράζονται μεταξύ τους ένα κρυφό κλειδί K, το οποίο είναι ένα στοιχείο του συνόλου S.

Έστω τώρα μια δημόσια συνάρτηση $H : S \longrightarrow \{0,1\}^n$ από το σύνολο S στο σύνολο των δυαδικών ακολουθιών μήκους n. Είναι λογικό να θέλουμε να έχουμε το n αρκετά μεγάλο, ας πούμε $\log_2|S|$, αν το S είναι πεπερασμένο ή οτιδήποτε μπορεί να σηκώσει η υπολογιστική μας ισχύ, αν το S είναι άπειρο. Μια τέτοια συνάρτηση είναι επίσης γνωστή και με το όνομα hash function (συνάρτηση κατακερματισμού). Σε άλλες περιπτώσεις, οι συναρτήσεις hash χρησιμοποιούνται ως συμπαγείς παραστάσεις ή ψηφιακά ίχνη των δεδομένων έτσι ώστε να εξασφαλίσουν την ακεραιότητα του μηνύματος.

Ας δούμε τώρα λίγο πως θα γίνει η κρυπτογράφηση και η αποκρυπτογράφηση:

Κρυπτογράφηση:

Ο Bob κρυπτογραφεί το μήνυμα του, έστω $m \in \{0,1\}^n$, ως

$$E(m) = m \oplus H(K)$$

με το $\oplus$ να είναι η πρόσθεση με modulo 2.

Αποκρυπτογράφηση:

Η Alice υπολογίζει:

$$(m \oplus H(K)) \oplus H(K) = m \oplus (H(K) \oplus H(K)) = m,$$

Κι έτσι μπορεί να πάρει το μήνυμα m.

Η μέθοδος που είδαμε πιο πάνω έχει παράγοντα επέκτασης ίσο με 1, κάτι που εύλογα μας λέει ότι το κρυπτογραφημένο μήνυμα έχει το ίδιο μήκος με το αρχικό μήνυμα. Όμως για να είμαστε σίγουροι για την ασφάλεια, θα πρέπει να αυξήσουμε τον παράγοντα επέκτασης σε μεγάλο βαθμό, κάτι που σίγουρα θα αυξήσει τον όγκο της πληροφορίας και θα απαιτήσει μεγαλύτερη υπολογιστική ισχύ, αλλά έτσι είμαστε σίγουροι για το αποτέλεσμα.

Ι.2.4. Πρωτόκολλα Κρυπτογραφίας

α. Κρυπτοσύστημα Diffie-Hellman-Merkle

Είναι πραγματικά σπάνιο ένα νέο πεδίο της επιστήμης να ξεκινάει από ένα και μόνον ένα συγκεκριμένο paper. Μια τέτοια περίπτωση είναι και η κρυπτογραφία δημοσίου κλειδιού που ξεκίνησε με ένα εμπνευσμένο paper το 1976 και μας επέτρεψε για πρώτη φορά στα χρονικά, να ανταλλάξουμε κάτι κρυφό σε δημόσιο ανοιχτό κανάλι. Το 2002, ο Martin Hellman αφιέρωσε μέρος της επιτυχίας και στον Merkle, κάνοντας μια δημόσια παραδοχή στην οποία ούτε λίγο, ούτε πολύ, παραδέχθηκε ότι ναι μεν το όλο σύστημα περιεγράφηκε για πρώτη φορά σε paper από τον ίδιο και τον Diffie, αλλά η όλη ιδέα για τη διανομή των δημόσιων κλειδιών ήταν εμπνευσμένη από τον Merkle και γι' αυτό ζήτησε να ονομαστεί το σύστημα ως ανταλλαγή κλειδιών Diffie-Hellman-Merkle. Με την προσπάθειά του αυτή, ήθελε να αναγνωριστεί και η προσπάθεια του Merkle στο όλο εγχείρημα της ανακάλυψης της κρυπτογραφίας δημοσίου κλειδιού.

Πρωτόκολλο Ι.1
Για να δούμε πως λειτουργεί το σύστημα των Diffie-Hellman-Merkle, θα πάρουμε την αρχική και πιο απλή εφαρμογή του πρωτοκόλλου που χρησιμοποιεί την πολλαπλασιαστική ομάδα των ακεραίων modulo p, όπου p είναι πρώτος και g είναι πρωταρχική ρίζα $mod\ p$, δηλαδή για κάθε ακέραιο x, που είναι σχετικά πρώτος με τον p, υπάρχει s τέτοιο ώστε $g^s \equiv xmodp$.

Μια ακόμη πιο γενική εκδοχή του πρωτοκόλλου χρησιμοποιεί μια τυχαία πεπερασμένη κυκλική ομάδα.

Όταν θα τρέξουμε τον σχετικό αλγόριθμο, θα λάβουν τόπο τα πιο κάτω βήματα:

1. Η Alice και ο Bob συμφωνούν σε μια πεπερασμένη κυκλική ομάδα G και ένα στοιχείο γεννήτορα, το g στο G. Θα γράψουμε την ομάδα G ως πολλαπλασιαστική ομάδα.
2. Η Alice επιλέγει έναν τυχαίο φυσικό αριθμό x και στέλνει στον Bob το g^x.
3. Ο Bob επιλέγει ένα τυχαίο φυσικό αριθμό y και στέλνει στην Alice το g^y.
4. Η Alice θα υπολογίσει το $K_A = (g^y)^x = g^{yx}$.
5. Ο Bob θα υπολογίσει το $K_B = (g^x)^y = g^{xy}$.

Επειδή όμως το $\mathbb{Z}$ είναι μεταθετικό, θα ισχύει $xy = yx$ και κατά συνέπεια η Alice και ο Bob θα έχουν στην κατοχή τους, από την ίδια ομάδα, το στοιχείο $K = K_A = K_B$ που μπορεί να χρησιμοποιηθεί και ως κρυφό κλειδί. □

Εάν τα G και g επιλεχθούν σωστά, τότε το πρωτόκολλο μπορεί να θεωρηθεί ως ασφαλές απέναντι σε κακόβουλες προσπάθειες. Κι όντως, εάν κάποιος τρίτος επιθυμεί να βρει το κοινό κρυφό κλειδί, θα πρέπει να λύσει το πρόβλημα των Diffie-Hellman, δηλαδή να βρει το g^{xy} από τα g^x και g^y. Όμως αυτό θα είναι ιδιαίτερα δύσκολο εάν επιλέξουμε τις σωστές παραμέτρους από την αρχή.

Στο Πρόβλημα του Διακριτού Λογαρίθμου προσπαθούμε να βρούμε το x από τα g και g^x. Εάν βρούμε κάποιον αλγόριθμο που να το επιλύει, τότε προφανώς θα μπορούμε να λύσουμε και το Πρόβλημα των Diffie-Hellman. Τότε όμως πολλά κρυπτοσυστήματα δημοσίου κλειδιού θα γίνονταν αυτόματα επισφαλή προς χρήση. Παρ' όλα αυτά, δεν έχει αποδειχθεί αν το Πρόβλημα του Διακριτού Λογαρίθμου είναι ή δεν είναι ισοδύναμο προς το Πρόβλημα των Diffie-Hellman.

Θα πρέπει να επισημάνουμε ότι υπάρχει μια brute force επίθεση η οποία και μπορεί να λύσει το πρόβλημα του διακριτού λογαρίθμου. Αυτό μπορεί να το κάνει κάποιος άμα ξεκινήσει από το 1 και συνεχίσει να ανεβαίνει κατά ένα στοιχείο μέχρι να φτάσει το n, δοκιμάζοντας όλα τα πιθανά g^n μέχρι να βρει ποιο είναι αυτό που αναζητεί. Όμως, για να το κάνει αυτό χρειάζονται $O(|g|)$ πολλαπλασιασμοί, όπου με $|g|$ συμβολίζουμε το βαθμό του g. Όμως στις συνήθεις περιπτώσεις, το $|g|$ είναι περίπου της τάξεως του 10^{300} και κατά συνέπεια η πιο πάνω επίθεση είναι υπολογιστικά ανέφικτη και μη αποτελεσματική.

Σε αυτό το σημείο, ίσως να δημιουργείται η πεποίθηση ότι το ίδιο πρόβλημα των $O(|g|)$ πολλαπλασιασμών θα πρέπει να αντιμετωπισθεί κι από τις δύο πλευρές που ανταλλάσσουν το μήνυμα. Όμως στην περίπτωση τους, μπορούν να χρησιμοποιήσουν τον αλγόριθμο της «τετραγωνοποίησης και του πολλαπλασιασμού», ο οποίος είναι πολύ πιο γρήγορος και θα τους υπολογίσει το g^x για ένα συγκεκριμένο x, βασιζόμενος στον πολλαπλασιασμό τετραγώνων. Δηλαδή, με αυτόν τον τρόπο για g^{22} θα έχουμε:

$$g^{22} = (((g^2)^2)^2)^2 \cdot (g^2)^2 \cdot g^2$$

Κατά συνέπεια, για να υπολογίσει κάποιος το g^x θα χρειαστεί $O(\log_2 \chi)$ πολλαπλασιασμούς, κάτι που είναι πρακτικά εφικτό.

β. Κρυπτοσύστημα El-Gamal

Το Κρυπτοσύστημα El-Gamal (Taher El-Gamal) είναι ένα κρυπτοσύστημα δημοσίου κλειδιού που βασίζεται στις ίδιες αρχές με αυτό των Diffie-Hellman-Merkle. Το πρωτόκολλο αυτό χρησιμοποιείται στο ελεύθερο λογισμικό GNU Privacy Guard, στις τελευταίες εκδόσεις του PGP και σε διάφορα άλλα κρυπτοσυστήματα. Να επισημάνουμε σε αυτό το σημείο ότι ο Αλγόριθμος Ψηφιακής Υπογραφής μοιάζει πολύ και είναι μια παραλλαγή της μεθόδου Υπογραφών του El-Gamal. Όμως δε θα πρέπει να τα συγχέουμε μεταξύ τους. Άλλωστε πιο κάτω θα αναλύσουμε ξεχωριστά και περαιτέρω τον Αλγόριθμο Ψηφιακής Υπογραφής.

Taher El-Gamal

Φωτογραφία Ι.13

Ας δούμε τώρα τα βήματα που ακολουθούνται στο Κρυπτοσύστημα El-Gamal:

Πρωτόκολλο Ι.2

Στο σύστημα αυτό, τρία είναι τα βασικά του στοιχεία, η δημιουργία των κλειδιών, ο αλγόριθμος κρυπτογράφησης και στη συνέχεια ακολουθεί ο αλγόριθμος αποκρυπτογράφησης.

Δημιουργία Κλειδιών:

Για να δημιουργήσουμε τα κλειδιά, ακολουθούμε τα εξής:

- Η Alice θα πρέπει να μας δώσει μια ικανή περιγραφή μιας κυκλικής ομάδας G της τάξεως q με έναν γεννήτορα g.
- Η Alice θα επιλέξει τυχαία ένα x από $\{1, \dots, q-1\}$.
- Η Alice θα υπολογίσει το $h := g^x$
- Η Alice θα δημοσιεύσει το h, μαζί με την περιγραφή των G, q, g ως το δημόσιο κλειδί της. Όμως η Alice θα κρατήσει το x ως το ιδιωτικό της κλειδί, το οποίο και θα πρέπει να μείνει κρυφό.

Κρυπτογράφηση:

Ο αλγόριθμος κρυπτογράφησης θα πρέπει να κρυπτογραφήσει ένα μήνυμα m για την Alice χρησιμοποιώντας το δημόσιο κλειδί της (G, q, g, h). Έτσι:

- Ο Bob θα επιλέξει ένα τυχαίο y από $\{1, \dots, q-1\}$ και θα υπολογίσει το $c_1 := g^y$.
- Ο Bob θα υπολογίσει το $s := h^y$.
- Ο Bob θα αντιστοιχήσει το μήνυμα του m σε ένα στοιχείο m' του G.
- Ο Bob θα υπολογίσει το $c_2 := m' \cdot s$.
- Ο Bob θα στείλει στην Alice το $(c_1, c_2) = (g^y, m' \cdot h^y) = (g^y, m' \cdot (g^x)^y)$

Εδώ θα πρέπει να επισημάνουμε ότι κάποιος μπορεί εύκολα να βρει το h^y αν γνωρίζει το m'. Για τον λόγο αυτό θα πρέπει να δημιουργούμε ένα νέο y για κάθε μήνυμα έτσι ώστε να βελτιώσουμε την ασφάλεια. Οπότε και το y θα είναι ένα εφήμερο κλειδί.

Αποκρυπτογράφηση:

Ο αλγόριθμος αποκρυπτογράφησης θα αποκρυπτογραφήσει το προστατευμένο κείμενο (c_1, c_2) κάνοντας χρήση του ιδιωτικού κλειδιού της Alice. Έτσι:

- Η Alice θα υπολογίσει το $s := {c_1}^x$
- Η Alice θα υπολογίσει το $m' := c_2 \cdot s^{-1}$, από το οποίο στη συνέχεια θα επαναφέρει το απλό κείμενο m, με το s^{-1} να είναι το αντίστροφο του s στην ομάδα G.

Ολοκληρώνοντας, ο πιο πάνω αλγόριθμος αποκρυπτογράφησης θα μας δώσει το ζητούμενο κείμενο, καθότι:

$$c_2 \cdot s^{-1} = m' \cdot h^y \cdot (g^{xy})^{-1} = m' \cdot g^{xy} \cdot g^{-xy} = m'$$

□

Συνήθως, το κρυπτοσύστημα El-Gamal χρησιμοποιείται σε υβριδικά κρυπτοσυστήματα, δηλαδή όταν το μήνυμα είναι κρυπτογραφημένο με ένα συμμετρικό κρυπτοσύστημα και στη συνέχεια χρησιμοποιούμε το El-Gamal ώστε να κρυπτογραφήσουμε το κλειδί του συμμετρικού κρυπτοσυστήματος. Ο λόγος είναι ότι τα ασύμμετρα κρυπτοσυστήματα όπως το El-Gamal είναι συνήθως πιο αργά από τα αντίστοιχα συμμετρικά για να έχουμε το ίδιο επίπεδο ασφάλειας. Οπότε είναι πιο αποδοτικό να κρυπτογραφήσουμε το μήνυμα με ένα συμμετρικό τρόπο και στη συνέχεια το συμμετρικό κλειδί με τη μέθοδο El-Gamal.

γ. DSA (Digital Signature Algorithm)

Η Πιστοποίηση είναι η διαδικασία κατά την οποία θέλουμε να επαληθεύσουμε την ψηφιακή ταυτότητα του αποστολέα της επικοινωνίας. Στην κρυπτογραφία δημοσίου κλειδιού, ιδιαίτερο ενδιαφέρον παρουσιάζουν οι αποδείξεις μηδενικής γνώσης. Αυτό σημαίνει ότι αν η ταυτοποίηση είναι σωστή, κανείς δε μπορεί να μάθει κάτι παραπάνω, εκτός από αυτήν την πληροφορία. Γι' αυτό η μια πλευρά (αυτός που προσπαθεί να αποδείξει) θέλει να αποδείξει την ταυτότητά του στην άλλη πλευρά (αυτόν που κάνει την επαλήθευση) μέσω κάποιας μυστικής πληροφορίας/επικοινωνίας (ιδιωτικό κλειδί), αλλά δε θέλει κανείς να μάθει τίποτα για το μυστικό αυτό.

Αρκετά πρωτόκολλα εγκατάστασης κλειδιού μπορούν να παραλλαχθούν ελαφρώς έτσι ώστε να γίνουν πρωτόκολλα πιστοποίησης. Αυτό μπορούμε να το δούμε να γίνεται και στο παράδειγμα του πρωτοκόλλου εγκατάστασης κλειδιού Diffie-Hellman. Έτσι:

Πρωτόκολλο Ι.3
Έστω ότι η Alice είναι αυτή που προσπαθεί να αποδείξει κι ο Bob αυτός που προσπαθεί να επαληθεύσει. Δηλαδή η Alice θέλει να πείσει τον Bob ότι γνωρίζει ένα μυστικό, χωρίς να αποκαλύψει το ίδιο το μυστικό.

Τα βήματα που θα ακολουθηθούν έχουν ως εξής:

- Η Alice θα δημοσιεύσει μια πεπερασμένη κυκλική ομάδα G κι έναν γεννήτορα g στη G. Στη συνέχεια θα επιλέξει έναν τυχαίο φυσικό αριθμό x και θα δημοσιεύσει το g^x.
- Ο Bob θα επιλέξει έναν τυχαίο φυσικό αριθμό y και θα στείλει το g^y ως πρόσκληση στην Alice.
- Η Alice θα απαντήσει με μια απόδειξη $P = (g^y)^x = g^{yx}$.
- Ο Bob θα επαληθεύσει εάν $(g^x)^y = P$.

Όπως είναι προφανές, το πρωτόκολλο αυτό είναι μια παραλλαγή της ανταλλαγής κλειδιών Diffie-Hellman. □

Από τα πιο πάνω, είναι προφανές ότι έχουμε την ανάγκη να αναπτύξουμε έναν Αλγόριθμο Ψηφιακής Υπογραφής (DSA). Ας δούμε λίγο πιο αναλυτικά τι είναι αυτό.

Ο Αλγόριθμος Ψηφιακής Υπογραφής (DSA) είναι ένα Ομοσπονδιακό Πρότυπο για την Επεξεργασία της Πληροφορίας των ψηφιακών υπογραφών. Είχε προταθεί αρχικά από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των Η.Π.Α. (NIST) τον Αύγουστο του 1991 για να χρησιμοποιούνταν στο δικό τους

Πρότυπο Ψηφιακής Υπογραφής (DSS). Στη συνέχεια υιοθετήθηκε ως FIPS 186 το 1993. Έκτοτε, ακολούθησαν τέσσερεις τροποποιημένες εκδόσεις.

Ο DSA προστατεύεται με πατέντα από το 1991 και έχει κατοχυρωθεί στον David W. Kravitz, έναν πρώην υπάλληλο της Υπηρεσίας Εθνικής Ασφάλειας των Η.Π.Α. Ο DSA αποτελεί μια παραλλαγή του Συστήματος Υπογραφών του El-Gamal.

Πρωτόκολλο Ι.4
Ας δούμε όμως πως λειτουργεί το όλο σύστημα.

Δημιουργία Κλειδιού

Η δημιουργία ενός κλειδιού μπορεί να διακριθεί σε δύο φάσεις. Η πρώτη φάση περιλαμβάνει την επιλογή των αλγοριθμικών παραμέτρων που μπορεί να έχουν διαμοιραστεί ανάμεσα στους διάφορους χρήστες του συστήματος. Ενώ η δεύτερη φάση υπολογίζει τα δημόσια και ιδιωτικά κλειδιά για έναν χρήστη.

Επιλογή αλγοριθμικών παραμέτρων:

- Θα επιλέξουμε μια αποδεκτή κρυπτογραφική συνάρτηση κατακερματισμού (hash). Στην αυθεντική μορφή του DSS, η συνάρτηση ήταν πάντα η $SHA-1$. Όμως στο τρέχον, σύγχρονο DSS, χρησιμοποιούμε τις πιο δυνατές συναρτήσεις $SHA-2$. Να επισημάνουμε εδώ ότι η έξοδος μια συνάρτησης κατακερματισμού μπορεί να περιοριστεί στο μέγεθος τους ζεύγους κλειδιών.
- Θα αποφασίσουμε για το μήκος των κλειδιών, έστω L και N. Πρόκειται για την πρωταρχική μορφή μέτρησης της κρυπτογραφικής δύναμης ενός κλειδιού. Το N θα πρέπει να είναι ίσο ή μικρότερο από το μήκος της εξόδου της συνάρτησης κατακερματισμού.
- Θα επιλέξουμε έναν $N-bit$ πρώτο q.
- Θα επιλέξουμε έναν $L-bit$ πρώτο modulus p, τέτοιο ώστε $p-1$ να είναι πολλαπλάσιο του q.
- Θα επιλέξουμε έναν g, δηλαδή ένα νούμερο του οποίου η πολλαπλασιαστική τάξη modulo p είναι q. Αυτό μπορούμε να το πετύχουμε με το να θέσουμε $g = h^{(p-1)/q} mod p$ για κάποιο τυχαίο h $(1 < h < p-1)$. Εάν το αποτέλεσμα βγει 1, τότε θα προσπαθήσουμε εκ νέου με κάποιο διαφορετικό h. Συχνά χρησιμοποιούμε το $h = 2$.

Οι πιο πάνω αλγοριθμικοί παράμετροι (p, q, g) μπορούν να διαμοιραστούν και να κοινοποιηθούν ανάμεσα στους διάφορους χρήστες του συστήματος.

Τα κλειδιά ανά χρήστη:

Εάν έχουμε το σύνολο των παραμέτρων, η δεύτερη φάση υπολογίζει τα ιδιωτικά και δημόσια κλειδιά του κάθε χρήστη. Έτσι:

- Θα επιλέξουμε με κάποια τυχαιότητα ένα μυστικό κλειδί x, όπου $0 < x < q$.
- Θα υπολογίσουμε το δημόσιο κλειδί $y = g^x mod p$.

Υπάρχουν αποτελεσματικοί αλγόριθμοι που μπορούν να υπολογίσουν τις σχέσεις $h^{(p-1)/q} mod p$ και $g^x mod p$.

Υπογραφή

Έστω H η συνάρτηση κατακερματισμού και m ένα μήνυμα. Τότε:

- Θα παράγουμε μια τυχαία τιμή k, όπου $0 < k < q$ για κάθε μήνυμα.
- Θα υπολογίσουμε $r = (g^k mod p) mod q$.
- Εάν είμαστε τόσο άτυχοι κι έχουμε $r = 0$, θα πρέπει να ξεκινήσουμε εκ νέου με ένα διαφορετικό τυχαίο k.
- Θα υπολογίσουμε $s = k^{-1}(H(m) + xr) mod q$
- Εάν είμαστε τόσο άτυχοι κι έχουμε $s = 0$, θα πρέπει να ξεκινήσουμε εκ νέου με ένα διαφορετικό τυχαίο k.
- Η υπογραφή είναι (r, s).

Με τα δύο πρώτα βήματα μπορούμε να φτιάξουμε ένα κλειδί για κάθε μήνυμα. Η εκθετοποίηση και η αντιστροφή $k^{-1} mod q$ θεωρούνται ως πράξεις που υπολογιστικά καταναλώνουν αρκετά και γι' αυτό μπορούν να υπολογιστούν πριν μάθουμε τη συνάρτηση κατακερματισμού του μηνύματος.

Επαλήθευση

- Θα απορρίψουμε την υπογραφή αν οι συνθήκες $0 < r < q$ ή $0 < s < q$ δεν ικανοποιούνται.
- Θα υπολογίσουμε $w = s^{-1} mod q$
- Θα υπολογίσουμε $u_1 = H(m) \cdot w \; mod q$
- Θα υπολογίσουμε $u_2 = r \cdot w \; mod q$
- Θα υπολογίσουμε $v = (g^{u_1} y^{u_2} mod \; p) \; mod \; q$
- Η υπογραφή δεν είναι αποδεκτή, εκτός κι αν $v = r$.

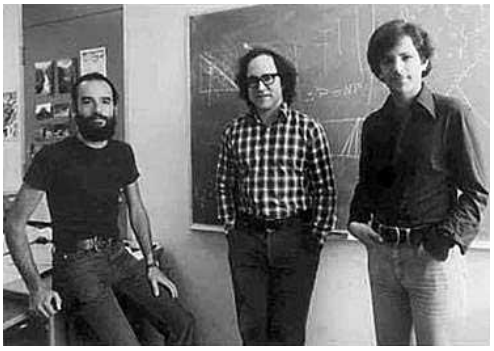
Το πιο πάνω σύστημα που περιγράψαμε είναι σωστό, με την έννοια ότι ο επαληθευτής θα αποδέχεται πάντα αυθεντικές υπογραφές. □

δ. Κρυπτοσύστημα RSA

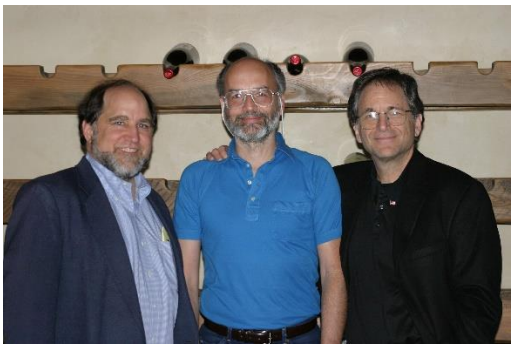
Το Κρυπτοσύστημα RSA είναι κι αυτό ένας αλγόριθμος ασύμμετρου κλειδιού, με εμπνευστές τους Ron Rivest, Adi Shamir και Len Adleman. Έχει διπλή χρήση καθότι μπορεί να κωδικοποιήσει μηνύματα αλλά και να χρησιμοποιηθεί ως ψηφιακή υπογραφή.

Από αριστερά: Ronald Rivest, Adi Shamir, Leonard Adleman

Φωτογραφία Ι.14



Adi Shamir, Ronald Rivest, Leonard Adleman



Ronald Rivest, Adi Shamir, Leonard Adleman

Φωτογραφία Ι.15

Κι αυτός με τη σειρά του βασίζεται στην υπολογιστική μας αδυναμία να παραγοντοποιήσουμε μεγάλους αριθμούς της τάξης των 1024-2048 bits). Όπως και στους προηγούμενους αλγόριθμους, έτσι κι εδώ χρησιμοποιούνται δύο κλειδιά. Ένα το οποίο είναι δημόσιο κι άλλο ένα που είναι ιδιωτικό για την κάθε πλευρά που επικοινωνεί.

Πρωτόκολλο Ι.5

Η ίδια λογική ακολουθείται και στην περίπτωση του RSA κι έτσι έχουμε τη Δημιουργία των κλειδιών, την Κρυπτογράφηση και τέλος την Αποκρυπτογράφηση.

Ας τα δούμε όμως λίγο επί μέρους και πιο αναλυτικά:

Δημιουργία των κλειδιών

- Θα επιλέξουμε δύο τυχαίους μεγάλους πρώτους αριθμούς p και q έτσι ώστε $p \neq q$.
- Στη συνέχεια θα υπολογίσουμε το $n = p \cdot q$.
- Μετά θα υπολογίσουμε τη συνάρτηση του Euler που είναι: $\varphi(n) = (p-1)(q-1)$.
- Θα επιλέξουμε έναν αριθμό $e > 1$ έτσι ώστε $e^{\varphi(n)} \equiv 1(mod n)$.
- Θα υπολογίσουμε τον αριθμό d έτσι ώστε $d \equiv e^{-1}(mod\ \varphi(n))$.

Για να βρούμε τους πρώτους αριθμούς θα χρησιμοποιήσουμε πιθανολογικούς αλγορίθμους, δηλαδή θα δώσουμε μια πρότερη γνώση πιθανότητας σε μια τρέχουσα παρατήρηση.

Συνήθως για το e επιλέγουμε το $3, 7$ και $2^{16} + 1$. Αν θέλουμε να έχουμε ταχύτερους υπολογισμούς, μπορούμε να χρησιμοποιήσουμε μικρότερους αριθμούς. Τότε όμως θα στερηθούμε σε ασφάλεια.

Τα κλειδιά που προκύπτουν από τα πιο πάνω βήματα θα είναι:

- Δημόσιο Κλειδί: (n, e)
- Ιδιωτικό Κλειδί: (n, d)

Έτσι μπορούμε να δημοσιεύσουμε το πρώτο κλειδί, το δημόσιο, και πλέον ο καθένας θα μπορεί να κρυπτογραφεί μηνύματα και να μας τα στέλνει. Άλλωστε μόνον εμείς θα μπορούμε να τα αποκρυπτογραφούμε χρησιμοποιώντας το ιδιωτικό μας κλειδί.

Κρυπτογράφηση

Στην κρυπτογράφηση μπορούμε να έχουμε την αναπαράσταση του μηνύματος σε δεκαεξαδική μορφή ASCII και στην συνέχεια την κρυπτογράφησή του. Έτσι, αν πάρουμε το μήνυμα “RSA” και θέλουμε να το δούμε στην ASCII μορφή, αυτό θα γίνει:

- $R \longmapsto 0x52$
- $S \longmapsto 0x53$
- $A \longmapsto 0x41$

Άρα παίρνουμε: $m \coloneqq RSA \longmapsto 0x525341$

Τώρα το κρυπτογραφημένο μήνυμα c του πιο πάνω μηνύματος m, θα είναι:

$$c = m^e \ mod \ n$$

Αποκρυπτογράφηση

Μόλις το κρυπτογραφημένο μήνυμα c ληφθεί, ακολουθούμε τα πιο κάτω βήματα έτσι ώστε να υπολογίσουμε το αρχικό μήνυμα m:

- $m = c^d \ mod \ n \equiv (m^e)^d \ mod \ n \equiv m^{e \cdot d} \ mod \ n$
- Όμως γνωρίζουμε πως $e \cdot d \equiv 1 (mod \ p-1)$ και $e \cdot d \equiv 1 (mod \ q-1)$ και με το μικρό θεώρημα του Fermat θα έχουμε:

$$m^{e \cdot d} \equiv m^1 \equiv m \ mod \ p-1 \text{ και } m^{e \cdot d} \equiv m^1 \equiv m \ mod \ q-1$$

- Οι αριθμοί p και q είναι πρώτοι μεταξύ τους και από το Κινέζικο Θεώρημα Υπολοίπων θα πάρουμε:

$$m^{e \cdot d} \equiv m \ mod \ n$$

□

Τέλος, αν θέλουμε να χρησιμοποιούμε τον RSA για την ψηφιακή υπογραφή μηνυμάτων, δηλαδή να αποστείλουμε ένα υπογεγραμμένο μήνυμα, θα χρησιμοποιήσουμε το ιδιωτικό κλειδί (n, d) και θα ακολουθήσουμε την εξής λογική:

$$s = m^d \ mod \ n$$

Ο παραλήπτης μας, λαμβάνει το μήνυμα m και την υπογραφή s και θα υπολογίσει την τιμή s^e χάρη στο δημόσιο κλειδί (n, e) και στη συνέχεια θα τη συγκρίνει με το m. Όμως αυτή την επιλογή δεν την χρησιμοποιούμε συχνά για λόγους ασφάλειας. Όπως είδαμε και πιο πάνω, χρησιμοποιείται μια hash function H (συνάρτηση κατακερματισμού) και τότε θα έχουμε:

$$s = H(m)^d \ mod \ n$$

Τώρα και πάλι ο παραλήπτης θα πράξει τα ίδια, θα πρέπει όμως να γνωρίζει τη συνάρτηση κατακερματισμού.

Αν και ο πιο πάνω αλγόριθμος γενικά θεωρείται ασφαλής αν και εφόσον χρησιμοποιήσουμε πολύ μεγάλες παραμέτρους, δεν ισχύει το ίδιο με κακή του χρήση, οπότε και εγείρονται θέματα ασφαλείας. Επιπροσθέτως, κανείς δεν

έχει αποδείξει ότι η ασφάλεια του εξαρτάται αποκλειστικά από την αδυναμία ως προς την παραγοντοποίηση των ακεραίων.

Μια γνωστή επίθεση στον RSA είναι η Επίθεση Επαναληπτικής Κρυπτογράφησης όπου αν έχουμε στην κατοχή μας το κρυπτογραφημένο μήνυμα και το δημόσιο κλειδί με το οποίο κρυπτογραφήθηκε, τότε μπορούμε να κρυπτογραφούμε το ήδη κρυπτογραφημένο μήνυμα με το δημόσιο κλειδί. Στη συνέχεια επαναλαμβάνουμε τη διαδικασία κρυπτογράφησης του αποτελέσματος μέχρι να πάρουμε κείμενο ίδιο με το πρώτο κρυπτογραφημένο μήνυμα. Τότε και η αμέσως προηγούμενη κρυπτογράφησης θα περιέχει το αποκρυπτογραφημένο μήνυμα.

Ενώ δύο γνωστά σφάλματα που μπορεί να οδηγήσουν σε μειωμένη ασφάλεια είναι:

- Αν πάρουμε κοινό n, δηλαδή αν έχουμε στην κατοχή μας δύο κλειδιά του τύπου (n, e_1) και (n, e_2) και δύο κρυπτογραφήσεις (c_1, c_2) του ιδίου μηνύματος m με τα κλειδιά αυτά, δηλαδή:

  $$c_1 = m^{e_1} mod n \text{ και } c_2 = m^{e_2} mod n$$

  Τότε μπορούμε να βρούμε το αρχικό μήνυμα m χωρίς να έχουμε πρόσβαση στα κρυφά κλειδιά. Επειδή είναι πολύ πιθανόν να έχουμε:

  $$e_1 \wedge e_2 = 1$$

  Τότε από το θεώρημα του Bézout θα έχουμε:

  $$\exists (u, v), e_1 \cdot u + e_2 \cdot v = 1$$

  Οπότε το αρχικό μήνυμα m θα το βρούμε υπολογίζοντας:

  $$(c_1)^u \cdot (c_2)^v \equiv (m^{e_1})^u \cdot (m^{e_2})^v \equiv m^{e_1 \cdot u + e_2 \cdot v} \equiv m^1 \equiv m \; mod \; n$$

- Αν πάρουμε μικρό e, π.χ. $e = 3$.

  Τότε ένα μήνυμα m θα κρυπτογραφηθεί και θα αποσταλεί από τρεις διαφορετικούς χρήστες με χρήση των δημοσίων κλειδιών $(n_1, 3)$, $(n_2, 3)$ και $(n_3, 3)$. Άρα κάποιος τρίτος θα μπορεί να έχει στην κατοχή του τα:

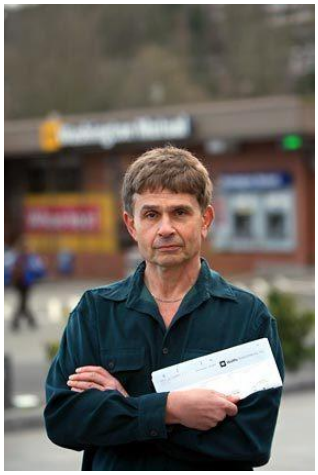
- $m^3 \ mod \ n_1$
- $m^3 \ mod \ n_2$
- $m^3 \ mod \ n_3$

Οπότε κι από το Κινέζικο Θεώρημα Υπολοίπων θα μπορούμε να βρούμε εύκολα το αρχικό μήνυμα m:

$$m^3 \ mod \ n_1 \cdot n_2 \cdot n_3$$

ε. Τεχνικές Ελλειπτικών Καμπυλών

Ιστορικά, η χρήση των ελλειπτικών καμπυλών αποδίδεται στους Neal Koblitz και Victor S. Miller ξεχωριστά, το 1985. Ενώ το 2004-2005, η χρήση των κρυπτογραφικών αλγορίθμων ελλειπτικών καμπυλών έγινε ευρεία.



Neal Koblitz

Victor S. Miller

Φωτογραφία Ι.16

Η Κρυπτογραφία που στηρίζεται στις Ελλειπτικές Καμπύλες προσεγγίζει την κρυπτογραφία δημοσίου κλειδιού βασισμένη στην αλγεβρική δομή των ελλειπτικών καμπυλών πάνω σε πεπερασμένα πεδία. Η Τεχνική αυτή, που για λόγους συντομίας θα τη συμβολίζουμε ΚΕΚ, χρειάζεται μικρότερα κλειδιά σε σύγκριση με άλλες κρυπτογραφίες, όπως αυτές που βασίζονται σε απλά πεδία Galois ώστε να μας εξασφαλίσουν το ίδιο επίπεδο ασφαλείας.

Οι ελλειπτικές καμπύλες εφαρμόζονται στην κρυπτογραφία, στις ψηφιακές υπογραφές, στις ψευδο-τυχαίες γεννήτριες και σε διάφορες άλλες περιπτώσεις. Χρησιμοποιούνται επίσης και σε αρκετούς αλγορίθμους παραγοντοποίησης ακεραίων, που έχουν εφαρμογή στην κρυπτογραφία, σαν την παραγοντοποίηση ελλειπτικών καμπυλών Lenstra.

Η κρυπτογραφία δημοσίου κλειδιού βασίζεται στην αδυναμία επιλυσιμότητας συγκεκριμένων μαθηματικών προβλημάτων. Στα πρωτόκολλα ελλειπτικών καμπυλών θεωρούμε ότι είναι πολύ δύσκολο να επιλύσουμε τον διακριτό λογάριθμο για ένα στοιχείο μιας τυχαίας ελλειπτικής καμπύλης, όταν ένα σημείο βάσης είναι γνωστό. Το πρόβλημα αυτό είναι γνωστό κι ως το Πρόβλημα Διακριτού Λογαρίθμου των Ελλειπτικών Καμπυλών (ΠΔΛΕΚ). Η ασφάλεια της Κρυπτογραφίας Ελλειπτικών Καμπυλών εξασφαλίζεται από τη δυνατότητα που έχουμε να υπολογίσουμε ένα σημείο πολλαπλασιασμού και

την αδυναμία να υπολογίσουμε το στοιχείο που πολλαπλασιάζεται αν μας δίνονται τα αρχικά και παραγόμενα σημεία. Το μέγεθος της ελλειπτικής καμπύλης προσδιορίζει και το βαθμό δυσκολίας του προβλήματος. Το προφανές όφελος από τη χρήση της ΚΕΚ είναι τα μικρότερα κλειδιά που θα χρησιμοποιήσουμε.

Εάν θέλουμε να δούμε λίγο τη θεωρία της Τεχνικής των Ελλειπτικών Καμπυλών, θα θεωρήσουμε μια ελλειπτική καμπύλη ως μια απλή καμπύλη πάνω σε ένα πεπερασμένο πεδίο (άλλο εκτός των πραγματικών αριθμών) που περιλαμβάνει τα σημεία που ικανοποιούν τη σχέση:

$$y^2 = x^3 + ax + b$$

μαζί με ένα διακεκριμένο σημείο στο άπειρο, που το συμβολίζουμε με ∞.

Το σύνολο αυτό, μαζί με τις πράξεις της ομάδας ελλειπτικών καμπυλών αποτελεί μια Αβελιανή ομάδα με το σημείο του απείρου να είναι το ταυτοτικό στοιχείο. Η δομή της ομάδας προκύπτει από την ομάδα διαιρέτη της υποκείμενης αλγεβρικής ποικιλίας:

$$Div^0(E) \to Pic^0(E) \simeq E$$

Πολλά πρωτόκολλα που στηρίζονται στον Διακριτό Λογάριθμο έχουν προσαρμοστεί στις ελλειπτικές καμπύλες, με την αντικατάσταση της ομάδας $(\mathbb{Z}_p)^\times$ με μια ελλειπτική καμπύλη.

Μερικά από αυτά είναι τα εξής:

- Η εγκατάσταση κλειδιού Diffie-Hellman για Ελλειπτικές Καμπύλες βασίζεται στο γνωστό σύστημα Diffie-Hellman.
- Το Ολοκληρωμένο Σύστημα Κρυπτογράφησης των Ελλειπτικών Καμπυλών, που είναι επίσης γνωστό με το όνομα Σύστημα Κρυπτογράφησης Ελλειπτικών Καμπυλών.
- Ο Αλγόριθμος Ψηφιακής Υπογραφής των Ελλειπτικών Καμπυλών, που βασίζεται στον Αλγόριθμο Ψηφιακής Υπογραφής.

Περιληπτικά, για να χρησιμοποιήσουμε την ΚΕΚ, όλες οι πλευρές θα πρέπει να συμφωνήσουν σε όλα τα στοιχεία που ορίζουν την ελλειπτική καμπύλη, δηλαδή, τις παραμέτρους του πεδίου ορισμού του συστήματος. Το πεδίο ορισμού ορίζεται από το p για την περίπτωση των πρώτων και από τα m και f

για την δυαδική περίπτωση. Η ελλειπτική καμπύλη ορίζεται από τις σταθερές a και b που χρησιμοποιούνται στην εξίσωσή ορισμού της. Τέλος, η κυκλική υποομάδα ορίζεται από τον γεννήτορά της (γνωστό κι ως σημείο βάσης) G. Για την κρυπτογραφική εφαρμογή, η τάξη του G, που είναι ο μικρότερος θετικός αριθμός n, τέτοιος ώστε $nG = \infty$, είναι συνήθως πρώτος. Επειδή το n είναι το μέγεθος μιας υποομάδας του $E(\mathrm{F}_p)$, από το θεώρημα του Lagrange προκύπτει ότι ο αριθμός $h = \frac{1}{n}\left|E(\mathrm{F}_p)\right|$ είναι ακέραιος. Στις κρυπτογραφικές εφαρμογές ο αριθμός h, που ονομάζεται συμπαράγοντας, πρέπει να είναι μικρός $(h \leq 4)$ και κατά προτίμηση $h = 1$. Ανακεφαλαιώνοντας, στην περίπτωση των πρώτων, οι παράμετροι του πεδίου ορισμού είναι (p, a, b, G, n, h) και στη δυαδική μορφή είναι (m, f, a, b, G, n, h).

Όμως για να χρησιμοποιηθούν οι πιο πάνω παράμετροι ενός πεδίου ορισμού, θα πρέπει πρώτα να επαληθευθούν, εκτός κι αν έχουν παραχθεί από μια πηγή που θεωρείται έμπιστη.

Σε αυτό το σημείο δεν κάνουμε εκτενέστερη αναφορά στις τεχνικές και μεθόδους της Κρυπτογραφίας Ελλειπτικών Καμπυλών, καθότι είναι πέρα από τα εύρος ενδιαφέροντος της παρούσας εργασίας.

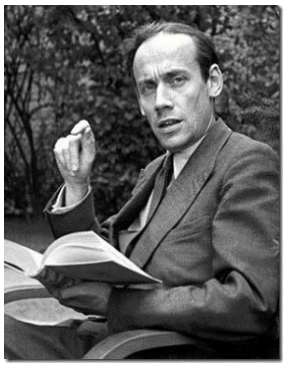
ΚΕΦΑΛΑΙΟ ΙΙ

ΟΜΑΔΕΣ ΠΛΕΞΙΔΩΝ

ΙΙ.1
Ορισμοί και Βασικές Έννοιες

ΙΙ.1.1. Ιστορική Ανασκόπηση

Οι ομάδες πλεξίδων εισήχθησαν αποκλειστικά από τον Emil Artin το 1925. Αν και σύμφωνα με τον Wilhelm Magnus (1974), είχαν ήδη κάνει σιωπηρά την εμφάνισή τους, στο έργο του Adolf Hurwitz πάνω στη Μονοδρομία το 1891. Πιο συγκεκριμένα, ο Magnus ισχυρίζεται ότι ο Hurwitz έδωσε την ερμηνεία της ομάδας πλεξίδας ως τη δομική ομάδα ενός χώρου διαμόρφωσης. Μια ερμηνεία που ο κόσμος αγνοούσε, μέχρι το 1962, όταν και ανακαλύφθηκε εκ νέου από τους Ralph Fox και Lee Neuwirth.


Emil Altin


Wilhelm Magnus


Adolf Hurwitz


Ralph Fox

Φωτογραφία ΙΙ.1

Η θεωρία των πλεξίδων μέσα στα χρόνια έχει βρει πολλές εφαρμογές σε πολλές περιοχές, όπως η τοπολογία, η μιγαδική ανάλυση και η θεωρία κόμβων που αποτέλεσε και την αρχική έμπνευση. Όμως, η θεωρία πλεξίδων δεν περιορίστηκε μόνον στα Μαθηματικά. Έτσι, η χημεία, η γενετική, η φυσική και πολλοί άλλοι χώροι γνώρισαν τις δυνατότητες πίσω από αυτή τη θεωρία.

Στην περίπτωσή μας, οι ομάδες πλεξίδων έχουν κάνει την εμφάνιση ως η πλατφόρμα ενός μη-μεταθετικού κρυπτογραφικού πρωτόκολλου δημόσιου κλειδιού, στο paper των I. Anshel, M. Anshel και D. Goldfeld [1]. Σύμφωνα με την παράδοση, οι συγγραφείς του πιο πάνω paper, μόλις επινόησαν το δικό τους πρωτόκολλο, προσέγγισαν την Joan Birman, για να τη συμβουλευτούν ως προς το ποια μη-αβελιανή ομάδα θεωρεί καλή ώστε να τη χρησιμοποιήσουν ως πλατφόρμα. Η άμεση απάντηση που πήραν είναι η «Ομάδα Πλεξίδων».


Michael Anshel and Iris Anshel


Michael Anshel


Dorian Goldfeld


Joan Birman

Φωτογραφία ΙΙ.2

Δυστυχώς, δεν είμαστε τόσο εξοικειωμένοι με την αφηρημένη έννοια των ομάδων, όπως είμαστε με τους αριθμούς, και για τον λόγο αυτόν γίνεται δύσκολο να μιλάμε για κάποια κρυπτογραφικά προϊόντα που βασίζονται σε ομάδες. Το γεγονός όμως ότι οι ομάδες πλεξίδων έχουν αρκετές εφαρμογές στο χώρο των Μαθηματικών και της Φυσικής, δίνει περισσότερη αξιοπιστία στη δυσκολία του προβλήματος.

Για να το καταλάβουμε αυτό, αρκεί να συνειδητοποιήσουμε ότι η ασφάλεια του κρυπτοσυστήματος RSA βασίζεται κυρίως στην μακρά ιστορία με τις χιλιάδες ατόμων, συμπεριλαμβανομένων και τους Euler και Gauss, να προσπαθούν να παραγοντοποιήσουν τους ακεραίους γρήγορα.

ΙΙ.1.2. Βασικές προαπαιτούμενες γνώσεις

Στο κεφάλαιο Ι, είδαμε πολλά στοιχεία και πληροφορίες σχετικά με τη θεωρία ομάδων και κυρίως σχετικά με το θέμα του προβλήματος της συζυγίας. Πολλά όμως από αυτά, μπορούν να εφαρμοστούν και σε κάθε κανονικό κρυπτογραφικό πρωτόκολλο μιας κατεύθυνσης και σε γενικές γραμμές θα έχουμε να κάνουμε με τα ακόλουθα αξιώματα:

1. Θα πρέπει να έχουμε μελετήσει και να γνωρίζουμε την ομάδα καλά.

2. Το πρόβλημα της λέξης στη G, θα πρέπει να μπορεί να επιλυθεί από έναν ντετερμινιστικό αλγόριθμο σε πραγματικά γρήγορο χρόνο, δηλαδή γραμμικό ή τετραγωνικό. Ακόμη καλύτερα, θα πρέπει να έχουμε έναν αποτελεσματικό τρόπο υπολογισμού για τα στοιχεία της G.

3. Θα πρέπει να μπορούμε να κωδικοποιήσουμε τα στοιχεία της G με τέτοιον τρόπο ώστε να είναι δύσκολο να υπολογίσουμε και να πάρουμε κάποια x και y από κάποιο προϊόν xy, με μια απλή παρατήρηση. Είναι προφανές ότι και πάλι θέλουμε έναν επαρκώς και αποτελεσματικό υπολογιστικό τρόπο.

   Εάν η G αποδίδεται μόνον από κάποιους γεννήτορες και κάποιες ορίζουσες σχέσεις, χωρίς να έχουμε κάποιες επιπλέον πληροφορίες σχετικά με τις ιδιότητες της G ή κάποιον αποτελεσματικό υπολογιστικό τρόπο, τότε και οι σχέσεις αυτές θα πρέπει να είναι σχετικά σύντομες.

4. Η G θα πρέπει να είναι κάποια ομάδα υπερ-πολυωνυμικής, πιθανών εκθετικής, ανάπτυξης. Αυτό σημαίνει ότι ο αριθμός των στοιχείων μήκους ν στη G θα πρέπει να αναπτυχθούν πιο γρήγορα από κάθε άλλο πολυώνυμο στο ν. Κάτι που είναι απαραίτητο για να αποφευχθούν επιθέσεις που έχουν ως στόχο να εξαντλήσουν όλα τα πιθανά κλειδιά. Στην περίπτωσή μας, με τον όρο «μήκος ν» αναφερόμαστε στο μήκος μια λέξης που αναπαριστά ένα στοιχείο της ομάδας, αν και γενικότερα, θα μπορούσε να σημαίνει και το μήκος υπό άλλη μορφή, όπως την πολυπλοκότητα.

ΙΙ.2
Παράσταση Ομάδας Πλεξίδων

Εισαγωγή

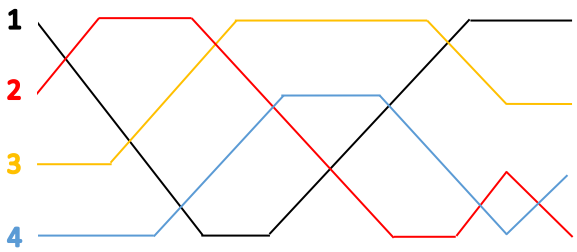
Για να κατανοήσουμε καλύτερα τη θεωρία των πλεξίδων και σύμφωνα με το [2], θα πάρουμε μερικά εύκολα παραδείγματα, όπου είναι χαρακτηριστικά για τις περιπτώσεις που θέλουμε να μελετήσουμε και με τη βοήθεια των σκίτσων, ελπίζουμε πως η κατανόησή τους θα γίνει ακόμη πιο εύκολη.

Ορισμός ΙΙ.1
Έτσι, για την περίπτωση των πλεξίδων, αυτές προκύπτουν αν:

i. Χρησιμοποιήσουμε νήματα που θα τα τοποθετήσουμε παράλληλα.
ii. Το πλήθος των νημάτων είναι πεπερασμένο.
iii. Τα νήματα κινούνται προς την ίδια κατεύθυνση και δημιουργούν μια 1-1 αντιστοιχία.
iv. Τα νήματα δε σχηματίζουν βρόγχους.

□

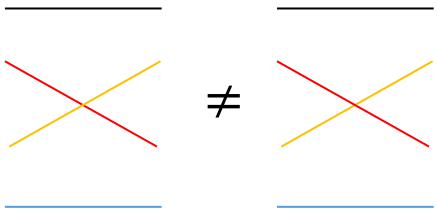
Στο πιο κάτω σχήμα, βλέπουμε μια παράσταση πλεξίδων, όπου τα νήματα που έχουμε χρησιμοποιήσει κατευθύνονται από αριστερά προς δεξιά. Ενώ αν θέλουμε να τα αριθμήσουμε, αυτό το έχουμε πράξει με αύξουσα σειρά από πάνω προς τα κάτω.



Σχήμα ΙΙ.1

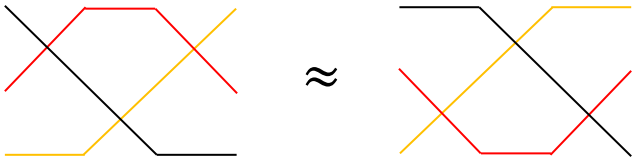
Παρατηρώντας κάποιος το πιο πάνω σχήμα, θα μπορούσε να πει ευθαρσώς ότι καθότι πρόκειται για 1-1 και επί απεικόνιση, έχουμε να κάνουμε με μια μετάθεση. Όμως, υπάρχει σημαντική διαφορά ανάμεσα στις πλεξίδες και τις

μεταθέσεις. Ο λόγος είναι ότι στις πρώτες, η όποια διασταύρωση μεταξύ των όποιων νημάτων, μπορεί να γίνει είτε από μπροστά, είτε από πίσω. Έτσι, κάθε μια από τις πιο πάνω επιλογές (μπροστά ή πίσω) σε μια διασταύρωση μας δίνει δύο διαφορετικές πλεξίδες. Αν θέλουμε να το δούμε αυτό γραφικά, στο πιο κάτω σχέδιο, παρατηρούμε ότι έχουμε μεν την ίδια μετάθεση, αλλά οι πλεξίδες που προκύπτουν δεν είναι ίδιες, γιατί στην πρώτη πλεξίδα το πορτοκαλί νήμα περνάει μπροστά από το κόκκινο ενώ στη δεύτερη από πίσω.



Σχήμα ΙΙ.2

Θεωρούμε ότι δύο πλεξίδες είναι ισοδύναμες, εάν είναι ισότοπες. Δηλαδή, εάν μετακινήσουμε μεταξύ τους τα νήματα της μιας πλεξίδας στο χώρο, χωρίς να μετακινήσουμε τις κορυφές των νημάτων, μέχρι να σχηματιστεί η άλλη πλεξίδα. Ένα τέτοιο παράδειγμα ισοδύναμων πλεξίδων είναι και το πιο κάτω:



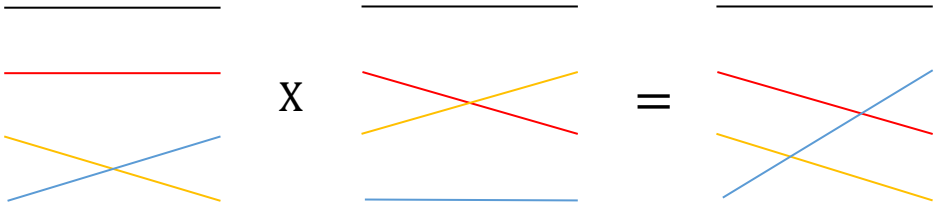
Σχήμα ΙΙ.3

Αξίζει σε αυτό το σημείο να κάνουμε αναφορά και στην πλεξίδα με ν νήματα, που δεν έχει όμως διασταυρώσεις και την οποία θα ονομάσουμε ως την τετριμμένη πλεξίδα.

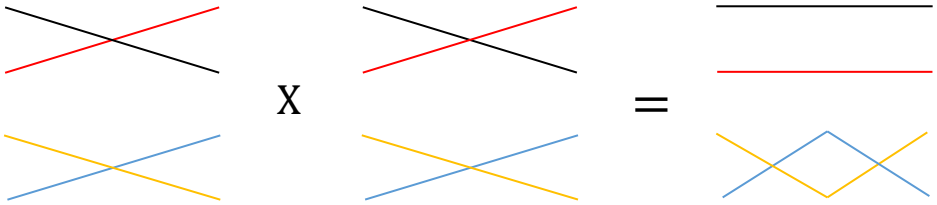
Τι γίνεται όμως όταν ενώσουμε δύο πλεξίδες με τέτοιο τρόπο ώστε να προκύψει το «γινόμενο» τους; Για να το δούμε αυτό στην πράξη, πρέπει να πάρουμε δύο πλεξίδες m και n και να τις ενώσουμε με τέτοιο τρόπο ώστε το

τέλος της m να συμπίπτει με την αρχή της n, δημιουργώντας την πλεξίδα mn. Εάν θέλουμε να το δούμε αυτό και γραφικά, θα έχουμε:

Παράδειγμα Α



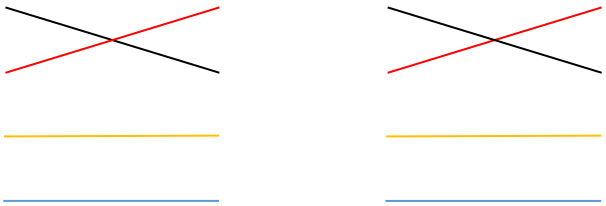
Παράδειγμα Β



Σχήμα ΙΙ.4

Έστω ότι έχουμε πλεξίδες με ν νήματα, τότε θα ονομάσουμε με B_ν το αντίστοιχο σύνολο. Αυτό θα έχει τη δομή ομάδας, καθότι αν πάρουμε και ενώσουμε μια πλεξίδα με την αντίστροφη εικόνα της ως προς τον κάθετο άξονα, το αποτέλεσμα που θα έχουμε θα είναι ισότοπο ως προς την τετριμμένη πλεξίδα.

Για να δούμε τι εννοούμε με την αντίστροφη εικόνα μιας πλεξίδας ως προς τον κάθετο άξονα, αρκεί να παρατηρήσουμε το πιο κάτω σχήμα. Έτσι, η αριστερή (m) αποτελεί την αρχική πλεξίδα και η δεξιά $(m)^{-1}$ την αντίστροφή της ως προς τον κάθετο άξονα.



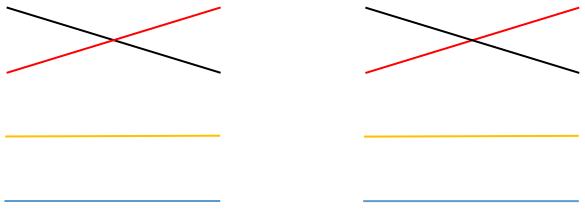
m m^{-1}

Σχήμα ΙΙ.5

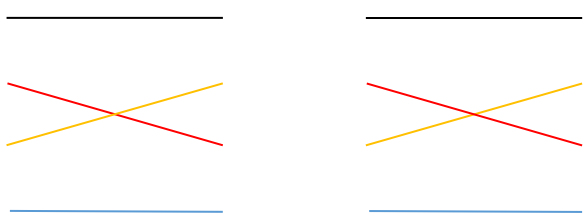
Στην ουσία, κάθε πλεξίδα είναι μια ακολουθία από διασταυρώσεις νημάτων. Θα λέμε ότι μια διασταύρωση νημάτων είναι θετική, εάν το νήμα που βρίσκεται μπροστά έχει θετική κλίση. Αλλιώς θα λέμε ότι είναι αρνητική.

Για πλεξίδες με ν νήματα, θα έχουμε ακριβώς $\nu - 1$ ικανούς τύπους διασταυρώσεων, τους οποίους και θα συμβολίσουμε με $x_1, \dots, x_{\nu-1}$ όπου το x_i είναι μια θετική διασταύρωση μεταξύ των i και $i + 1$ νημάτων.

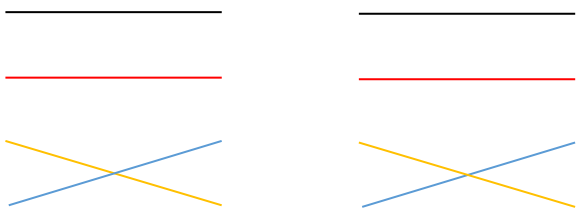
Αυτό μπορούμε να το δούμε πιο εύκολα και στο κάτω σχήμα, όπου αριστερά έχουμε τις θετικές διασταυρώσεις και δεξιά τις αντίστροφες απεικονίσεις (αρνητικές διασταυρώσεις):



x_1 ${x_1}^{-1}$



x_2 ${x_2}^{-1}$



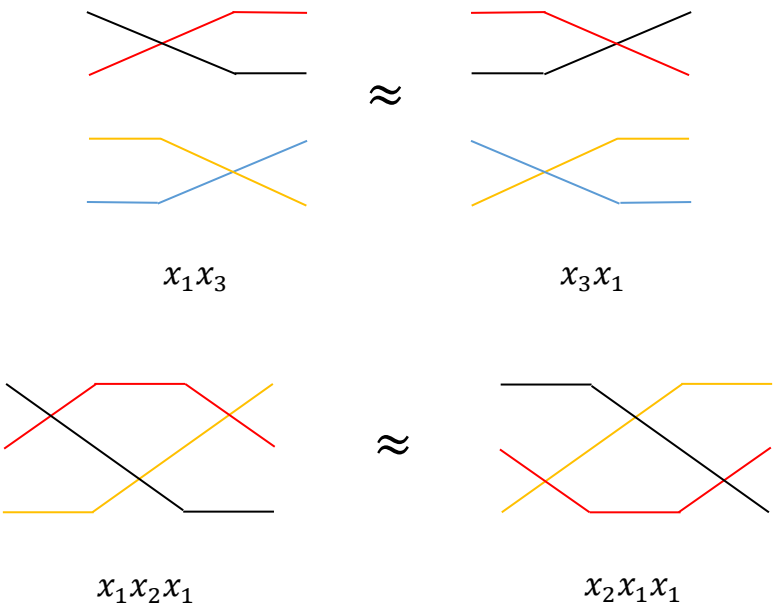
Σχήμα ΙΙ.6

Κατά συνέπεια, επειδή κάθε πλεξίδα είναι μια ακολουθία από διασταυρώσεις, το σύνολο $\{x_1, \dots, x_{\nu-1}\}$ θα παράγει το B_ν.

Μπορούμε εύκολα να διαπιστώσουμε ότι οι διασταυρώσεις $x_1, \dots, x_{\nu-1}$ υπόκεινται στις ακόλουθες σχέσεις:

1. $[x_i, x_j] = 1$, για κάθε i, j τέτοια ώστε $|i-j| > 1$ και
2. $x_i x_{i+1} x_i = x_{i+1} x_i x_{i+1}$, για κάθε i τέτοιο ώστε $1 \leq i \leq \nu - 2$.

Μπορούμε να δούμε και τα πιο κάτω σχήματα για να καταλάβουμε καλύτερα:



Σχήμα ΙΙ.7

Οι δύο σχέσεις που είδαμε πιο πάνω, περιγράφουν την ισοδυναμία των πλεξίδων, αλλά αυτό είναι δύσκολο να το αποδείξουμε.

Για παράδειγμα, η ομάδα πλεξίδων B_ν έχει την Artin παράσταση:

$$B_\nu = \langle x_1, \dots, x_{\nu-1} \mid \begin{cases} x_i x_j x_i = x_j x_i x_j & \alpha\nu\ |i-j| = 1 \\ x_i x_j = x_j x_i & \alpha\nu\ |i-j| > 1 \end{cases} \rangle$$

Αν τώρα έχουμε μια ομάδα G και ένα ομομορφισμό ομάδων f, για $B_\nu \longrightarrow G$, τότε και τα ακόλουθα στοιχεία g_i της G, με $g_i = f(x_i)$ και $i = 1, \dots, \nu - 1$ θα ικανοποιούν τις σχέσεις που είδαμε πιο πάνω, δηλαδή τις:

1. $x_i x_j = x_j x_i$, για κάθε i, j τέτοια ώστε $|i - j| > 1$ και
2. $x_i x_{i+1} x_i = x_{i+1} x_i x_{i+1}$, για κάθε i τέτοιο ώστε $1 \leq i \leq \nu - 2$.

Η ομάδα των μεταθέσεων S_ν είναι μη-Αβελιανή για $\nu \geq 3$, γιατί μπορούμε να δούμε το παράδειγμα $(1\ 2)(2\ 3) \neq (2\ 3)(1\ 2)$.

Άρα, επειδή η προβολή της B_ν στην S_ν είναι επιμορφισμός ομάδων, θα έχουμε πως και η B_ν είναι μη-Αβελιανή για $\nu \geq 3$.

Από την πιο πάνω περιγραφή, καθίσταται σαφές ότι υπάρχουν αρκετά ζευγάρια μεταθετικών υποομάδων στη B_ν, κάτι που την κάνει μια ιδανική ομάδα για αρκετά πρωτόκολλα.

Για παράδειγμα, οι Ko και Lee [3], στο έργο τους χρησιμοποίησαν τις ακόλουθες δύο μεταθετικές υποομάδες:

- LB_ν, που παράγεται από $x_1, \dots, x_{\left[\frac{\nu}{2}\right]-1}$ και
- UB_ν, που παράγεται από $x_{\left[\frac{\nu}{2}\right]+1}, \dots, x_{\nu-1}$.

Να σημειώσουμε σε αυτό το σημείο ότι η ομάδα B_ν και όλες οι υποομάδες της είναι προσεγγιστικά πεπερασμένες και αυτό βοηθάει στο να γίνεται το πρόβλημα της λέξης επιλύσιμο σε αυτήν.

Στην αρχή του Κεφαλαίου, κάναμε μια αναφορά σε κάποιες ιδιότητες που τις θεωρήσαμε ως βασική γνώση. Αναμφισβήτητα, υπάρχει μεγάλος όγκος αρθρογραφίας που σχετίζεται με τα προβλήματα της λέξης και της συζυγίας

για τις ομάδες πλεξίδων. Μερικές πρώτες απόπειρες επίλυσης από τον Garside, μπορούν να βρεθούν στη μονογραφία της J. Birman [4]. Έκτοτε, παρουσιάστηκαν πολλοί αλγόριθμοι που θα μπορούσαμε να τους χαρακτηρίσουμε ως αρκετά αποτελεσματικούς. Ο καλύτερος ντετερμινιστικός αλγόριθμος για το πρόβλημα της λέξης, έχει τετραγωνικό χρόνο πολυπλοκότητας σε συνάρτηση με το μήκος της λέξης που θα εισάγουμε και μπορούμε να τον βρούμε στο έργο [5].

Σε αυτό το σημείο θα πρέπει να αναφέρουμε και τον αλγόριθμο του Dehorney για το πρόβλημα της λέξης. Δε γνωρίζουμε ποια θα μπορούσε να είναι η χειρότερη πολυπλοκότητα που αυτός μπορεί να μας δώσει, αλλά σίγουρα για διάφορες πρακτικές εφαρμογές μπορεί να αγγίξει και τον γραμμικό χρόνο. Πιο πολλές πληροφορίες μπορούμε να βρούμε στο [6].

Τα ίδια ισχύουν και για το πρόβλημα της συζυγίας που αποκτάει όλο και περισσότερο ενδιαφέρον ως πρόβλημα. Αν και έχουν γίνει πραγματικά αξιοσημείωτες προσπάθειες και έχει σημειωθεί πρόοδος, εξακολουθεί να παραμένει ανοιχτό πρόβλημα το ζήτημα αν το πρόβλημα της συζυγίας και τα προβλήματα αναζήτησης στις ομάδες πλεξίδων μπορούν να επιλυθούν από έναν ντετερμινιστικό αλγόριθμο σε πολυωνυμικό χρόνο. Με άλλα λόγια παραμένει ανοιχτό ζήτημα εάν το πρόβλημα της συζυγίας στις ομάδες πλεξίδων ανήκει στην κλάση πολυπλοκότητας NP ή όχι.

Τέλος, κλείνοντας το κομμάτι αυτό, θα πρέπει να σημειώσουμε ότι όλες οι ομάδες πλεξίδων B_ν, για $\nu \geq 2$, έχουν εκθετική αύξηση. Ενώ για $\nu \geq 3$ είμαι προφανές επειδή η B_ν έχει ελεύθερες υποομάδες. Για παράδειγμα τα x_1^2 και x_2^2 παράγουν μια ελεύθερη υποομάδα [7]. Αν θέλουμε να βρούμε περισσότερες πληροφορίες σχετικά με τους χρόνους και τις πολυπλοκότητες, αρκεί να ανατρέξουμε στο [8].

ΙΙ.3
Κανονικές μορφές ομάδων πλεξίδων

Οι κανονικές μορφές μας εξασφαλίζουν τη δυνατότητα να συγκρίνουμε τα στοιχεία μιας ομάδας αλλά και μας παρέχουν έναν αντιπρόσωπο από κάθε κλάση ισοδυναμίας ανάμεσα στα στοιχεία της ομάδας. Ας δούμε δύο τέτοιες μορφές παρακάτω.

ΙΙ.3.1. Ελεύθερη μορφή του Dehornoy

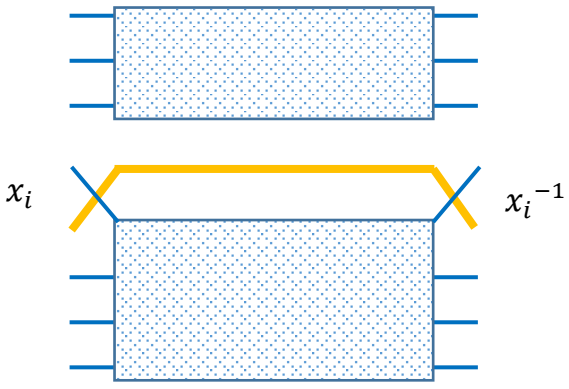
Στην προσπάθειά του να αποδείξει την επιλυσιμότητας του προβλήματος της λέξης σε ομάδες πλεξίδων, ο Dehornoy παρουσίασε τη μέθοδο με την οποία έκανε αναγωγή των λαβών σε μια πλεξίδα. Αυτή δεν αφορά μόνον συλλαβές της μορφής xx^{-1} ή $x^{-1}x$, αλλά και λέξεις της μορφής $x_i \dots x_i^{-1}$ ή $x_i^{-1} \dots x_i$.

Ας δούμε όμως και πιο συγκεκριμένα πως αυτή λειτουργεί.

Ορισμός ΙΙ.2
Έστω ότι έχουμε μια λέξη w με γράμματα από το σύνολο των γεννητόρων της B_ν. Τότε μια λαβή x_i θα είναι μια υπολέξη της w και θα έχει τη μορφή:

$$x_i^{-\varepsilon} w(x_1, \dots, x_{i-2}, x_{i+1}, \dots, x_\nu) x_i^{\varepsilon} \text{ με } \varepsilon = \pm 1$$

□
Αν θέλουμε να δούμε και γραφικά πως θα ήταν μια λαβή x_i, αρκεί να εστιάσουμε στο πιο κάτω σχήμα:



Λαβή x_i

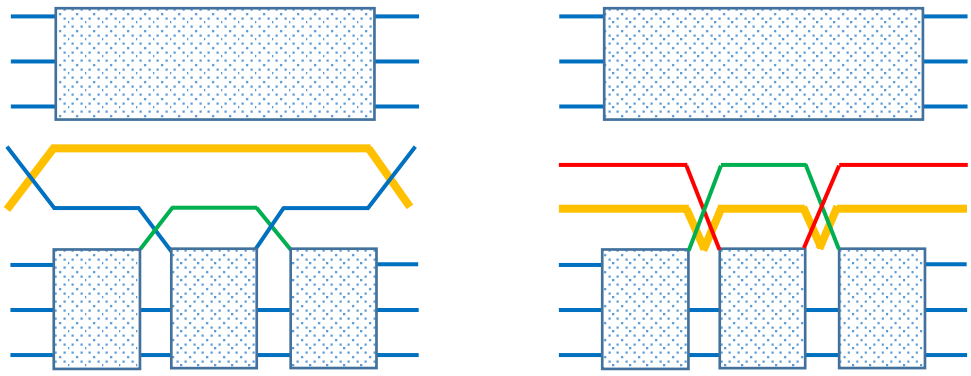
Σχήμα ΙΙ.8

Έστω μια λαβή x_i με $x_i{}^{-\varepsilon} w x_i{}^{\varepsilon}$ όπου $w = w(x_1, \dots, x_{i-2}, x_{i+1}, \dots, x_n)$ και $\varepsilon = \pm 1$, τότε αυτή θα λέγεται επιτρεπτή αν η w δεν περιέχει λαβές x_{i+1}.

Έστω ότι έχουμε μια λέξη πλεξίδων u. Τότε θα παίρνουμε τη λέξη πλεξίδων u' από τη u, με αναγωγή λαβής σε ένα βήμα, εάν κάποια υπολέξη της u είναι μια επιτρεπτή λαβή x_i με $x_i{}^{-\varepsilon} w x_i{}^{\varepsilon}$. Τη u' την παίρνουμε εφαρμόζοντας τις ακόλουθες αντικαταστάσεις για όλα τα γράμματα της λαβής $x_i{}^{-\varepsilon} w x_i{}^{\varepsilon}$ όπου θα διαγράψουμε το αρχικό και το τελικό γράμμα $x_i^{\pm 1}$ και θα αντικαταστήσουμε κάθε γράμμα $x_{i+1}^{\pm 1}$ με $x_{i+1}^{-\varepsilon} x_i^{\pm 1} x_{i+1}^{\varepsilon}$

$$x_j^{\pm 1} \to \begin{cases} 1, & \text{εάν } j = 1 \\ x_{i+1}^{-\varepsilon} x_i^{\pm 1} x_{i+1}^{\varepsilon}, & \text{εάν } j = i+1 \\ x_j^{\pm 1}, & \text{εάν } j < i \text{ ή } j > i+1 \end{cases}$$

Αν θα θέλαμε να το δούμε αυτό και γραφικά, αρκεί να μελετήσουμε το πιο κάτω σχήμα:



Αναγωγή λαβής σε ένα βήμα για μια επιτρεπτή Λαβή x_i

Σχήμα ΙΙ.9

Θα μπορούσαμε να πούμε ότι παίρνουμε τη λέξη πλεξίδων u' από τη λέξη πλεξίδων u με αναγωγή λαβής σε s βήματα, εάν υπάρχει μια ακολουθία $m+1$ λέξεων $u = u_0, u_1, \dots, u_m = u'$ όπου το καθένα το παίρνουμε από το προηγούμενο με αναγωγή λαβής σε ένα βήμα.

Έτσι, θα έχουμε πλεξίδα ισοδύναμη με την αρχική και επιπροσθέτως, με τον ίδιο τρόπο που έχουμε την αναγωγή στις ελεύθερες ομάδες, έτσι κι εδώ, μια

λέξη πλεξίδων w θα είναι ισοδύναμη με την τετριμμένη πλεξίδα ε, αν έχουμε κάποια ακολουθία αναγωγών της w στο ε, της μορφής:

$$w = w_0 \to w_1 \to \cdots \to w_N = \varepsilon$$

Όπου η λέξη w_{m+1} θα προκύψει με την αναγωγή λαβής από τη λέξη:

$$w_m, \forall m = 0, \dots, N-1.$$

Μια λέξη πλεξίδων θα την ονομάσουμε ελεύθερης λαβών εάν δεν περιέχει λαβές. Συνοψίζοντας, η ουσία της αναγωγής λαβών μπορεί να συνοψιστεί στο ακόλουθο θεώρημα:

Θεώρημα:

Θεώρημα ΙΙ.1
Έστω ότι έχουμε μια λέξη πλεξίδων u. Τότε θα ισχύουν τα ακόλουθα:

- Κάθε ακολουθία από αναγωγές λαβών που εφαρμόζονται στη u, μπορεί να σταματήσει και να μας δώσει μια λέξη πλεξίδων u' απαλλαγμένη από λαβές (κάτι που εξαρτάται από μια συγκεκριμένη ακολουθία αναγωγών), αντιπροσωπεύοντας το ίδιο στοιχείο της ομάδας πλεξίδας όπως η u.

- Η λέξη u αντιπροσωπεύει το τετριμμένο στοιχείο της ομάδας πλεξίδων αν και μόνον αν κάθε ακολουθία από αναγωγές λαβών που εφαρμόζονται στη u μας δίνει την τετριμμένη λέξη, δηλαδή το τετριμμένο στοιχείο της ομάδας.

□

Πολυπλοκότητα:

Αν και γενικά η μέθοδος με τις αναγωγές λαβών είναι πρακτικά εφικτή και στις περισσότερες των περιπτώσεων τρέχει σε γραμμικό χρόνο ως προς το μήκος της λέξης πλεξίδων, ακόμη δεν υπάρχει κάποια θεωρητική προσέγγιση της πολυπλοκότητας. Για περισσότερες πληροφορίες σχετικά με την προσέγγιση της πολυπλοκότητας, κάποιος μπορεί να μελετήσει το μέρος 3.3 στο [9].

ΙΙ.3.2. Κανονική μορφή του Garside

Τι είναι κανονική μορφή; Πρόκειται για ένα ερώτημα που θα πρέπει να απαντήσουμε λίγο αναλυτικότερα πριν προχωρήσουμε στην περαιτέρω ανάπτυξη της Κανονικής μορφής του Garside.

Ορισμός ΙΙ.3
Έτσι, κανονική μορφή είναι μια μοναδική παράσταση στο κάθε στοιχείο της ομάδας. Ας δούμε την επιλυσιμότητα του προβλήματος της λέξης όταν έχουμε κάποια κανονική μορφή.

Έστω ότι έχουμε μια κανονική μορφή κι έστω ε η κενή λέξη, τότε θα πρέπει να λύσουμε το ακόλουθο πρόβλημα της λέξης:

Εάν έχουμε μια λέξη πλεξίδων w, ισχύει ότι $w \equiv \varepsilon$;
Με άλλα λόγια, εάν έχουμε δύο λέξεις πλεξίδων w, w', ισχύει ότι $w \equiv w'$;

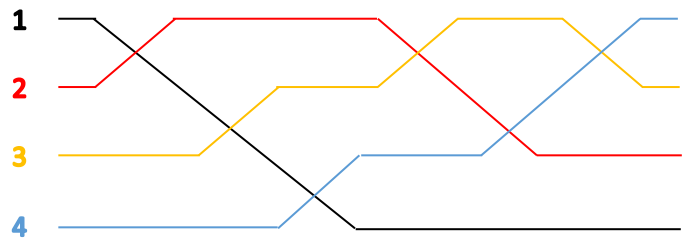
Όμως, ξέρουμε πως $w \equiv w'$ είναι ισοδύναμο με το $w^{-1}w' \equiv \varepsilon$.
□

Ορισμός ΙΙ.4
Θετική λέξη πλεξίδων είναι αυτή που μπορεί να γραφεί ως το προϊόν θετικών δυνάμεων. Το B_ν^+ είναι το μονοειδές των θετικών πλεξίδων.

Θεμελιώδης λέξη πλεξίδων είναι η $\Delta_\nu \in B_\nu^+$, όπου:

$$\Delta_\nu = (\sigma_1 \dots \sigma_{\nu-1})(\sigma_1 \dots \sigma_{\nu-2}) \dots \sigma_1$$

Από γεωμετρικής άποψης, τη Δ_ν είναι μια πλεξίδα πάνω σε ν νήματα, όπου κάθε δύο νήματα διασταυρώνονται θετικά ακριβώς μια φορά.
□



Για την ομάδα B_4 έχουμε τη $\Delta_4 = \sigma_1\sigma_2\sigma_3\sigma_1\sigma_2\sigma_1$

Σχήμα ΙΙ.10

Ιδιότητες:

Η προαναφερθείσα θεμελιώδη πλεξίδα Δ_ν, $\forall$ γεννήτορα σ_i με $1 \leq i \leq \nu - 1$ έχει και αρκετές ιδιότητες. Μερικές από τις οποίες είναι:

a. $\Delta_\nu = \sigma_i A = B\sigma_i$ για $A, B \in B_\nu^+$ (δηλαδή A, B θετικές πλεξίδες).

b. $\sigma_i \Delta_\nu = \Delta_\nu \sigma_{\nu-i} \Rightarrow B_\nu \to B_\nu$ που είναι εσωτερικός αυτομορφισμός της B_ν, ο οποίος καλείται και απεικόνιση μετατόπισης.

c. Το Δ_ν^2 είναι ο γεννήτορας του κέντρου της ομάδας B_ν.
Αυτό είναι προφανές επειδή έχουμε:

$$\Delta_\nu^{-1}\sigma_i\Delta_\nu = \sigma_{\nu-i} \Rightarrow \Delta_\nu^{-1}\sigma_{\nu-i}\Delta_\nu = \sigma_{\nu-(\nu-i)} = \sigma_i$$

Και κατά συνέπεια: $\sigma_i\Delta_\nu^2 = \sigma_i\Delta_\nu\Delta_\nu = \Delta_\nu\sigma_{\nu-i}\Delta_\nu = \Delta_\nu\Delta_\nu\sigma_i = \Delta_\nu^2\sigma_i$

Ορισμός ΙΙ.5
Μια σχέση μερικής διάταξης στην ομάδα B_ν, για $A, B \in B_\nu$, είναι η $A \preccurlyeq B$ όπου $B = A\Gamma$ για κάποια θετική πλεξίδα $\Gamma \in B_\nu^+$. Τότε θα λέμε ότι η πλεξίδα A είναι πρόθεμα της πλεξίδας B.
□

Ιδιότητες:

Η σχέση μερικής διάταξης που μόλις ορίσαμε, έχει της ακόλουθες ιδιότητες, με ε να είναι η τετριμμένη πλεξίδα:

- $B \in B_\nu^+ \Leftrightarrow \varepsilon \preccurlyeq B$
- $A \preccurlyeq B \Leftrightarrow B^{-1} \preccurlyeq A^{-1}$

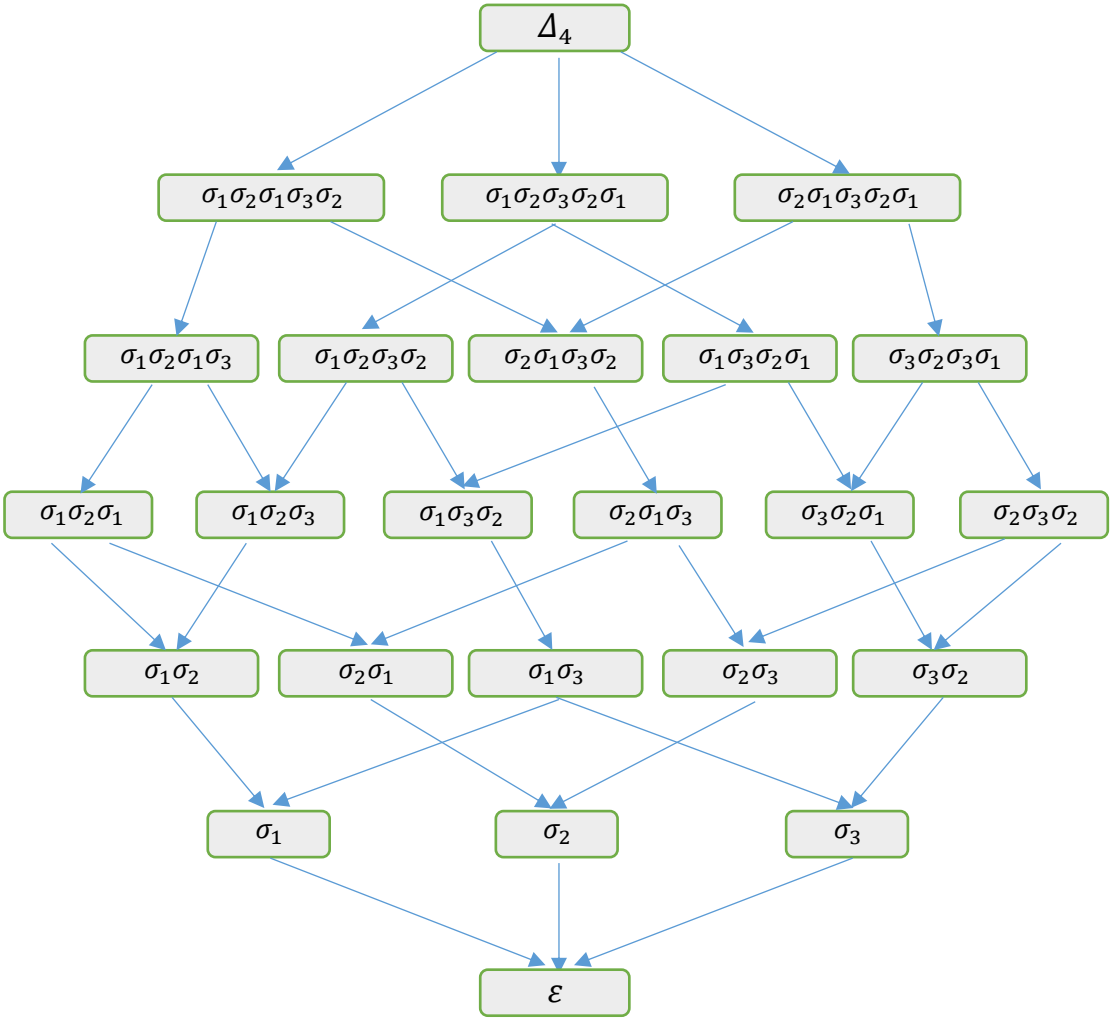
Ορισμός ΙΙ.6
Έστω $P \in B_\nu$ και τότε θα λέμε ότι το P είναι μεταθετική πλεξίδα αν:

$$\varepsilon \preccurlyeq P \preccurlyeq \Delta_\nu$$

Γνωρίζουμε ότι υπάρχουν $\nu!$ το πλήθος μεταθετικές πλεξίδες.
□

Παράδειγμα ΙΙ.1

Αν το δούμε γεωμετρικά, η μεταθετική πλεξίδα είναι μια πλεξίδα πάνω σε ν νήματα, όπου ανά δύο διασταυρώνονται θετικά το πολύ μια φορά. Τώρα, αν ενσωματώσουμε τη σχέση μερικής διάταξης $\preccurlyeq$ που ορίσαμε πιο πάνω στο σύνολο των μεταθετικών πλεξίδων, αυτά θα συμπεριφέρονται ως σύνδεσμος. Έτσι για την ομάδα B_4 θα έχουμε:



Σύνδεσμος μεταθετικών στοιχείων της B_4

Σχήμα ΙΙ.11

□

Ορισμός ΙΙ.7
Έστω $P \in B_\nu$ μια μεταθετική πλεξίδα. Τότε θα έχουμε:

- $S(P) = \{i \mid P = \sigma_i P' \; για \; κάποια \; P' \in B_\nu^+\}$
- $F(P) = \{i \mid P = P'\sigma_i \; για \; κάποια \; P' \in B_\nu^+\}$

Από την πιο πάνω σχέση συμπεραίνουμε ότι το σύνολο $S(P)$ είναι ο δείκτης των γεννητόρων της B_ν που απαρτίζουν το αρχικό τμήμα μιας παράστασης του P. Κατά τον ίδιον τρόπο, το σύνολο $F(P)$ είναι ο δείκτης των γεννητόρων της B_ν, που απαρτίζουν το τελικό τμήμα μιας παράστασης του P.
□

Ιδιότητες:

a. Το $i \in S(P)$ αν και μόνον αν τα νήματα i και $i+1$ εναλλάσσονται εντός της P.

b. $F(P) = S(rev(P))$ όπου κατά συνέπεια η $rev(P)$ αντιστρέφει τη σειρά των γραμμάτων στην P.

Για παράδειγμα: $S(\Delta_\nu) = F(\Delta_\nu) = \{1, \dots, \nu - 1\}$

Ορισμός ΙΙ.8
Έστω ότι έχουμε μια θετική πλεξίδα $A \in B_\nu^+$ και θα την αναλύσουμε σε μεταθετικές πλεξίδες ως εξής:

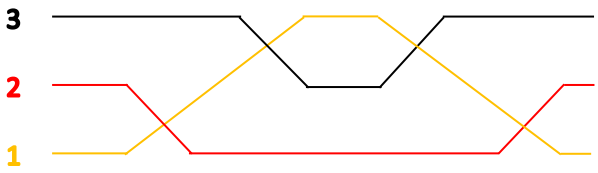
$$A = P_1 P_2 \dots P_k, \; όπου \; S(P_{i+1}) \subset F(P_i)$$

Παρατηρούμε ότι το P_i δε θα είναι πλέον μεταθετική πλεξίδα, όταν έχουμε την προσθήκη ενός γεννήτορα από το P_{i+1} στο P_i.

Η πιο πάνω μορφής ανάλυση ονομάζεται αριστερά βεβαρημένη ανάλυση (Left-weighted decomposition).
□

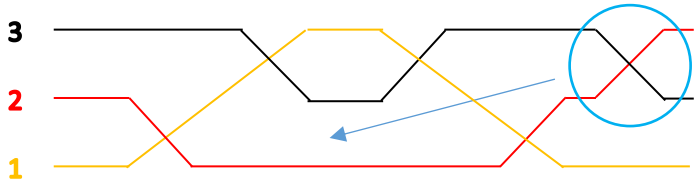
Παράδειγμα ΙΙ.2

Ας δούμε πιο κάτω δύο παραδείγματα, ένα αριστερά βεβαρημένο και ένα που δεν είναι αριστερά βεβαρημένο:



$\sigma_1\sigma_2 \quad \sigma_2\sigma_1$

Αριστερά βεβαρημένο



$\sigma_1\sigma_2 \quad \sigma_2\sigma_1\sigma_2$

Δεν είναι αριστερά βεβαρημένο

Σχήμα ΙΙ.12

Αυτό προκύπτει από: $\sigma_1\sigma_2 \cdot \sigma_2\sigma_1\sigma_2 = \sigma_1\sigma_2 \cdot \sigma_1\sigma_2\sigma_1 = \sigma_1\sigma_2\sigma_1 \cdot \sigma_2\sigma_1$

□

Θεώρημα ΙΙ.2

Σύμφωνα με το Θεώρημα του Garside για κάθε λέξη πλεξίδων $w \in B_\nu$, υπάρχει μια μοναδική παράσταση που θα την ονομάσουμε Κανονική μορφή Garside και θα την πάρουμε από:

$$w = \Delta_\nu^r P_1 P_2 \dots P_k$$

όπου το $r \in \mathbb{Z}$ είναι το μέγιστο, τα P_i είναι μεταθετικές πλεξίδες, ισχύει $P_k \neq \varepsilon$ και τα $P_1 P_2 \dots P_k$ αποτελούν την αριστερά βεβαρημένη ανάλυση.

□

Για να μετατρέψουμε μια λέξη πλεξίδων w στην Κανονική της μορφή Garside θα πρέπει να ακολουθήσουμε τα πιο κάτω βήματα:

1. Θα πρέπει να αντικαταστήσουμε τα σ_i^{-1} με $\Delta_\nu^{-1} B_i$, όπου B_i είναι η μεταθετική πλεξίδα.

2. Θα πρέπει να μετακινήσουμε κάθε εμφάνιση του Δ_ν προς τα αριστερά.

   Αυτό μπορούμε να το κάνουμε χρησιμοποιώντας τη σχέση

   $$\Delta_\nu^{-1}\sigma_i\Delta_\nu = \sigma_{\nu-i}$$

   Έτσι θα πάρουμε $w = \Delta_\nu^{r'}A$, όπου A είναι μια θετική πλεξίδα.

3. Θα πρέπει να γράψουμε την A ως μια αριστερά βεβαρημένη ανάλυση μεταθετικών πλεξίδων, υπολογίζοντας τα αρχικά και τελικά σύνολα.

   Για να το κάνουμε όμως αυτό, θα πάρουμε και θα χωρίσουμε την ανάλυση του A παίρνοντας τις μεγαλύτερες ακολουθίες γεννητόρων που μας δίνουν μεταθετικές πλεξίδες.

   Έτσι θα έχουμε $A = T_1T_2 \dots T_j$, όπου κάθε T_i με $1 \leq i \leq j$ είναι μεταθετική πλεξίδα. Τώρα $\forall i$ με $1 \leq i \leq j-1$ θα πάρουμε και θα υπολογίσουμε τα σύνολα $F(T_i)$ και $S(T_{i+1})$.

   Αν θα έχουμε $S(T_{i+1}) \nsubseteq F(T_i)$, τότε με $x \in S(T_{i+1})\backslash F(T_i)$ και με χρήση των οριζουσών σχέσεων της ομάδας πλεξίδων, θα μετατοπίσουμε το x από το T_{i+1} στο T_i.

   Έτσι θα πάρουμε:

   $A = T_1T_2 \dots T_{i'}T_{i'+1} \dots T_j$

   Εάν συνεχίσουμε μέχρι να έχουμε $S(T_{i+1}) \subset F(T_i)$, $\forall i$ με $1 \leq i \leq j-1$, θα πάρουμε την αριστερά βεβαρημένη ανάλυση που θέλαμε.

Εάν θέλουμε να δούμε και την πολυπλοκότητα της όλης διαδικασίας, θα μπορούσαμε να πούμε ότι αυτή είναι:

$O(|W|^2 \nu log\nu)$ όπου $|W|$ το μήκος της λέξης στη B_ν

Παράδειγμα ΙΙ.3
Ας δούμε τον πιο πάνω αλγόριθμο με όλα του τα βήματα στην πράξη.

Έτσι, έστω $w = \sigma_1\sigma_3^{-1}\sigma_2 \in B_4$. Θα έχουμε:

1. Ισχύει $\Delta_4 = \sigma_3\sigma_2\sigma_1\sigma_3\sigma_2 \cdot \sigma_3$, οπότε αντικαθιστούμε τα σ_3^{-1} με $\Delta_4^{-1}\sigma_3\sigma_2\sigma_1\sigma_3\sigma_2$ και θα πάρουμε:

$$w = \sigma_1\Delta_4^{-1}\sigma_3\sigma_2\sigma_1\sigma_3\sigma_2 \cdot \sigma_2$$

2. Θα μετατοπίσουμε το Δ_4^{-1} προς τα αριστερά, οπότε:

$$w = \Delta_4^{-1} \cdot \sigma_3\sigma_3\sigma_2\sigma_1\sigma_3\sigma_2\sigma_2$$

3. Τώρα θα αναλύσουμε το θετικό μέρος σε αριστερά βεβαρημένη μορφή:

$$w = \Delta_4^{-1} \cdot \sigma_2\sigma_1\sigma_3\sigma_2\sigma_1 \cdot \sigma_1\sigma_2$$

□

Ορισμός ΙΙ.9
Ας δούμε πως ορίζονται και τα Infimum και Supremum:

- $inf(w) = max\{r: \Delta^r \preccurlyeq w\}$
- $\sup(w) = \min\{s: w \preccurlyeq \Delta^s\}$

□

Τώρα αν έχουμε την Κανονική μορφή του Garside για την πλεξίδα:

$$w = \Delta_\nu^m P_1 P_1 \dots P_k$$

Θα προκύπτει:

$$\inf(w) = m, \sup(w) = m + k$$

Τέλος θα ονομάσουμε ως κανονικό μήκος της w:

$$len(w) = \sup(w) - \inf(w) = \#\mu\varepsilon\tau\alpha\theta\varepsilon\tau\iota\kappa\acute{\omega}\nu\ \pi\lambda\varepsilon\xi\acute{\iota}\delta\omega\nu$$

ΙΙ.4
Ομάδα του Thompson

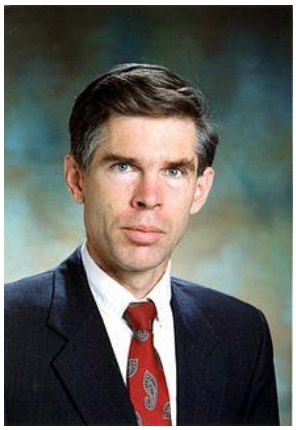
Εισαγωγή

Στην Ενότητα αυτή θα ρίξουμε μια γρήγορη και εποπτική ματιά, χωρίς να εμβαθύνουμε ιδιαίτερα, στην Ομάδα του Thompson [10].

Γενικότερα, υπάρχουν τρεις ασυνήθιστες και άπειρες ομάδες F, T και V που διατυπώθηκαν από τον Thompson. Είναι επίσης γνωστές και με τα ονόματα Vagabond (Περιπλανώμενες) Ομάδες ή Chameleon (Χαμαιλέων) Ομάδες. Εμφανίζονται για πρώτη φορά σε κάποια αδημοσίευτα χειρόγραφα του Richard Thompson από το 1965 ως πιθανό αντιπαράδειγμα στην εικασία του von Neumann και συμβολίζονται με:

$$F \subseteq T \subseteq V$$

Από τις τρεις πιο πάνω ομάδες, η F είναι αυτή που έχει μελετηθεί περισσότερο και θα μας απασχολήσει.



Richard L. Thompson

John von Neumann

Φωτογραφία ΙΙ.3

Οι Ομάδες Thompson και κυρίως η F έχει μια σειρά από ασυνήθιστες ιδιότητες, κάτι που τις έχει καταστήσει ως αντιπαράδειγμα σε πολλές εικασίες της θεωρίας ομάδων. Και οι τρεις ομάδες Thompson είναι άπειρες, αλλά

μπορούν να παρασταθούν με πεπερασμένο τρόπο. Οι ομάδες T και V είναι σπάνια παραδείγματα άπειρων, αλλά με πεπερασμένη παράσταση, περιπτώσεων απλών ομάδων. Από την άλλη, η ομάδα F μπορεί να μην είναι απλή, αλλά η υποομάδα $[F,F]$ που προκύπτει και το πηλίκο της F που προκύπτει από αυτήν είναι η ελεύθερη αβελιανή ομάδα βαθμού 2. Η F είναι πλήρως διατεταγμένη, έχει εκθετική αύξηση και δεν περιέχει κάποια υποομάδα ισομορφική προς την ελεύθερη ομάδα βαθμού 2.

Εικάζεται ότι η F δεν είναι υπαγόμενη και αυτό την καθιστά ως άλλο ένα αντιπαράδειγμα στην προσφάτως διαψευσμένη διαχρονική εικασία του von Neumann για τις ομάδες πεπερασμένης παράστασης. Είναι γνωστό ότι η F δεν είναι στοιχειωδώς υπαγόμενη.

Ορισμός ΙΙ.10
Να επισημάνουμε σε αυτό το σημείο ότι μια ομάδα G είναι υπαγόμενη όταν είναι τοπικά συμπαγής τοπολογική ομάδα και φέρει ένα είδος εφαρμογής σε φραγμένες συναρτήσεις που είναι αμετάβλητες στην απόδοσή τους από τα στοιχεία της ομάδας. Ο αρχικός ορισμός που κάνει λόγο για πεπερασμένα προσθετικό αμετάβλητο μέσο μέτρησης των υποσυνόλων της G, οφείλεται στον John von Neumann και χρονολογείται πίσω στο 1929.
□

Το 1974, ο Higman εισήγαγε μια άπειρη οικογένεια απλών ομάδων που παρουσιάζονται πεπερασμένα, συμπεριλαμβανομένου της ομάδας Thompson V ως μια ειδική περίπτωση.

Τέλος, η ομάδα F, όπως και οι ομάδες πλεξίδων B_ν, είναι ευρέως γνωστές σε αρκετούς χώρους των μαθηματικών, όπως η άλγεβρα, η γεωμετρία και η ανάλυση. Πρόκειται για άλλη μια ομάδα που είναι μη-αβελιανή.

Παραστάσεις

Η ακόλουθη έκφραση μας δίνει μια πεπερασμένη παράσταση της F:

$$\langle A, B | [AB^{-1}, A^{-1}BA] = [AB^{-1}, A^{-2}BA^2] = id \rangle$$

όπου $[x,y]$ είναι ο συνήθης μετατροπέας της θεωρίας ομάδων, $xyx^{-1}y^{-1}$.

Παρ' όλο που η F έχει μια πεπερασμένη παράσταση με 2 γεννήτορες και 2 σχέσεις, περιγράφεται πολύ πιο εύκολα και διαισθητικά από την άπειρη παράσταση:

$$\langle x_0, x_1, x_2, \dots \mid x_k^{-1} x_\nu x_k = x_{\nu+1} \; για \; k < \nu \rangle$$

Οι δύο παραστάσεις σχετίζονται με $x_0 = A$, $x_\nu = A^{1-\nu}BA^{\nu-1}$ για $\nu > 0$.

Φυσικά, εκτός από την πιο πάνω άπειρη παράσταση, υπάρχουν επίσης και πεπερασμένες παραστάσεις της ίδιας ομάδας. Για παράδειγμα:

$$F = \langle x_0, x_1, x_2, x_3, x_4 \mid x_k^{-1} x_\nu x_k = x_{\nu+1} (\nu > k, \nu < 4 \rangle$$

Αλλά αν θέλουμε να πάρουμε μια βολική κανονική μορφή, τότε θα χρησιμοποιήσουμε την άπειρη παράσταση, καθότι ενδείκνυται καλύτερα.

ΙΙ.5
Ομάδες πινάκων

Εισαγωγή

Πιθανολογούμε ότι οι ομάδες πινάκων πάνω σε πεπερασμένους μεταθετικούς δακτυλίους, είναι η καλύτερη λύση για «κανονικά» κρυπτογραφικά πρωτόκολλα, επειδή αυτές οι ομάδες συμμερίζονται τα θετικά και των δύο πλευρών. Έτσι, ο πολλαπλασιασμός πινάκων είναι μη-μεταθετικός και τα δεδομένα του πίνακα που προέρχονται από έναν μεταθετικό δακτύλιο μας προσφέρουν έναν πολύ καλό μηχανισμό απόκρυψης.

Στις ομάδες πινάκων, ο τρόπος με τον οποίον παρουσιάζουμε τα στοιχεία τους ως τετραγωνικούς πίνακες, είναι στην πραγματικότητα μια φυσική κανονική μορφή.

Για να έχουμε καλύτερη διάχυση, χρειάζεται ο βασικός δακτύλιος να είναι πεπερασμένος. Οι πεπερασμένοι δακτύλιοι R είναι περιοδικοί, κάτι που σημαίνει πώς για κάθε $u \in R$, υπάρχουν θετικοί ακέραιοι p, s τέτοιοι ώστε $u^p = u^s$. Η περιοδικότητα εξυπηρετεί τη διάχυση επειδή δημιουργεί ένα δυναμικό σύστημα και τα συστήματα αυτά, ειδικά αν έχουν έναν μεγάλο αριθμό από καταστάσεις, παρουσιάζουν πολύ σύνθετη συμπεριφορά. Σε αυτό το σημείο μπορούμε να αναφέρουμε το πολύ φημισμένο πρόβλημα «$3x + 1$», για το οποίο περισσότερες πληροφορίες βρίσκονται στο [11].

Να επισημάνουμε και πάλι πως η Μεταθετικότητα και η Περιοδικότητα αποτελούν δύο κορυφαία εργαλεία που χρησιμοποιούνται για την απόκρυψη των παραγόντων σε ένα γινόμενο. Όμως δεν πρέπει και να υπερεκτιμήσουμε την σημασία τους για την κρυπτογραφική ασφάλεια.

Μπορούμε εδώ να αναφέρουμε ότι η Μεταθετικότητα επιδέχεται ενίσχυση από τη μη-Μεταθετικότητα κι έτσι να εξασφαλίσουμε καλύτερη ασφάλεια. Οπότε η Μεταθετικότητα, σε συνεργασία με τη μη-Μεταθετικότητα, είναι ένα πολύ σημαντικό στοιχείο της κρυπτογραφικής ασφάλειας. Μπορεί να αποτρέψει τον οποιονδήποτε κακόβουλο που πραγματοποιεί μια επίθεση από το να χρησιμοποιήσει προφανείς σχέσεις, όπως η $ab = ba$, έτσι ώστε να απλοποιήσει το γινόμενο.

Να σημειώσουμε ότι οι βασικοί δακτύλιοι στις ομάδες πινάκων των κρυπτογραφικών σχημάτων, πρέπει να είναι συγκεκριμένοι, πεπερασμένοι και μεταθετικοί. Ίσως ο πλέον απλός δακτύλιος να είναι ο $\mathbb{Z}_\nu$. Οι πίνακες του $\mathbb{Z}_\nu$ μπορούν να χρησιμοποιηθούν ως μέσο στην αρχική ανταλλαγή κλειδιών Diffie-Hellman. Όμως το αρνητικό αυτής της ομάδας είναι ότι το ν πρέπει να είναι πολύ μεγάλο έτσι ώστε να εξασφαλίσει επαρκή χώρο για μεγάλα κλειδιά.

Μια άλλη περίπτωση θα μπορούσε να είναι η χρήση του $R = F_p[x]/(f(x))$. Όπου F_p είναι το πεδίο με p στοιχεία, $F_p[x]$ είναι ο δακτύλιος των πολυωνύμων πάνω στο F_p και $f(x)$ το ιδεώδες του $F_p[x]$ που παράγεται από ένα αμείωτο πολυώνυμο $f(x)$ βαθμού ν. Ο δακτύλιος θα είναι ισομορφικός ως προς το πεδίο F_{p^ν}, αλλά η παράσταση του R ως πεδίο πηλίκο επιτρέπει τη χρήση μεγάλου χώρου για τα κλειδιά, ενώ διατηρεί όλες τις βασικές παραμέτρους μικρές. Μια τέτοια απόπειρα δακτυλίου έχει γίνει από τους Tillich και Zémor [12] όταν κατασκεύαζαν μια hash συνάρτηση [13].

Στο δακτύλιο χρησιμοποίησαν τις ιδιότητες:

- $P = 2$
- $\nu\ είναι\ πρώτος$
- $και\ 100 < \nu < 200$

Και πέτυχαν το ζητούμενο τους.

ΙΙ.6
Ομάδες ακύρωσης και Αλγόριθμος του Dehn

Εισαγωγή

Μια άλλα κατηγορία ομάδων που είχε προταθεί ως λύση είναι οι ομάδες περιορισμένης ακύρωσης. Πιο πολλά μπορεί κάποιος να διαβάσει στο [14].

Ορισμός ΙΙ.11
Οι ορίζουσες σχέσεις ικανοποιούν κάτι απλό και ευκόλως αποδεικτέο στις ομάδες περιορισμένης ακύρωσης. Πιο συγκεκριμένα, έστω $F(X)$ η ελεύθερη ομάδα με βάση το $X = \{x_i \mid i \in I\}$, όπου το I είναι ταυτοτικό σύνολο. Έστω $\varepsilon_k \in \{\pm 1\}$, όπου $1 \leq k \leq \nu$.

Μια λέξη: $w(x_1, \dots, x_\nu) = x_{i_1}^{\varepsilon_1} x_{i_2}^{\varepsilon_2} \dots x_{i_\nu}^{\varepsilon_\nu}$ στην $F(X)$, με όλα τα x_{i_k} όχι απαραιτήτως διακεκριμένα, είναι η αναγωγή μιας λέξης X αν $x_{i_k}^{\varepsilon_k} \neq x_{i_{k+1}}^{-\varepsilon_{k+1}}$, για $1 \leq k \leq \nu - 1$.

Επιπλέον, μπορούμε να ισχυριστούμε ότι η λέξη $w(x_1, \dots, x_\nu)$ προκύπτει από κυκλική αναγωγή εάν έχουμε την αναγωγή από τη λέξη X και ισχύει $x_{i_1}^{\varepsilon_1} \neq x_{i_\nu}^{-\varepsilon_\nu}$.
□

Έστω ένα σύνολο R που περιέχει λέξεις που προκύπτουν από κυκλικές αναγωγές από την $F(X)$. Τότε αυτό είναι συμμετρικό εάν είναι κλειστό ως προς τις διάφορες παραλλαγές κι αν επιδέχεται αντιστροφές.

Έστω ότι έχουμε μια ομάδα με παράσταση $\langle X; R \rangle$. Μια μη κενή λέξη $u \in F(X)$ θα αποκαλείται «τμήμα» εάν υπάρχουν δύο διακεκριμένες ορίζουσες σχέσεις $r_1, r_2 \in R$ της G, τέτοιες ώστε $r_1 = uv_1$ και $r_2 = uv_2$ για κάποια $v_1, v_2 \in F(X)$, χωρίς κάποια ακύρωση μεταξύ των u και v_1 ή μεταξύ των u και v_2.

Θα λέμε ότι η ομάδα G ανήκει στην κλάση $C(p)$ εάν όλα τα στοιχεία του R είναι προϊόν τουλάχιστον p «τμημάτων». Επίσης, η ομάδα G ανήκει στην κλάση $C'(\lambda)$ εάν για κάθε $r \in R$ όπου $r = uv$ και u είναι ένα «τμήμα», έχουμε $|u| < \lambda |r|$.

Αλγόριθμος του Dehn

Ας δούμε τώρα επί μέρους τον Αλγόριθμο του Dehn. Έτσι, αν η G ανήκει στην κλάση $C'\left(\frac{1}{6}\right)$, τότε και ο αλγόριθμος του Dehn μπορεί και επιλύει αποτελεσματικά το πρόβλημα της λέξης στην G. Ο τρόπος λειτουργίας και τα βήματα του αλγορίθμου είναι πολύ απλά. Ας τα δούμε πιο κάτω:

Πρωτόκολλο ΙΙ.1

1. Έστω ότι έχουμε μια μη κενή λέξη w. Θα ψάξουμε να βρούμε κάποιο μεγάλο «τμήμα» κάποιας ορίζουσας σχέσης από το R. Αυτό σημαίνει ότι θέλουμε κάποιο «τμήμα» του οποίου το μήκος είναι μεγαλύτερο από το μισό του μήκους όλης της ορίζουσας σχέσης. Εάν δε μπορούμε να βρούμε κάποιο «τμήμα» με την πιο πάνω περιγραφή, τότε θα πάρουμε ότι $w \neq 1$ στη G.

2. Τώρα έστω ότι το προαναφερθέν «τμήμα» υπάρχει και το ονομάζουμε u. Τότε $r = uv$ για κάποιο $r \in R$, όπου το μήκος του v είναι μικρότερο από το μήκος του u. Μετά θα αντικαταστήσουμε το u με v^{-1} στη w. Το μήκος της λέξης w' που θα πάρουμε θα είναι μικρότερο από αυτό της w. Εάν $w' = 1$, τότε παίρνουμε ότι $w = 1$ στη G.

3. Εάν $w' \neq 1$, τότε θα επαναλάβουμε από το 1ο βήμα με $w := w'$.

□

Βλέπουμε πως το μήκος της w μειώνεται μετά από κάθε επανάληψη. Αυτό σημαίνει πως ο αλγόριθμος θα τερματίσει μετά από έναν πεπερασμένο αριθμό βημάτων. Η πολυπλοκότητά του ως προς τον χρόνο είναι τετραγωνική, σε σχέση με το μήκος της λέξης w.

Τέλος παρατηρούμε ότι μια ομάδα που έχει γενικώς πεπερασμένη παράσταση είναι μια μικρή ομάδα ακύρωσης.

ΙΙ.7
Επιλύσιμες ομάδες

Εισαγωγή

Ας θυμηθούμε σε αυτό το σημείο ότι μια ομάδα G ονομάζεται αβελιανή (ή μεταθετική) εάν $[a,b]=1$ για κάθε $a,b \in G$, όπου $[a,b]$ είναι εν συντομία η $\alpha^{-1}b^{-1}ab$. Αυτό μπορεί να γενικευθεί με διάφορους τρόπους.

Ορισμός ΙΙ.12
Μια ομάδα G θα ονομάζεται μετα-αβελιανή, εάν $\big[[x,y],[z,t]\big]=1$ για κάθε $x,y,z,t \in G$. Μια ομάδα G αποκαλείται Nilpotent τάξης $c \geq 1$ εάν $[y_1,y_2,\dots,y_{c+1}]=1$ για κάθε $y_1,y_2,\dots y_{c+1} \in G$ όπου $[y_1,y_2,y_3]=\big[[y_1,y_2],y_3\big]$, κτλ.
□

Η μεταθετική υποομάδα της G είναι η ομάδα $G'=[G,G]$ που παράγεται από όλες τις μεταθετικές καταστάσεις, όπως τις εκφράσεις της μορφής $[u,v]=u^{-1}v^{-1}uv$ όπου $u,v \in G$. Επιπλέον, μπορούμε να ορίσουμε με επαγωγή τον k-στο όρο της σειράς της G:

$$\gamma_1(G)=G, \qquad \gamma_2(G)=[G,G], \qquad \gamma_k(G)=[\gamma_{k-1}G,G]$$

Να σημειώσουμε εδώ ότι κάποιος μπορεί να πάρει $\alpha([u,v])=[a(u),a(v)]$ για κάθε ενδομορφισμό a στη G. Οπότε και $\gamma_k(G)$ είναι μια πλήρως αμετάβλητη υποομάδα της G για κάθε $k \geq 1$, κι έτσι $G''=[G',G']$.

Στα κρυπτογραφικά μοντέλα, συνήθως χρησιμοποιούμε τις ελεύθερες μετα-αβελιανές ομάδες.

Ορισμός ΙΙ.13
Έστω F_ν η ελεύθερη ομάδα βαθμού ν. Ενώ η ελεύθερη ομάδα F_ν/F_ν'' ονομάζεται ελεύθερη μετα-αβελιανή ομάδα βαθμού ν και θα την ονομάσουμε ως M_ν.
□

Ας δούμε όμως λίγα πράγματα σχετικά με την κανονική και ημι-κανονική μορφή των στοιχείων μιας ελεύθερης μετα-αβελιανής ομάδας M_ν. Η ημι-κανονική μορφή είναι καλή για μεταβάσεις, επειδή μπορούμε εύκολα να την επαναφέρουμε σε τέτοια μορφή που να αντιπροσωπεύει το στοιχείο μετάβασης. Όμως, αν $\nu > 2$, η μορφή δε θα είναι μοναδική (Γι' αυτό και την αποκαλούμε ημι-κανονική). Κατά συνέπεια, δε μπορεί να χρησιμοποιηθεί ως κοινό μυστικό από την Alice και τον Bob σε κάποιο κρυπτογραφικό πρωτόκολλο. Αντ' αυτού μπορεί να χρησιμοποιηθεί η κανονική μορφή, δηλαδή ένας $2x2$ πίνακας.

Έστω $u \in M_\nu$. Θα συμβολίσουμε με u_{ab} την αβελιανή μορφή του u. Ένα τέτοιο παράδειγμα είναι και η εικόνα του u όταν έχουμε τον κανονικό επιμορφισμό $\alpha: M_\nu \to M_\nu/[M_\nu/M_\nu]$. Να σημειώσουμε σε αυτό το σημείο ότι μπορούμε να ταυτοποιήσουμε το $M_\nu/[M_\nu/M_\nu]$ με το $F_\nu/[F_\nu/F_\nu]$. Τεχνικά, το u_{ab} είναι στοιχείο μιας ομάδας παραγόντων της F_ν, αλλά μπορούμε να το χρησιμοποιήσουμε και για κάθε λέξη από τους γεννήτορες x_i (ας πούμε κάποιο στοιχείο μιας συνηθισμένης ελεύθερης ομάδας F_ν) που θα αντιπροσωπεύει την u_{ab} όταν δε θα δημιουργείται ασάφεια.

Έστω $u, v \in M_\nu$. Τότε θα συμβολίσουμε με u^v την έκφραση $v^{-1}uv$. Θα μπορούσαμε επίσης να πούμε ότι το v βρίσκεται σε σύζευξη με το u. Εάν το $u \in [M_\nu/M_\nu]$, τότε έχουμε επέκταση σε ομάδα δακτύλιο $\mathbb{Z}(M_\nu/\left[\frac{M_\nu}{M_\nu}\right])$, το όποιο και για λόγους διευκόλυνσης θα το ονομάσουμε $\mathbb{Z}A_\nu$.

Άρα η ομάδα $A_\nu = M_\nu/[M_\nu/M_\nu]$ είναι η ελεύθερη αβελιανή ομάδα βαθμού ν. Έστω τώρα ότι εκφράζουμε το $W \in \mathbb{Z}A_\nu$, με τη μορφή $W = \sum \alpha_i v_i$, όπου $\alpha_i \in \mathbb{Z}$, $v_i \in A_\nu$. Τότε με u^w θα συμβολίσουμε το προϊόν $\prod (u^{a_i})^{v_i}$. Αυτό το προϊόν θα είναι καλά ορισμένο, καθότι τα στοιχεία του $[M_\nu, M_\nu]$ μετατίθενται ανά δύο στην M_ν.

Έστω τώρα $u \in M_\nu$. Τότε η u θα μπορεί να γραφεί στην ακόλουθη ημι-κανονική μορφή:

$$u = u_{ab} \cdot \prod_{i<j} [x_i, x_j]^{w_{ij}}$$

όπου $W_{ij} \in \mathbb{Z}A_\nu$.

Δε θα επεκταθούμε ως προς το πως καταλήγουμε σε αυτή τη μορφή. Όμως περισσότερες πληροφορίες μπορούν να αντληθούν από το [15].

Τώρα, αν θέλουμε να μετατρέψουμε την πιο πάνω ημι-κανονική μορφή (σχέση) σε λέξη, είναι κάτι τετριμμένο, καθότι είναι ήδη λέξη. Το μόνο

πρόβλημα με αυτήν τη μορφή (σχέση) είναι ότι δεν είναι μοναδική για $\nu > 2$ και κατά συνέπεια δε μπορεί να χρησιμοποιηθεί ως κοινό μυστικό από την Alice και τον Bob.

Για τον σκοπό αυτό θα πρέπει να χρησιμοποιήσουμε μια κανονική μορφή που θα είναι μοναδική και υπολογιστικά εφικτή (απαιτεί τετραγωνικό χρόνο σε συνάρτηση με το μήκος της u). Αυτή όμως δε θα είναι τόσο εύκολο να την επαναφέρουμε σε λέξη.

Έτσι, θα πρέπει να κάνουμε μια εισήγηση στην έννοια των παραγώγων Fox, τα οποία είναι μη μεταθετικά ανάλογα των συνηθισμένων Leibniz παραγώγων.

Όμως δε θα επεκταθούμε περισσότερο αναλύοντας την προαναφερθείσα κανονική μορφή γιατί απαιτεί εργαλεία που ξεφεύγουν από το αντικείμενο της εργασίας και τα οποία θα πρέπει να επεξηγηθούν αναλυτικά.

ΙΙ.8
Ομάδες Artin
(Γενικευμένες Ομάδες Πλεξίδων)

Εισαγωγή

Οι ομάδες Artin έχουν χρησιμοποιηθεί ως εργαλείο σε κρυπτογραφικά πρωτόκολλα στο [16]. Ας δούμε όμως λίγο τη φύση τους.

Ορισμός ΙΙ.14
Έτσι, έστω $G(\Gamma)$ μια ομάδα με παράσταση:

$$G(\Gamma) = \langle g_1, \dots, g_\nu \,;\, r(g_i, g_j) = 1 \ (\gamma\iota\alpha\ 1 \le i, j \le \nu\ \kappa\alpha\iota\ i \ne j) \rangle$$

όπου $\nu \ge 2$ και $r(g_i, g_j) \vDash 1$ είναι μια ορίζουσα σχέση που περιλαμβάνει δύο γεννήτορες. Δεδομένου του $G(\Gamma)$, υπάρχει ένα γράφημα, το Γ_G, που συσχετίζεται μαζί του και αντίστροφα. Οι κορυφές του Γ_G αντιστοιχούν στους γεννήτορες του $G(\Gamma)$. Εάν υπάρχει κάποια σχέση $r(g_i, g_j) \in G$ μεταξύ δύο γεννητόρων, τότε θα έχουμε και μια ακμή που θα ενώνει τις αντίστοιχες δύο κορυφές $g_i, g_j \in \Gamma_G$. Με άλλα λόγια, οι ακμές αντιστοιχούν σε σχέσεις.
□

Παράδειγμα ΙΙ.4
Μια ομάδα Artin, έστω $A(\Gamma)$, είναι ομάδα με παράσταση:

$$A(\Gamma) = \langle \alpha_1, \dots, \alpha_\nu \,;\, m_{ij} = m_{ji} \ (\gamma\iota\alpha\ 1 \le i < j \le \nu\ ) \rangle, \text{όπου } m_{ij} = \alpha_i\alpha_j\alpha_i \dots$$

Επίσης $s_{ij}\{\alpha_i\alpha_j\alpha_i \dots,\ \ \kappa\alpha\iota\ s_{ij} = s_{ji}$.

Οι ομάδες Artin προέκυψαν ως γενίκευση των ομάδων πλεξίδων [17]. Όταν έχουμε μια ομάδα Artin $A(\Gamma)$, το αντίστοιχο γράφημα Γ_A δε θα έχει πολλαπλές ακμές ή επαναλήψεις. Οι κορυφές α_i του Γ_A είναι και οι γεννήτορες της ομάδας Artin. Κάθε δύο κορυφές $\alpha_i, \alpha_j \in \Gamma_A$ συνδέονται με μια ακμή, την οποία και θα συμβολίσουμε με s_{ij} και θα έχει άμεση σχέση με την $m_{ij} = m_{ji}$. Δηλαδή μεταξύ των αντίστοιχων γεννητόρων $\alpha_i, \alpha_j \in A(\Gamma)$.

Σε γενικές γραμμές, οι αυτομορφισμοί (ή ενδομορφισμοί) του γραφήματος Γ_G εισάγουν αυτομορφισμούς (ή ενδομορφισμούς) της ομάδας $G(\Gamma)$. Για τον λόγο αυτόν, το γράφημα που σχετίζεται με τη $G(\Gamma)$ μας δίνει ένα τρόπο να κατασκευάσουμε μια ημιομάδα ενδομορφισμών της $G(\Gamma)$ που περιλαμβάνει έναν μεγάλο αριθμό από μεταθετικά στοιχεία. Στο [16], μπορούμε να δούμε την εφαρμογή σε πρωτόκολλο ανταλλαγής κλειδιών.
□

Παράδειγμα ΙΙ.5
Οι σχέσεις των ομάδων πλεξίδων B_ν, συμπεριλαμβάνουν δύο γεννήτορες. Το γράφημα που αντιστοιχεί στην B_ν είναι ένα απλό μονοπάτι και για τον λόγο αυτόν έχει μόνον έναν αυτομορφισμό που μας εισάγει τον ακόλουθο αυτομορφισμό της B_ν: $\sigma_i \longmapsto \sigma_{\nu-i}$, που θα είναι επίσης ένας εσωτερικός αυτομορφισμός της B_ν. Για τις υπόλοιπες ομάδες $G(\Gamma)$, τα αντίστοιχα γραφήματά τους είναι πιο περίπλοκα.

Οι ομάδες Artin $A(\Gamma)$, όταν έχουν την ιδιότητα με όλους του ακεραίους να είναι $s_{ij} \geq 4$ ονομάζονται ομάδες Artin μεγάλου τύπου. Ένα δέντρο Γ_A μπορεί να συσχετιστεί με μια ομάδα Artin μεγάλου τύπου, παρέχοντας μια άμεση διαδικασία για την κατασκευή μιας ημι-ομάδας ενδομορφισμών της $A(\Gamma)$. Επιπλέον, οι ομάδες Artin μεγάλου τύπου, είναι αυτόματες [18], και για τον λόγο αυτόν το πρόβλημα της λέξης σε ομάδες αυτής της κλάσης μπορεί να επιλυθεί σε τετραγωνικό χρόνο, και από το αποτέλεσμα που μπορούμε να διαβάσουμε στο [19], το πρόβλημα της λέξης γενικά επιλύεται σε γραμμικό χρόνο.
□

ΚΕΦΑΛΑΙΟ ΙΙΙ

ΚΑΝΟΝΙΚΗ ΜΗ-ΜΕΤΑΘΕΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

III.1
Ορισμοί και Βασικές Έννοιες

Εισαγωγή

Η μη-μεταθετική κρυπτογραφία είναι ο τομέας της κρυπτολογίας, όπου τα κρυπτογραφικά μοντέλα, μέθοδοι και συστήματα στηρίζονται σε διάφορες αλγεβρικές δομές όπως οι ημιομάδες, ομάδες και δακτύλιοι. Μια από τις πρώτες εφαρμογές μη-μεταθετικών αλγεβρικών δομών στην Κρυπτογραφία είναι και η χρήση ομάδων πλεξίδων στην ανάπτυξη πρωτοκόλλων. Αργότερα, πολλές άλλες μη-μεταθετικές δομές, όπως οι ομάδες Thompson, οι πολυκυκλικές ομάδες, οι ομάδες Grigorchuk και οι ομάδες πινάκων έχουν θεωρηθεί ως πιθανοί υποψήφιοι για χρήση στην κρυπτογραφία. Σε αντίθεση με τη μη-μεταθετική κρυπτογραφία, τα ευρέως διαδεδομένα κρυπτογραφικά μοντέλα δημοσίου κλειδιού, όπως το σύστημα RSA, η ανταλλαγή κλειδιών Diffie-Hellman και η κρυπτογραφία ελλειπτικών καμπυλών στηρίζονται στη θεωρία αριθμών και για τον λόγο αυτόν βασίζονται σε μεταθετικές αλγεβρικές δομές.

Τα διάφορα πρωτόκολλα μη-μεταθετικής κρυπτογραφίας έχουν αναπτυχθεί για την επίλυση διάφορων κρυπτογραφικών προβλημάτων όπως η ανταλλαγή κλειδιών, η κρυπτογράφηση και η αποκρυπτογράφηση, η πιστοποίηση κα. Τα πρωτόκολλα αυτά μοιάζουν κατά πολύ με τα αντίστοιχα της μεταθετικής Κρυπτογραφίας.

Στο Κεφάλαιο αυτό θα έχουμε τη δυνατότητα να συναντήσουμε διάφορα κρυπτογραφικά σχήματα που χρησιμοποιούν μη-μεταθετικές (ημί)ομάδες ως το μέσο, χωρίς να αποκλίνουν από τη μορφή των πρωτοκόλλων δημοσίου κλειδιού που στηρίζεται κυρίως σε συναρτήσεις μιας κατεύθυνσης.

Μεταξύ άλλων, θα δούμε μερικά πρωτόκολλα που φέρουν το πνεύμα των γνωστών μας μορφών που στηρίζονται στις μεταθετικές (ημί)ομάδες, αλλά και το ανατρεπτικό πρωτόκολλο των Anshel-Anshel-Goldfeld.

III.2
Το πρόβλημα αναζήτησης της συζυγίας και σχετικά πρωτόκολλα

Εισαγωγή

Ορισμός ΙΙΙ.1
Έστω μια ομάδα G με επιλύσιμο το πρόβλημα της λέξης. Για $w, n \in G$, η έκφραση w^n ισχύει για $n^{-1}wn$. Το πρόβλημα της συζυγίας (ή το πρόβλημα απόφασης της συζυγίας) είναι όταν για την ομάδα G έχουμε δύο στοιχεία $u, v \in G$ και θα πρέπει να αποφανθούμε εάν υπάρχει κάποιο $x \in G$ τέτοιο ώστε $u^x = v$. Από την άλλη, το πρόβλημα αναζήτησης της συζυγίας είναι όταν έχουμε δύο στοιχεία $a, b \in G$, γνωρίζουμε πως $u^x = v$ για κάποιο $x \in G$, και πρέπει να βρούμε ένα τουλάχιστον τέτοιο στοιχείο x. □

Το πρόβλημα απόφασης της συζυγίας έχει ιδιαίτερο ενδιαφέρον στη θεωρία ομάδων. Δεν ισχύει το ίδιο και για το πρόβλημα αναζήτησης της συζυγίας που αποκτά ενδιαφέρον στη θεωρία πολυπλοκότητας.

Όντως, εάν γνωρίζουμε πως το u είναι συζυγές προς το v, αρκεί να πάρουμε λέξεις της μορφής u^x και να τις συγκρίνουμε μια κάθε φορά με το v, μέχρι να βρούμε το ζητούμενο.

Παρατηρούμε ότι ο πλέον αναμενόμενος αλγόριθμος είναι τουλάχιστον εκθετικού χρόνου ως προς το μήκος του v και για τον λόγο αυτό θεωρείται ανέφικτος από πρακτική σκοπιά.

Οπότε, εάν δε γνωρίζουμε κάποιον άλλον αλγόριθμο για το πρόβλημα αναζήτησης της συζυγίας σε μια ομάδα G, δεν είναι παράλογο να ισχυριστούμε ότι η $x \to u^x$ είναι συνάρτηση μιας κατεύθυνσης και μπορούμε πάνω της να δομήσουμε ένα ολόκληρο κρυπτογραφικό πρωτόκολλο δημόσιου κλειδιού.

Θα δανειστούμε σε αυτό το σημείο ένα απλό πρωτόκολλο από τους Ko και Lee για το οποίο μπορούμε να ανατρέξουμε για περισσότερες πληροφορίες στη σχετική βιβλιογραφία [3].


Ki Hyoung Ko


Sang Jin Lee

Φωτογραφία ΙΙΙ.1

Πρωτόκολλο ΙΙΙ.1
Έτσι έχουμε:

1. Δημοσιεύεται ένα στοιχείο w ∈ G.
2. Η Alice επιλέγει ένα στοιχείο $a \in G$, που το γνωρίζει μόνον αυτή και στέλνει στον Bob το w^a.
3. Ο Bob επιλέγει ένα στοιχείο $b \in G$, που το γνωρίζει μόνον αυτός και στέλνει στην Alice το w^b.
4. Η Alice υπολογίζει το $(w^b)^\alpha = w^{ba}$ και ο Bob υπολογίζει το $(w^a)^b = w^{ab}$.

Εάν τα a και b έχουν επιλεχθεί από μια δεξαμενή μεταθετικών στοιχείων της ομάδα G, τότε $ab = ba$, και κατά συνέπεια η Alice και ο Bob θα λάβουν το ίδιο ιδιωτικό κλειδί $w^{ab} = w^{ba}$. □

Κανονικά, υπάρχουν δύο δημόσιες υποομάδες A και B της ομάδας G, που προκύπτουν από τα πεπερασμένα σύνολα γεννήτορες, τέτοια ώστε $ab = ba$ για κάθε $a \in A$, $b \in B$.

Στο [3], χρησιμοποιούμε την ομάδα πλεξίδων B_n, η οποία έχει κάποιες κανονικές μεταθετικές υποομάδες. Η επιλογή της σωστής ομάδας που θα χρησιμοποιήσουμε για το όλο πρωτόκολλο που περιγράφουμε είναι πάρα πολύ σημαντική. Μερικές προϋποθέσεις για την επιλογή, είναι και οι εξής:

a. Η ομάδα θα πρέπει να είναι γνωστή. Πιο συγκεκριμένα, το πρόβλημα αναζήτησης της συζυγίας στην ομάδα θα πρέπει να έχει μελετηθεί καλά ή να μπορεί να αναχθεί σε ένα ευρέως γνωστό πρόβλημα (πιθανών σε κάποιον άλλον τομέα των μαθηματικών).

   Η συγκεκριμένη προϋπόθεση, παρ' όλο που δεν είναι μαθηματικής φύσεως, είναι απαραίτητη εάν θέλουμε το κρυπτογραφικό μας προϊόν να έχει εφαρμογή στον πραγματικό κόσμο. Είναι εύκολο να

διαπιστώσουμε ότι με τη συγκεκριμένη προϋπόθεση, η λίστα των υποψήφιων ομάδων συρρικνώνεται σημαντικά.

b. Το πρόβλημα της λέξης στην ομάδα G θα πρέπει να έχει μια γρήγορη (γραμμικού ή τετραγωνικού χρόνου) λύση από έναν ντετερμινιστικό αλγόριθμο. Ακόμη καλύτερα, θα πρέπει να υπάρχει μια αποτελεσματική υπολογίσιμη «κανονική μορφή» για τα στοιχεία της G.

   Αυτό είναι απαραίτητο για να εξάγουμε με αποτελεσματικό τρόπο τα κλειδιά απ' όλες τις πιστοποιημένες πλευρές στην εφαρμογή ενός πρωτόκολλου κλειδιών ή στο βήμα επιβεβαίωσης ενός πρωτοκόλλου πιστοποίησης.

c. Το πρόβλημα αναζήτησης της συζυγίας δεν θα πρέπει να έχει μια υπό-εκθετικού χρόνου λύση που θα μας δίνει κάποιος ντετερμινιστικός αλγόριθμος.

   Στο σημείο αυτό θα πρέπει να αναφέρουμε ότι η διαδικασία απόδειξης πως μια ομάδα έχει την προϋπόθεση (c) θα πρέπει να είναι υπερβολικά δύσκολη, για να μην πούμε αδύνατη. Στην κυριολεξία, πρόκειται για ένα πρόβλημα του ενός εκατομμυρίου δολαρίου [29]. Κατά συνέπεια θα πρέπει να λαμβάνουμε υπ' όψιν μας την προϋπόθεση (c) μαζί με την προϋπόθεση (a). Για παράδειγμα, η μόνη απτή ένδειξη ότι η ομάδα G έχει την ιδιότητα (c) είναι το γεγονός ότι το πρόβλημα αναζήτησης της συζυγίας στην ομάδα G έχει ήδη μελετηθεί από αρκετούς ανθρώπους για αρκετά μεγάλο χρονικό διάστημα.

   Η επόμενη ιδιότητα είναι ελαφρώς άτυπη, όμως είναι μεγάλης σημασίας για διάφορες πρακτικές εφαρμογές.

d. Θα πρέπει να υπάρχει κάποιος τρόπος να αποκρύψουμε τα στοιχεία της G έτσι ώστε να είναι ακατόρθωτο να επανακτήσουμε το x από το $x^{-1}wx$ με απλή παρατήρηση.

   Ένας τρόπος για να το πετύχουμε είναι να έχουμε μια κανονική μορφή για τα στοιχεία της G, κάτι που σημαίνει ότι υπάρχει ένας αλγόριθμος που θα μπορούσε να μετατρέψει κάθε είσοδο u_{in}, που είναι μια λέξη στους γεννήτορες της G, σε μια έξοδο u_{out}, που είναι επίσης μια άλλη λέξη στους γεννήτορες της G, τέτοιος ώστε να ισχύει $u_{in} = u_{out}$ στην ομάδα G. Δυστυχώς όμως, κάτι τέτοιο είναι δύσκολο να το εντοπίσουμε με απλή παρατήρηση.

Εάν δεν έχουμε μια τέτοια κανονική μορφή, και γνωρίζουμε την G μόνον από τους γεννήτορες και τις σχέσεις που συνεπάγονται, χωρίς καμία περαιτέρω πληροφορία σχετική με τις ιδιότητες της G, τότε τουλάχιστον κάποιες από τις προαναφερθείσες σχέσεις θα πρέπει να είναι ιδιαιτέρως βραχείες.

e. Η ομάδα G θα πρέπει να είναι υπέρ-πολυωνυμικής (π.χ. εκθετικής) ανάπτυξης. Αυτό σημαίνει πως ο αριθμός των στοιχείων μήκους n στην G θα πρέπει να αυξάνει πιο γρήγορα από κάθε άλλο πολυώνυμο στο n. Αυτό είναι απαραίτητο για να αποφευχθούν επιθέσεις που αποσκοπούν στην πλήρη εξάντληση του χώρου του κλειδιού. Στην περίπτωσή μας, με τον όρο «μήκος n», εννοούμε το μήκος μια λέξης που αντιπροσωπεύει ένα στοιχείο της ομάδας. Όμως, σε μια γενικότερη κατάσταση, αυτό θα μπορούσε να είναι και το μήκος κάποιας άλλης περιγραφής, όπως της πληροφορίας που σχετίζεται με την πολυπλοκότητα.

Υπάρχουν ομάδες στις οποίες θα μπορούσαμε να συναντήσουμε τις προϋποθέσεις (b), (e), πιθανών τη (c) και υπό κάποιες λογικές προεκτάσεις να έχουν και τη (d). Όλες αυτές οι ομάδες έχουν επιλύσιμο το πρόβλημα της λέξης, αλλά μη επιλύσιμο το πρόβλημα της συζυγίας. Περισσότερα μπορείτε να διαβάσετε στο [30].

Ολοκληρώνοντας, θα θέλαμε να πούμε ότι το πρόβλημα αναζήτησης της συζυγίας δεν έχει κάποιο ξεχωριστό ενδιαφέρον στη θεωρία ομάδων. Από τη στιγμή που αποδείχθηκε ότι το πρόβλημα της συζυγίας δεν έχει κάποια αλγοριθμική λύση, όλοι όσοι ασχολούνται με τη θεωρία ομάδων σταμάτησαν να μελετούν το πρόβλημα αναζήτησης της συζυγίας στις προαναφερθείσες ομάδες.

III.3
Το πρόβλημα της διάσπασης και σχετικά πρωτόκολλα

Εισαγωγή

Θα μπορούσαμε να πούμε πως μια από τις φυσικές διακλαδώσεις του προβλήματος αναζήτησης της συζυγίας (γενικευμένη εκδοχή του) είναι και το ακόλουθο πρόβλημα αναζήτησης της διάσπασης:

Ορισμός ΙΙΙ.2
Έστω ότι έχουμε μια ομάδα G και δύο στοιχεία της, τα w, w'. Επίσης, έστω ότι $A \subseteq G$. Δεδομένου ότι υπάρχει, να βρεθεί ένα ζεύγος στοιχείων $x, y \in A$, τέτοιο ώστε $xwy = w$'. □

Ορισμός ΙΙΙ.3
Στην περίπτωση που το σύνολο A είναι υποομάδα της G, τότε το πρόβλημα αποκαλείται και πρόβλημα του διπλού συμπλόκου. □

Να παρατηρήσουμε σε αυτό το σημείο ότι πάντα υπάρχουν κάποια x και y που να ικανοποιούν την εξίσωση $x \cdot w \cdot y = w$' (π.χ. $x = 1$, $y = w^{-1}w'$). Οπότε το ζητούμενο είναι να ικανοποιούν τη συνθήκη $x, y \in A$. Είναι προφανές ότι η λύση που ζητάμε θα βρίσκεται πάντα ανάμεσα στις υποομάδες της G.

Μπορεί να αποδειχθεί ότι η επίλυση του προβλήματος αναζήτησης της συζυγίας στο οποίο βασίζεται το πρωτόκολλο των Ko και Lee κ.α., μπορεί να αναχθεί σε πρόβλημα αναζήτησης της διάσπασης [3].

Να σημειώσουμε σε αυτό το σημείο ότι η συνθήκη $x, y \in A$ μπορεί να μην είναι εύκολο να επαληθευθεί για ορισμένα υποσύνολα A. Η προαναφερθείσα δυσκολία επαλήθευσης είναι επίσης γνωστή και ως πρόβλημα απόφασης του μέλους. Οι συγγραφείς του [3] δεν κάνουν αναφορά σε αυτή τη δυσκολία. Αντί αυτού, ισχυρίζονται ότι εάν κάποιος χρησιμοποιήσει «brute force» επίθεση πάνω στα στοιχεία του A (σε ένα κάθε φορά), η πιο πάνω συνθήκη θα ικανοποιηθεί αυτόματα. Όμως αυτό δεν ισχύει για άλλες πιο πρακτικές επιθέσεις.

Επίσης, πρέπει να επισημάνουμε ότι το πρόβλημα αναζήτησης της συζυγίας αποτελεί ειδική περίπτωση του προβλήματος της διάσπασης, όπου το w' είναι συζυγές προς το w και $x = y^{-1}$. Είναι προφανές ότι ο ισχυρισμός πως το πρόβλημα της διάσπασης είναι ευκολότερο από το πρόβλημα αναζήτησης της συζυγίας πρέπει να ισχύει, καθότι γενικά είναι ευκολότερο να επιλύσουμε μια εξίσωση με δύο αγνώστους, παρά μια ειδική περίπτωση της ίδιας εξίσωσης με έναν άγνωστο. Φυσικά, και σε αυτήν την περίπτωση, υπάρχουν εξαιρέσεις στον κανόνα.

Πρωτόκολλο ΙΙΙ.2

Τώρα θα δούμε μια αυστηρή περιγραφή ενός τυπικού πρωτοκόλλου που βασίζεται στον πρόβλημα της διάσπασης. Έστω ότι έχουμε μια δημόσια ομάδα G και δύο δημόσιες υποομάδες $A, B \subseteq G$ με μεταθετικά στοιχεία, π.χ. $ab = ba$ για κάθε $a \in A$, $b \in B$. Τότε:

1. Η Alice θα επιλέξει τυχαία τα ιδιωτικά στοιχεία $a_1, a_2 \in A$. Στη συνέχεια θα στείλει στον Bob το στοιχείο $a_1 w a_2$.

2. Ο Bob θα επιλέξει τυχαία τα ιδιωτικά στοιχεία $b_1, b_2 \in B$. Στη συνέχεια θα στείλει στην Alice το στοιχείο $b_1 w b_2$.

3. Η Alice θα υπολογίσει το $K_A = a_1 b_1 w b_2 a_2$ και ο Bob θα υπολογίσει το $K_B = b_2 a_1 w b_1 a_2$. Καθότι ισχύει πως $a_i b_i = b_i a_i$ στη G, κάποιος μπορεί να πάρει $K_A = K_B = K$ (ως στοιχείο της G), το οποίο και θα αποτελέσει το κοινό μυστικό κλειδί των Alice και του Bob.

□

III.3.1 Μια παραλλαγή - Twisted πρωτόκολλο

Πιο κάτω θα αναλύσουμε μια ιδέα που την οφείλουμε στους Shpilrain και Ushakov [31]. Ύστερα από προσομοιώσεις σε υπολογιστές, μπορούμε να πούμε με σιγουριά ότι πρόκειται για μια πιο ασφαλή παραλλαγή (σε αρκετές περιπτώσεις) του πιο πάνω αναλυθέντος πρωτοκόλλου προβλήματος της διάσπασης, εναντίον επιθέσεων που εκμεταλλεύονται αδυναμίες ως προς το μήκος.


Vladimir Shpilrain


Alexander Ushakov

Φωτογραφία III.2

Πρωτόκολλο III.3

Έτσι έχουμε:

1. Έστω ότι υπάρχει μια δημόσια ομάδα G και δύο δημόσιες υποομάδες $A, B \subseteq G$ με μεταθετικά στοιχεία.

2. Η Alice θα επιλέξει τυχαία τα ιδιωτικά στοιχεία $a_1 \in A$ και $b_1 \in B$. Στη συνέχεια θα στείλει στον Bob το στοιχείο $a_1 w b_1$.

3. Ο Bob θα επιλέξει τυχαία τα ιδιωτικά στοιχεία $b_2 \in B$ και $a_2 \in A$. Στη συνέχεια θα στείλει στην Alice το στοιχείο $b_2 w a_2$.

4. Η Alice θα υπολογίσει το $K_A = a_1 b_2 w a_2 b_1 = b_2 a_1 w b_1 a_2$ και ο Bob θα υπολογίσει το $K_B = b_2 a_1 w b_1 a_2$. Καθότι ισχύει πως $a_i b_i = b_i a_i$ στη G, κάποιος μπορεί να πάρει $K_A = K_B = K$ (ως στοιχείο της G), το οποίο και θα αποτελέσει το κοινό μυστικό κλειδί των Alice και Bob.

□

Είναι προφανές ότι η ασφάλεια του πιο πάνω πρωτοκόλλου στηρίζεται σε μια γενικότερη εκδοχή του προβλήματος αναζήτησης της διάσπασης, διαφορετική από την αρχική που αναλύσαμε. Έτσι:

Έστω ότι έχουμε δύο στοιχεία w, w' και δύο υποομάδες $A, B \subseteq G$. Δεδομένου ότι υπάρχει, θέλουμε να βρούμε ένα ζεύγος στοιχείων $x \in A$ και $y \in B$ τέτοια ώστε $x \cdot w \cdot y = w'$.

III.3.2 Αποκρύπτοντας μια από τις υποομάδες

Πρόκειται για άλλη μια ιδέα που την οφείλουμε στους Shpilrain και Ushakov [32]. Ας πάρουμε μια πρόγευση της όλης ιδέας.

Πρωτόκολλο III.4
Έστω ότι έχουμε μια ομάδα G και $g \in G$. Θα συμβολίσουμε με $C_{G(g)}$ τον κεντροποιητή της g στο G, π.χ. το σύνολο των στοιχείων $h \in G$ τέτοιο ώστε $hg = gh$. Για $S = \{g_1, \dots, g_k\} \subseteq G$, το $C_G(g_1, \dots, g_k)$ εκφράζει τον κεντροποιητή του S στη G, που είναι η τομή των κεντροποιητών $C_{G(g_i)}$, με $i = 1, \dots, k$.

1. Έστω τώρα ότι έχουμε ένα δημόσιο $w \in G$.

2. Η Alice θα επιλέξει ένα ιδιωτικό $a_1 \in G$ και θα δημοσιεύσει ένα υποσύνολο $B \subseteq C_{G(a_1)}$ (υποθέτοντας ότι το B μπορεί να υπολογιστεί αποτελεσματικά).

3. Κατά τον ίδιον τρόπο, ο Bob θα επιλέξει ένα ιδιωτικό $b_2 \in G$ και θα δημοσιεύσει μια υποομάδα $A \subseteq C_{G(b_2)}$.

4. Στη συνέχεια, η Alice θα επιλέξει $a_2 \in A$ και θα στείλει στον Bob το $w_1 = a_1 w a_2$, ενώ ο Bob επιλέγει το $b_1 \in B$ και στέλνει στην Alice το $w_2 = b_1 w b_2$.

□

Έτσι, στην πρώτη επικοινωνία, ο επιτιθέμενος θα δυσκολευτεί να βρει τα a_1, a_2, τέτοια ώστε $w_1 = a_1 w a_2$, όπου $a_2 \in A$, χωρίς όμως να υπάρχει κάποια ιδιαίτερη επισήμανση ως προς το από πού πρέπει να επιλέξουμε το a_1. Οπότε, πριν προβεί σε κάποια επίθεση, όπως αυτές που βασίζονται στο μήκος, ο επιτιθέμενος θα πρέπει πρώτα να υπολογίσει τους γεννήτορες του κεντροποιητή $C_G(B)$ (επειδή $a_1 \in C_G(B)$), κάτι που είναι συνήθως από μόνο του ένα δύσκολο πρόβλημα.

Η δυσκολία οφείλεται στο ότι πρέπει να βρούμε την τομή των κεντροποιητών των μεμονωμένων στοιχείων και το γεγονός αυτό, δηλαδή η εύρεση (των γεννητόρων) της τομής των υποομάδων αποτελούν ένα ιδιαιτέρως δύσκολο πρόβλημα για τις περισσότερες ομάδες που αναφέρονται στη θεωρία συνδυαστικών ομάδων.

Πρωτόκολλο ΙΙΙ.5

Ας δούμε όμως και μια πιο αυστηρή περιγραφή του πρωτοκόλλου όπως αυτή περιγράφεται στο [32]. Έτσι, έχουμε:

1. Έστω ότι έχουμε μια δημόσια ομάδα G κι ένα δημόσιο $w \in G$.

2. Η Alice θα επιλέξει ένα στοιχείο $a_1 \in G$ και μια υποομάδα του $C_G(a_1)$ και στη συνέχεια θα δημοσιεύσει τους γεννήτορες $A = \{ a_1, \dots, a_k\}$.

3. Ο Bob θα επιλέξει ένα στοιχείο $b_2 \in G$ και μια υποομάδα του $C_G(b_2)$ και στη συνέχεια θα δημοσιεύσει τους γεννήτορες $B = \{ b_1, \dots, b_m\}$.

4. Η Alice θα επιλέξει ένα τυχαίο στοιχείο a_2 από τα $\langle b_1, \dots, b_m \rangle$ και θα στείλει στον Bob το $P_A = a_1 w a_2$.

5. Ο Bob θα επιλέξει ένα τυχαίο στοιχείο b_1 από τα $\langle a_1, \dots, a_k \rangle$ και θα στείλει στην Alice το $P_B = b_1 w b_2$.

6. Η Alice θα υπολογίσει το $K_A = a_1 P_B a_2$.

7. Ο Bob θα υπολογίσει το $K_B = b_1 P_A b_2$.

Όμως, επειδή ισχύει $a_1 b_1 = b_1 a_1$ και $a_2 b_2 = b_2 a_2$, θα έχουμε $K = K_A = K_B$, που θα είναι το κοινό μυστικό κλειδί.

□

ΙΙΙ.3.3 Το πρόβλημα της τριπλής διάσπασης

Το ακόλουθο πρωτόκολλο το οφείλουμε στην Kurt [33]. Η ιδέα της ήταν να εναποθέσει την ασφάλεια των αρχών ανταλλαγής κλειδιών στο πρόβλημα της τριπλής διάσπασης. Πρόκειται για την περίπτωση στην οποία ένα γνωστό στοιχείο θα παραγοντοποιηθεί σε γινόμενο τριών άγνωστων παραγόντων. Σε αυτό το σημείο ας θυμηθούμε ότι στην περίπτωση του συνηθισμένου προβλήματος της διάσπασης που μελετήσαμε, ένα γνωστό στοιχείο θα παραγοντοποιηθεί σε γινόμενο τριών παραγόντων, εκ των οποίων οι δύο είναι άγνωστοι κι ο τρίτος (ο μεσαίος) γνωστός. Ποιος όμως ο λόγος να χρησιμοποιήσουμε την τροποποιημένη εκδοχή της τριπλής διάσπασης; Ας δούμε την πιο κάτω περίπτωση και θα καταλάβουμε.

Yeşem Kurt

Φωτογραφία ΙΙΙ.3

Αν η ομάδα που θα χρησιμοποιηθεί για το συγκεκριμένο πρωτόκολλο είναι γραμμική, τότε η συνηθισμένη εκδοχή του προβλήματος της διάσπασης μπορεί να αναχθεί σε ένα σύστημα γραμμικών εξισώσεων, κάνοντας εφικτή μια επίθεση που θα έχει ως βάση τη γραμμική άλγεβρα. Με το πρόβλημα της τριπλής διάσπασης μπορούμε να κάνουμε ακόμη πιο δύσκολο το έργο των επιτιθέμενων, καθότι αν προσπαθήσουν να κάνουν την ίδια αναγωγή, θα πάρουν ένα σύστημα τετραγωνικών εξισώσεων, κάτι που όπως είναι αυτονόητο είναι λιγότερο ευάλωτο σε συνήθεις επιθέσεις.

Στο πρωτόκολλο της Kurt, το ιδιωτικό κλειδί έχει τρία συστατικά μέρη. Η όλη ιδέα έγκειται στο να κρύψουμε κάθε ένα από αυτά τα μέρη με το να τα πολλαπλασιάσουμε με τυχαία στοιχεία μιας δημόσιας υποομάδας. Είναι αξιοσημείωτο να αναφέρουμε πως ένα από τα μέρη θα πολλαπλασιαστεί με τυχαία στοιχεία κι από τις δύο πλευρές, δηλαδή κι από δεξιά κι από αριστερά. Ας δούμε τώρα την υπόλοιπη περιγραφή του πρωτοκόλλου. Έτσι:

Πρωτόκολλο ΙΙΙ.6

Έστω ότι έχουμε μια δημόσια ομάδα G (μονοειδές) που θα χρησιμοποιήσουμε, και δύο σύνολα υποσυνόλων της G, που το κάθε ένα θα περιλαμβάνει πέντε υποσύνολα της G, έστω τα:

$$A = A_1, A_2, A_3, X_1, X_2 \text{ και } B = B_1, B_2, B_3, Y_1, Y_2$$

που ικανοποιούν τις ακόλουθες συνθήκες της αντιστρεψιμότητας και της μεταθετικότητας:

Αντιστρεψιμότητα: Τα στοιχεία των X_1, X_2, Y_1, Y_2 είναι αντιστρέψιμα.

Μεταθετικότητα: $[A_2, Y_1] = 1$, $[A_3, Y_2] = 1$, $[B_1, X_1] = 1$ και $[B_2, X_2] = 1$.

Η Alice και ο Bob συμφωνούν ως προς το ποιο σύνολο υποσυνόλων θα χρησιμοποιήσει ο καθένας. Έτσι, έστω ότι η Alice χρησιμοποιεί το A και ο Bob το B. Τότε η ανταλλαγή που θα ακολουθήσει μεταξύ των Alice και Bob θα είναι η ακόλουθη:

1. Η Alice θα επιλέξει τα $\alpha_1 \in A_1, \alpha_2 \in A_2, \alpha_3 \in A_3, x_1 \in X_1, x_2 \in X_2$ και θα υπολογίσει τα $u = \alpha_1 x_1$, $v = {x_1}^{-1} a_2 x_2$ και $w = {x_2}^{-1} a_3$. Οπότε το ιδιωτικό της κλειδί θα είναι $(\alpha_1, \alpha_2, \alpha_3)$.

2. Ο Bob θα επιλέξει τα $b_1 \in B_1, b_2 \in B_2, b_3 \in B_3, y_1 \in Y_1, y_2 \in Y_2$ και θα υπολογίσει τα $p = b_1 y_1$, $q = {y_1}^{-1} b_2 y_2$ και $r = {y_2}^{-1} b_3$. Οπότε το ιδιωτικό του κλειδί θα είναι (b_1, b_2, b_3).

3. Η Alice θα στείλει στον Bob το (u, v, w).

4. Ο Bob θα στείλει στην Alice το (p, q, r).

5. Η Alice θα υπολογίσει το:
$$\alpha_1 p \alpha_2 q \alpha_3 r = \alpha_1 (b_1 y_1) \alpha_2 ({y_1}^{-1} b_2 y_2) \alpha_3 ({y_2}^{-1} b_3) = \alpha_1 b_1 \alpha_2 b_2 \alpha_3 b_3 = K_A$$

6. Ο Bob θα υπολογίσει το:
$$u b_1 v b_2 w b_3 = (a_1 x_1) b_1 ({x_1}^{-1} a_2 x_2) b_2 ({x_2}^{-1} a_3) b_3 = \alpha_1 b_1 \alpha_2 b_2 \alpha_3 b_3 = K_B$$

Οπότε, καθότι ισχύει $K_A = K_B = K$, αυτό θα είναι και το κοινό μυστικό κλειδί των Alice και Bob. Για περισσότερες πληροφορίες σχετικά με το όλο πρωτόκολλο και το σχήμα λειτουργίας του, μπορούμε να ανατρέξουμε στο [33]. □

III.4
Το πρόβλημα της παραγοντοποίησης και το σχετικό πρωτόκολλο

Εισαγωγή

Πιο κάτω θα έχουμε την ευκαιρία να δούμε ένα πρωτόκολλο που βασίζεται στο πρόβλημα αναζήτησης της παραγοντοποίησης, που είναι:

Πρόβλημα αναζήτησης της παραγοντοποίησης

Ορισμός III.4
Έστω ότι έχουμε ένα στοιχείο w από μια ομάδα G καθώς και δύο υποομάδες $A, B \leq G$. Θέλουμε να βρούμε δύο στοιχεία $a \in A$ και $b \in B$ που να ικανοποιούν τη $a \cdot b = w$.

Πρωτόκολλο III.7

Ας αφιερώσουμε λίγο χρόνο και στο πρωτόκολλο.

Έστω ότι έχουμε μια δημόσια ομάδα G, και δύο δημόσιες υποομάδες $A, B \leq G$ με μεταθετικότητα στοιχείων, π.χ. $ab = ba$ για κάθε $a \in A$, $b \in B$.

Τότε:

1. Η Alice θα επιλέξει τυχαία τα ιδιωτικά της στοιχεία $\alpha_1 \in A$, $b_1 \in B$ και θα στείλει στον Bob το στοιχείο $\alpha_1 b_1$.

2. Ο Bob θα επιλέξει τυχαία τα ιδιωτικά του στοιχεία $\alpha_2 \in A$, $b_2 \in B$ και θα στείλει στην Alice το στοιχείο $\alpha_2 b_2$.

3. Η Alice θα υπολογίσει το:

$$K_A = b_1(\alpha_2 b_2)a_1 = a_2 b_1 a_1 b_2 = a_2 a_1 b_1 b_2$$

4. Ο Bob θα υπολογίσει το:

$$K_B = a_2(\alpha_1 b_1)b_2 = a_2 a_1 b_1 b_2$$

Καθότι $K_A = K_B = K$, αυτό θα είναι και το κοινό μυστικό κλειδί των Alice και Bob. □

Θα πρέπει να σημειώσουμε σε αυτό το σημείο ότι ο επιτιθέμενος γνωρίζει τα στοιχεία $\alpha_1 b_1$ και $\alpha_2 b_2$, οπότε και μπορεί να υπολογίσει τα:

$$(\alpha_1 b_1)(\alpha_2 b_2) = \alpha_1 b_1 \alpha_2 b_2 = \alpha_1 \alpha_2 b_1 b_2 \text{ και } (\alpha_2 b_2)(\alpha_1 b_1) = \alpha_2 \alpha_1 b_2 b_1.$$

Όμως, αν $\alpha_1 \alpha_2 \neq \alpha_2 \alpha_1$ και $b_1 b_2 \neq b_2 b_1$, τότε κανένα από αυτά τα γινόμενα δεν είναι ίσο με το K.

Πρόβλημα απόφασης

Έτσι καταλήγουμε και στο πρόβλημα απόφασης για την παραγοντοποίηση:

Ορισμός ΙΙΙ.5
Έστω ότι έχουμε ένα στοιχείο w από μια ομάδα G καθώς και δύο υποομάδες $A, B \leq G$. Θέλουμε να βρούμε εάν υπάρχουν ή όχι δύο στοιχεία $a \in A$ και $b \in B$ που να ικανοποιούν τη $a \cdot b = w$. □

Όπως φαίνεται πρόκειται για ένα καινούργιο και μη τετριμμένο πρόβλημα στη θεωρία ομάδων που προτείνεται από την κρυπτογραφία. Άλλωστε αποτελεί κοινό μυστικό πως έχουμε μια αξιοσημείωτη, σχετική προς το πρόβλημα, ροή πληροφοριών από την κρυπτογραφία προς τη θεωρία ομάδων.

III.5
Το πρωτόκολλο ανταλλαγής κλειδιού του Stickel

Εισαγωγή

Το πρωτόκολλο του Stickel, όπως αυτό περιγράφεται στο [34], μας θυμίζει το κλασσικό πρωτόκολλο των Diffie-Hellman-Merkle, παρ' όλο που επίσημα δεν πρόκειται για κάποια γενίκευση του. Όπως θα δούμε και στην επόμενη ενότητα των αλγεβρικών επιθέσεων, η επιλογή που κάνει ο Stickel με το να χρησιμοποιήσει την ομάδα των αντιστρέψιμων πινάκων πάνω σε ένα πεπερασμένο πεδίο, καθιστά το πρωτόκολλο ευάλωτο στις επιθέσεις γραμμικής άλγεβρας.

Όπως αντιλαμβάνεται κανείς, ακόμη και με μια τόσο μικρή παραλλαγή (βελτίωση), δηλαδή τη χρήση μη-αντιστρέψιμων πινάκων αντί των αντιστρέψιμων, μπορούμε να κάνουμε το πρωτόκολλο του Stickel πιο ανθεκτικό, και ειδικότερα στις επιθέσεις γραμμικής άλγεβρας. Για τον λόγο αυτόν θεωρούμε ότι το συγκεκριμένο πρωτόκολλο θα μπορούσε να έχει κάποιες προοπτικές. Η πιο κάτω περιγραφή που ακολουθεί στηρίζεται στο [35].

Πρωτόκολλο III.8

Έστω ότι έχουμε μια δημόσια μη-αβελιανή πεπερασμένη ομάδα G και δύο δημόσια στοιχεία $a, b \in G$, τέτοια ώστε $ab \neq ba$. Το πρωτόκολλο ανταλλαγής κλειδιών αναπτύσσεται ως εξής:

1. Έστω N και M οι τάξεις των a και b αντίστοιχα, όπου τάξη ενός στοιχείου g μιας ομάδας G, ονομάζεται ο μικρότερος θετικός ακέραιος n για τον οποίον ισχύει n: $g^n = e$ (όπου e το ταυτοτικό στοιχείο).

2. Η Alice θα επιλέξει δύο τυχαίους φυσικούς αριθμούς $n < N, m < M$ και θα στείλει στον Bob το $u = a^n b^m$.

3. Ο Bob θα επιλέξει δύο τυχαίους φυσικούς αριθμούς $r < N, s < M$ και θα στείλει στην Alice το $v = a^r b^r$.

4. Η Alice θα υπολογίσει το $K_A = a^n v b^m = a^{n+r} b^{m+s}$.

5. Ο Bob θα υπολογίσει το $K_B = a^r u b^s = a^{n+r} b^{m+s}$.

Κατά συνέπεια, οι Alice και Bob θα καταλήξουν με το ίδιο στοιχείο της ομάδας $K = K_A = K_B$, το οποίο και θα λειτουργήσει ως το κοινό μυστικό κλειδί. □

Όμως, όταν περάσουμε από τη θεωρία στην εφαρμογή, η περιγραφή που γίνεται στο [34] δεν είναι και τόσο ξεκάθαρη. Συγκεκριμένα, για κάποιον λόγο ο συγγραφέας προτιμάει την ακόλουθη πιο γενική εκδοχή του παραπάνω πρωτοκόλλου:

Πρωτόκολλο ΙΙΙ.9

1. Έστω ότι έχουμε το δημόσιο $w \in G$.

2. Η Alice θα επιλέξει δύο τυχαίους φυσικούς αριθμούς $n < N$, $m < M$, ένα στοιχείο c_1 από το κέντρο της ομάδας G και θα στείλει στον Bob το $u = c_1 a^n w b^m$.

3. Ο Bob θα επιλέξει δύο τυχαίους φυσικούς αριθμούς $r < N$, $s < M$, ένα στοιχείο c_2 από το κέντρο της ομάδας G και θα στείλει στην Alice το $v = c_2 a^r w b^s$.

4. Η Alice θα υπολογίσει το $K_A = c_1 a^n v b^m = c_1 c_2 a^{n+r} w b^{m+s}$.

5. Ο Bob θα υπολογίσει το $K_B = c_2 a^r u b^s = c_1 c_2 a^{n+r} w b^{m+s}$.

Οπότε οι Alice και Bob θα καταλήξουν με το ίδιο στοιχείο της ομάδας $K = K_A = K_B$. □

Παρατηρούμε ότι για να λειτουργήσει το πιο πάνω πρωτόκολλο, δε χρειάζεται το G να είναι κάποια ομάδα. Ακόμη και μια υποομάδα θα μπορούσε να κάνει την ίδια δουλειά, ίσως και καλύτερα.

Επιθέσεις

Στο [34] διαβάζουμε πως χρησιμοποιούμε την ομάδα των αντιστρέψιμων πινάκων $k \times k$ πάνω σε ένα πεπερασμένο πεδίο F_{2^l}. Στην επόμενη ενότητα των αλγεβρικών επιθέσεων θα δούμε πως αν επιλέξουμε την προαναφερθείσα ομάδα, το πρωτόκολλο θα γίνει ευάλωτο στις επιθέσεις γραμμικής άλγεβρας.

Όμως πρώτα, ας πάρουμε μια γενικότερη εικόνα για τον τρόπο επίθεσης στο πρωτόκολλο του Stickel.

Όπως είπαμε, η Alice στέλνει στον Bob το $u = c_1 a^n w b^m$.

Παρατηρούμε πως εάν στο τέλος μείνουμε στο κοινό μυστικό κλειδί K, αυτό θα ήταν αρκετό για τον επιτιθέμενο να βρει κάποια στοιχεία $x, y \in G$, τέτοια ώστε να έχουμε $xa = ax$, $yb = by$, $u = xwy$.

Όντως, αν ο επιτιθέμενος βρει τα προαναφερθέντα x, y, θα μπορεί να χρησιμοποιήσει το μήνυμα $v = c_2 a^r w b^s$ του Bob, για να κάνει τον ακόλουθο υπολογισμό:

$$xvy = xc_2 a^r w b^s y = v = c_2 a^r xwyb^s = v = c_2 a^r u b^s = K$$

Έτσι καταλήγουμε στο συμπέρασμα πως ο πολλαπλασιασμός με το c_i, δεν αυξάνει την ασφάλεια του πρωτοκόλλου. Επιπροσθέτως, ο επιτιθέμενος δε χρειάζεται να ανακτήσει κάποιον από τους εκθέτες n, m, r, s. Το μόνο που χρειάζεται να κάνει είναι να λύσει το σύστημα εξισώσεων $xa = ax$, $yb = by$, $u = xwy$, όπου τα a, b, u, w είναι γνωστά και τα x, y είναι άγνωστα στοιχεία της (ημί)ομάδας G. Η τελευταία μας παρατήρηση μας υποδεικνύει ότι το πρωτόκολλο του Stickel αποκλίνει από το πρωτόκολλο των Diffie-Hellman-Merkle περισσότερο απ' ότι νομίζαμε.

Επίσης, να σημειώσουμε σε αυτό το σημείο ότι η επίλυση του πιο πάνω συστήματος εξισώσεων στη G, είναι το ίδιο σαν να επιλύουμε το πρόβλημα αναζήτησης της διάσπασης για υπό-ημί-ομάδα (sub-semigroup). Ας δούμε τον ορισμό για να το καταλάβουμε καλύτερα:

<u>Ορισμός ΙΙΙ.6</u>
Έστω ότι έχουμε μια (ημί)ομάδα G, που παριστάνεται αναδρομικά, δύο αναδρομικώς παραγόμενες υπό(ημί)ομάδες $A, B \leq G$ και δύο στοιχεία $u, w \in G$. Δεδομένου ότι υπάρχει, βρείτε ένα ζεύγος στοιχείων $x \in A$ και $y \in B$ που θα μπορούσαν να ικανοποιήσουν τη $x \cdot w \cdot y = u$. □

Στην περίπτωση του πρωτοκόλλου του Stickel, οι υπό(ημί)ομάδες A και B είναι οι κεντροποιητές των στοιχείων a και b αντιστοίχως. Ο κεντροποιητής ενός στοιχείου $g \in G$ είναι το σύνολο όλων των στοιχείων $c \in G$, τέτοιων ώστε $gc = cg$. Το σύνολο αυτό είναι μια υπό-ημί-ομάδα της G. Εάν η G είναι ομάδα, τότε το προαναφερθέν σύνολο είναι υποομάδα.

Κλείνοντας, να αναφέρουμε ότι καμία ημί-ομάδα δε φαίνεται να παρέχει έναν ασφαλή τρόπο λειτουργίας για κάποιο από τα πρωτόκολλα που στηρίζονται στο πρόβλημα αναζήτησης της διάσπασης. Παρ' όλα αυτά, πιστεύουμε ότι

κάποιες ημί-ομάδες πινάκων πάνω σε συγκεκριμένους δακτυλίους, μπορούν να δώσουν κάποιες καλές λύσεις. Ο Sramka στο [36] δίνει μια καλή επίθεση, στην οποία είναι εφικτή η ανάκτηση ενός από τους εκθέτες n, m, r, s.

III.6
Επίθεση μέσω Γραμμικής Άλγεβρας

Εισαγωγή

Στην προηγούμενη ενότητα είδαμε την ομάδα G που πρότεινε ο Stickel στο πρωτόκολλό του και κάναμε λόγο για επιθέσεις γραμμικής άλγεβρας. Στο έργο του [34], η ομάδα G είναι η ομάδα των αντιστρέψιμων πινάκων $k \times k$ πάνω σε ένα πεπερασμένο πεδίο F_{2^l}, όπου $k = 31$. Αν και το έργο [34] δεν κάνει ιδιαίτερη μνεία στην παράμετρο l, είναι λογικό να υποθέσουμε ότι ισχύει $2 \leq l \leq k$. Η επιλογή των πινάκων a, b, w δεν παίζει σημαντικό ρόλο για την επίθεση που θα περιγράψουμε. Το σημαντικό είναι τα a και b να είναι αντιστρέψιμα. Να σημειώσουμε σε αυτό το σημείο ότι η επιλογή των a και b που γίνεται στο [34] (και πιο συγκεκριμένα, το γεγονός ότι η είσοδος σε αυτούς τους πίνακες είναι 0 ή 1) καθιστούν το πρωτόκολλο ακόμη πιο ευάλωτο όπως θα δούμε και πιο κάτω.

Πρωτόκολλο III.10
Να θυμηθούμε σε αυτό το σημείο ότι αρκεί ο επιτιθέμενος να βρει τουλάχιστον μια λύση του συστήματος εξισώσεων $xa = ax,\ yb = by,$ $u = xwy$, όπου τα a, b, u, w είναι γνωστά και τα x, y άγνωστοι πίνακες $k \times k$ πάνω στο F_{2^l}.

Κάθε μια από τις πρώτες δύο εξισώσεις του συστήματος μπορεί να μετατραπεί σε ένα σύστημα k^2 γραμμικών εξισώσεων για τα άγνωστα στοιχεία που παίρνουμε στην είσοδο των πινάκων x και y. Όμως, η εξίσωση $u = xwy$ δε μπορεί να μετατραπεί σε ένα σύστημα γραμμικών εξισώσεων ως προς τα στοιχεία της εισόδου, επειδή πρόκειται για το γινόμενο δύο άγνωστων πινάκων. Οπότε, θα προβούμε στο ακόλουθο τέχνασμα για να πετύχουμε αυτό που θέλουμε:

- Θα πολλαπλασιάσουμε και τα δύο μέρη της εξίσωσης $u = xwy$ από τα αριστερά με x^{-1} (καθότι όπως είπαμε το x είναι αντιστρέψιμο) και παίρνουμε:

$$x^{-1}u = x^{-1}xwy \Longrightarrow x^{-1}u = wy \quad (1)$$

- Καθότι η εξίσωση $xa = ax$ ισχύει αν και μόνον αν $x^{-1}a = ax^{-1}$, τότε μπορούμε να πούμε πως έχουμε και $x_1 = x^{-1}$ και στη συνέχεια θα αντικαταστήσουμε το σύστημα εξισώσεων (1) που αναφέραμε πιο πάνω με το ακόλουθο:

$$x_1\alpha = \alpha x_1, yb = by, x_1u = wy$$

- Τώρα θα μετατρέψουμε κάθε εξίσωση του συστήματος σε ένα σύστημα k^2 γραμμικών εξισώσεων για τα άγνωστα στοιχεία ως προς την είσοδο των πινάκων x_1 και y. Έτσι, προκύπτει πως έχουμε ένα σύνολο $3n^2$ γραμμικών εξισώσεων με $2k^2$ αγνώστους. Να σημειώσουμε σε αυτό το σημείο ότι το σύστημα θα μας δώσει το μυστικό κλειδί K αν και μόνον αν το x_1 είναι αντιστρέψιμο, επειδή έχουμε $K = xvy$, όπου $x = {x_1}^{-1}$.

- Επειδή το u είναι ένας γνωστός αντιστρέψιμος πίνακας, μπορούμε να πολλαπλασιάσουμε και τα δύο μέρη της εξίσωσης $x_1u = wy$ από τη δεξιά πλευρά με u^{-1} και θα πάρουμε:

$$x_1uu^{-1} = wyu^{-1} \Rightarrow x_1 = wyu^{-1}$$

- Στη συνέχεια θα απαλείψουμε το x_1 από το σύστημα:

$$wyu^{-1}\alpha = \alpha wyu^{-1}, yb = by$$

- Έτσι θα καταλήξουμε να έχουμε μόνον έναν άγνωστο πίνακα y, με $2k^2$ γραμμικές εξισώσεις για k^2 στοιχεία εισόδου του y.

□

Συμπεράσματα

Με αυτόν τον τρόπο θα προκύψει ένα αρκετά αυστηρώς ορισμένο σύστημα γραμμικών εξισώσεων. Γνωρίζουμε όμως ότι το σύστημα αυτό θα πρέπει να έχει τουλάχιστον μια μη τετριμμένη (π.χ. μη μηδενική) λύση. Οπότε, αν περιορίσουμε τον πίνακα του συστήματος σε μια μορφή ιεραρχίας, θα πρέπει να υπάρχει τουλάχιστον μια ελεύθερη μεταβλητή. Από την άλλη, καθότι το σύστημα είναι πολύ αυστηρώς ορισμένο, αναμένουμε ο αριθμός των ελεύθερων μεταβλητών να μην είναι τόσο μεγάλος, οπότε και μπορούμε να δοκιμάσουμε όλες τις υποψήφιες τιμές των ελεύθερων μεταβλητών, μια κάθε φορά, μέχρι να βρούμε κάποιες τιμές που θα μας δώσουν έναν αντιστρέψιμο πίνακα y.

Όμως, όπως είπαμε πιο πάνω, οι τιμές εισόδου στο y είναι 0 ή 1, κάτι που καθιστά το πρωτόκολλο του Stickel ακόμη πιο ευάλωτο. Το καλό είναι ότι μπορούμε εύκολα να εξετάσουμε αν ένας πίνακας είναι αντιστρέψιμος, επειδή στην ουσία πρόκειται για αναγωγή του πίνακα σε μια ιεραρχική δομή.

Σε όλες όμως τις περιπτώσεις που εξετάσαμε, υπήρχε μόνον μια ελεύθερη μεταβλητή, οπότε και το τελευταίο βήμα ελέγχου της αντιστρεψιμότητας δεν είναι απαραίτητο, καθότι αν το παραπάνω σύστημα έχει μια μοναδική μη-μηδενική λύση, τότε κι ο αντίστοιχος πίνακας y θα είναι αντιστρέψιμος.

Βελτίωση πρωτοκόλλου του Stickel

Καταλήγουμε ότι ο καλύτερος τρόπος για να βελτιώσουμε το πρωτόκολλο του Stickel είναι να χρησιμοποιήσουμε μη-αντιστρέψιμα στοιχεία a, b, w. Συγκεκριμένα, αυτό σημαίνει ότι θα πρέπει να χρησιμοποιήσουμε μια ημί-ομάδα με αρκετά μη-αντιστρέψιμα στοιχεία. Εάν κάποιος πρέπει να χρησιμοποιήσει πίνακες, τότε έχει σημασία να κάνουμε λόγο για χρήση της ημί-ομάδας όλων των $k \times k$ πινάκων πάνω σε ένα πεπερασμένο δακτύλιο (όχι απαραίτητα πεδίο).

Συνήθως, μια τέτοια ημί-ομάδα έχει πολλά μη-αντιστρέψιμα στοιχεία, οπότε και θα είναι εύκολο να επιλέξουμε τα μη-αντιστρέψιμα στοιχεία a, b, w. Έτσι σε αυτήν την περίπτωση η επίθεση μέσω της γραμμικής άλγεβρας δεν ευδοκιμεί. Ένα άλλο πλεονέκτημα του να μην περιορίσουμε τους προσφερόμενους πίνακες μόνον σε αυτούς που είναι αντιστρέψιμους, είναι το γεγονός ότι θα μπορούμε να χρησιμοποιήσουμε τυχαίες εκφράσεις της μορφής $\sum_{i=1}^{p} c_i \cdot a^i$ (όπου τα c_i είναι σταθερές). Έτσι, δε θα είμαστε περιορισμένοι να χρησιμοποιούμε μόνον δυνάμεις a^j από έναν δοσμένο δημόσιο πίνακα του πρωτοκόλλου του Stickel.

Φυσικά, δεν υπάρχει κάποιος επιτακτικός λόγος να χρησιμοποιήσουμε πίνακες στο όλο σύστημα του Stickel, αλλά όπως έχουμε εξηγήσει και πιο πάνω, όταν χρησιμοποιούμε μια τυχαία (ημί)ομάδα G, το σύστημα του Stickel μπορεί να παραβιαστεί αν το σχετικό πρόβλημα αναζήτησης της διάσπασης θεωρηθεί ως επιλύσιμο. Όμως, μέχρι στιγμή, καμία συγκεκριμένη τυχαία (ημί)ομάδα δεν έχει επιβεβαιωθεί ότι είναι ανθεκτική στις επιθέσεις που σχετίζονται με το πρόβλημα αναζήτησης της διάσπασης.

ΙΙΙ.7
Το πρωτόκολλο AAG (Anshel-Anshel-Goldfeld)

Εισαγωγή

Σε αυτήν την ενότητα θα μιλήσουμε για ένα πρωτόκολλο εγκατάστασης κλειδιού που ξεχωρίζει από τα άλλα, επειδή δε χρησιμοποιεί κατ' ανάγκην κάποια μεταθετική υποομάδα μιας συγκεκριμένης ομάδας και αντ' αυτού μπορεί να χρησιμοποιήσει κάθε μη-αβελιανή ομάδα στην οποία το πρόβλημα της λέξης επιλύεται αποτελεσματικά. Αυτό και μόνον είναι αρκετό για να καταστήσουν το πρωτόκολλο των Anshel-Anshel-Goldfeld ξεχωριστό, έχοντας σαφές πλεονέκτημα έναντι των υπολοίπων που αναλύσαμε.

Πρόκειται για ένα πρωτόκολλο που το οφείλουμε στους Drs. Michael Anshel, Iris Anshel και Dorian Goldfeld.

Πρωτόκολλο ΙΙΙ.11

1. Έστω ότι έχουμε μια δημόσια ομάδα G και τα δημόσια στοιχεία $\alpha_1, \dots, \alpha_k, b_1, \dots, b_m \in G$.

2. Η Alice θα επιλέξει ένα ιδιωτικό $x \in G$, ως λέξη των $\alpha_1, \dots, \alpha_k$ (π.χ. $x = x(\alpha_1, \dots, \alpha_k)$) και στέλνει στον Bob το $b_1^x, \dots, b_m^x$.

3. Ο Bob θα επιλέξει ένα ιδιωτικό $y \in G$, ως λέξη των $b_1, \dots, b_m$ και στέλνει στην Alice το $a_1^y, \dots, a_k^y$.

4. Η Alice θα υπολογίσει το $x\left(a_1^y, \dots, a_k^y\right) = x^y = y^{-1}xy$ και ο Bob θα υπολογίσει το $y(b_1^x, \dots, b_m^x) = y^x = x^{-1}yx$.

5. Στη συνέχεια η Alice και ο Bob θα καταλήξουν σε ένα κοινό μυστικό κλειδί $K = x^{-1}y^{-1}xy$, που θα αποκαλείται «μετατροπέας (commutator)» των x και y ακολουθώντας τον ακόλουθο συλλογισμό:
   Η Alice θα πολλαπλασιάσει από τα αριστερά το $y^{-1}xy$ με x^{-1}, ενώ ο Bob θα πολλαπλασιάσει από τα αριστερά το $x^{-1}yx$ με y^{-1} και στη συνέχεια θα πάρει το αντίστροφο που θα είναι:
   $$(y^{-1}x^{-1}yx)^{-1} = x^{-1}y^{-1}xy$$

□

Συμπεράσματα

Τα πιο πάνω μπορεί να μας δίνουν την εντύπωση πως αν ο επιτιθέμενος καταφέρει να επιλύσει το πρόβλημα αναζήτησης της συζυγίας για τα $b_1^x, \dots, b_m^x$ και $a_1^y, \dots, a_k^y$ στην ομάδα G, θα μπορεί να βρει και το κλειδί K. Όμως με μια πιο προσεκτική ματιά στο βήμα 4 πιο πάνω, θα παρατηρήσουμε ότι ο επιτιθέμενος θα πρέπει να γνωρίζει είτε το x είτε το y, όχι απλά σαν μια λέξη των γεννητόρων της ομάδας G, αλλά ως μια λέξη των $\alpha_1, \dots, \alpha_k$ ή των $b_1, \dots, b_m$ αντίστοιχα. Διαφορετικά, δε θα είναι σε θέση να προβεί σε συνθέσεις στοιχείων όπως το x^y από τα $a_1^y, \dots, a_k^y$. Με άλλα λόγια, ο επιτιθέμενος θα πρέπει να είναι σε θέση να επιλύσει και το πρόβλημα αναζήτησης του μέλους, για το οποίο αν και κάναμε κουβέντα προηγουμένως, θα μπορούσαμε να το ξαναδούμε:

Ορισμός ΙΙΙ.7
Έστω ότι έχουμε μια ομάδα G και τα στοιχεία της $x, \alpha_1, \dots, \alpha_k$ και θέλουμε να βρούμε (εάν υπάρχει) μια έκφραση του x ως λέξη των $\alpha_1, \dots, \alpha_k$. □

Να σημειώσουμε σε αυτό το σημείο ότι το πρόβλημα απόφασης του μέλους είναι όταν πρέπει να βρούμε αν κάποιο $x \in G$ ανήκει ή δεν ανήκει στην υποομάδα της G που παράγεται από τα $\alpha_1, \dots, \alpha_k$. Όμως, το πρόβλημα αυτό είναι πολύ δύσκολο για περιπτώσεις αρκετών ομάδων. Για παράδειγμα, το πρόβλημα απόφασης του μέλους σε μια ομάδα πλεξίδων B_n δε μπορεί να επιλυθεί αλγοριθμικά για $n \geq 6$, επειδή μια τέτοια ομάδα πλεξίδων περιλαμβάνει υποομάδες ισομορφικές προς το $F_2 \times F_2$, όπου η F_2 είναι η ελεύθερη ομάδα τάξης 2 (θα μπορούσε να είναι για παράδειγμα η υποομάδα που παράγεται από τα $\sigma_1^2, \sigma_2^2, \sigma_4^2$ και σ_5^2 όπως μπορούμε να δούμε και στο [7]. Η Mihailova το 1958, στο [37] μας δείχνει ότι το πρόβλημα απόφασης του μέλους για την ομάδα $F_2 \times F_2$, δεν επιλύεται αλγοριθμικά.

Αξίζει σε αυτό το σημείο να παρατηρήσουμε πως αν ο επιτιθέμενος βρει κάποιο στοιχείο $x' \in G$ τέτοιο ώστε $b_1^x = b_1^{x'}, \dots, b_m^x = b_m^{x'}$, αυτό θα συνεπάγεται ότι $x = x'$ στην G. Πράγματι, έστω ότι $x' = c_b x$, με $c_b b_i = b_i c_b$, δηλαδή το c_b είναι στοιχείο του κεντροποιητή του συνόλου των b_i. Τότε θα έχουμε ότι $b_i^x = b_i^{x'}$ για κάθε i, επομένως και $b^x = b^{x'}$ για κάθε στοιχείο b της υποομάδας που παράγεται από τα $b_1, \dots, b_m$, για $1 \leq i \leq m$. Πιο συγκεκριμένα $y^x = y^{x'}$.

Όμως, αν τα στοιχεία x' και y' αντίστοιχα δεν ανήκουν στις υποομάδες $A = \langle a_1, \dots, a_k \rangle$ και $B = \langle b_1, \dots, b_m \rangle$ αντίστοιχα, τότε ο επιτιθέμενος ενδέχεται να μη βρει το σωστό μυστικό κλειδί K. Από την άλλη όμως, αν το στοιχείο x' και αντίστοιχα το στοιχείο y' ανήκουν στην υποομάδα A και αντίστοιχα στην

υποομάδα B, τότε ο επιτιθέμενος θα μπορούσε υπό διάφορες προϋποθέσεις να βρει το σωστό μυστικό κλειδί K, ακόμη και στην περίπτωση που τα στοιχεία x', y' είναι διαφορετικά από τα αντίστοιχα x, y. Όντως, έστω ότι έχουμε $x' = c_b x, y' = c_a y$ όπου το c_b είναι στοιχείο του κεντροποιητή του συνόλου B και c_α στοιχείο του κεντροποιητή του συνόλου A. Επομένως θα έχουμε ότι:

$$(x')^{-1}(y')^{-1}x'y' = (c_b x)^{-1}(c_a y)^{-1}c_b x c_a y = x^{-1}{c_b}^{-1}y^{-1}{c_a}^{-1}c_b x c_a y$$
$$= x^{-1}y^{-1}xy = K$$

Επειδή ισχύουν οι ακόλουθες σχέσεις:

- $c_b y = y c_b$ με $y \in B$ και $B = \langle b_1, \dots, b_m \rangle$.

- $c_b c_\alpha = c_\alpha c_b$ με $c_\alpha \in B$, αφού $y' = c_\alpha y \in B$ και $c_b \in A$, αφού $x' = c_b x \in A$.

- $c_\alpha x = x c_\alpha$ με $x \in A$ και $A = \langle a_1, \dots, a_k \rangle$.

Σε αυτό το σημείο θα πρέπει να σημειώσουμε ότι για να μπορέσει ο επιτιθέμενος να βρει το σωστό μυστικό κλειδί K, θα πρέπει τα στοιχεία c_α, c_b να μπορούν μα μετατεθούν. Αυτό όμως μπορεί να γίνει μόνον αν επιλέξουμε κατάλληλα τα x', y' έτσι ώστε να ισχύει $x' \in A$ και $y' \in B$. Εάν ο επιτιθέμενος δε μπορεί να επαληθεύσει τουλάχιστον μια εκ των προηγούμενων συνθηκών, δε θα μπορέσει να είναι σίγουρος ότι βρήκε το σωστό μυστικό κλειδί.

Αυτό μας οδηγεί στο συμπέρασμα ότι αν ο επιτιθέμενος προσπαθήσει να βρει τα στοιχεία x, y επιλύοντας το πρόβλημα αναζήτησης της συζυγίας στην ομάδα G, τότε θα πρέπει στη συνέχεια να αποπειραθεί να επιλύσει και το πρόβλημα αναζήτησης του μέλους ή το πρόβλημα απόφασης του μέλους. Όπως είπαμε και πιο πάνω, στο παράδειγμα της ομάδας πλεξίδων, το πρόβλημα απόφασης του μέλους, φαίνεται να μην επιλύεται με αλγοριθμικό τρόπο για μια δεδομένη ομάδα.

Οπότε καταλήγουμε στο συμπέρασμα πως ο επιτιθέμενος θα πρέπει να επιλύσει μια δύσκολη εκδοχή του προβλήματος αναζήτησης συζυγίας, η οποία μπορεί να διατυπωθεί ως εξής:

Ορισμός ΙΙΙ.8
Έστω ότι έχουμε μια ομάδα G, μια υποομάδα $A \leq G$ και δύο στοιχεία $g, h \in G$ και θέλουμε να βρούμε $x \in A$ τέτοιο ώστε $h = x^{-1}gx$, δεδομένου ότι υπάρχει τουλάχιστον ένα τέτοιο x. □

Κλείνοντας, οφείλουμε να πούμε ότι όλα όσα αναλύσαμε σε αυτήν την ενότητα δε σχετίζονται με διάφορες προσπάθειες επιθέσεων, κυρίως heuristic αλγορίθμων [38 & 39], στο πρωτόκολλο των Anshel-Anshel-Goldfeld. Αυτό οφείλεται στο γεγονός ότι αυτές οι απόπειρες επιθέσεων χρησιμοποιούν heuristic αλγορίθμους αναζήτησης της γειτνίασης και έχουν σχεδιαστεί κατά τέτοιον τρόπο ώστε να βρίσκουν τη λύση μιας δεδομένης εξίσωσης (ή ενός συστήματος εξισώσεων) ως λέξη, σε κάποια δεδομένα στοιχεία.

Το συμπέρασμα στο οποίο καταλήξαμε με την όλη ενότητα που αναπτύξαμε είναι ότι ακόμη κι αν βρούμε κάποιον γρήγορο πολυωνυμικού χρόνου ντετερμινιστικό αλγόριθμο για την επίλυση του προβλήματος αναζήτησης της συζυγίας στις ομάδες πλεξίδων, αυτός δε θα μπορεί να μας εξασφαλίσει κάποια ντετερμινιστική επίθεση, ικανή να επιτεθεί αποτελεσματικά στο πρωτόκολλο των Anshel-Anshel-Goldfeld.

III.8
Πρωτόκολλα πιστοποίησης που στηρίζονται στο πρόβλημα της συζυγίας

Εισαγωγή

Ο κύριος σκοπός ενός πρωτοκόλλου πιστοποίησης είναι να δώσει σε έναν χρήστη, έστω την Alice, τη δυνατότητα να αποδείξει την ταυτότητά της σε έναν server, έστω τον Bob, μέσω ενός μη ασφαλούς διαύλου επικοινωνίας, χρησιμοποιώντας μόνον το ιδιωτικό της κλειδί, χωρίς όμως να έχουμε κάποια διαρροή πληροφορίας που να σχετίζεται με το κλειδί. Σε τέτοιες περιπτώσεις, η Alice (χρήστης) ονομάζεται prover (αυτός που προσπαθεί να αποδείξει την ταυτότητά του) και ο Bob (server) ονομάζεται verifier (αυτός που προβαίνει στην ταυτοποίηση της Alice).

Υπάρχουν αρκετές διαθέσιμες προτάσεις που χρησιμοποιούν μη-αβελιανές ομάδες. Οι περισσότερες από αυτές είναι άμεσες υιοθετήσεις συστημάτων ανταλλαγής κλειδιών, όπως είναι και το πρωτόκολλο ανταλλαγής κλειδιών των Ko-Lee.

III.8.1 Diffie-Hellman-Merkle

Πρωτόκολλο III.12
Στο ακόλουθο σύστημα που θα περιγράψουμε, έστω ότι έχουμε μια ομάδα G και δύο μεταθετικές υποομάδες $A, B < G$, π.χ. $ab = ba$ για κάθε $a \in A$ και $b \in B$.

Το ιδιωτικό κλειδί της Alice θα είναι ένα στοιχείο $s \in A$. Το δημόσιο κλειδί της Alice θα είναι ένα ζευγάρι, έστω το (w, t), όπου το w είναι ένα τυχαίο στοιχείο της G και $t = s^{-1}ws$. Σε αυτήν την περίπτωση, τα βήματα του πρωτοκόλλου πιστοποίησης θα είναι τα ακόλουθα:

1. Ο Bob επιλέγει ένα $r \in B$ και στέλνει στην Alice το «ερώτημα» $w' = r^{-1}wr$.

2. Η Alice στέλνει στον Bob την απάντηση $w'' = s^{-1}w's$.

3. Ο Bob ελέγχει αν ισχύει $w'' = r^{-1}tr$.

Αν ο prover (Alice) δώσει τη σωστή απάντηση στο 2ο βήμα, τότε ο verifier (Bob) θα την αποδεχθεί και θα ταυτοποιήσει την Alice, επειδή τα στοιχεία r και s από την κατασκευή τους μπορούν και μετατίθενται.

Οπότε και παίρνουμε την ακόλουθη ισότητα που ικανοποιείται:

$$w'' = s^{-1}w's = s^{-1}r^{-1}wrs = r^{-1}s^{-1}wsr = r^{-1}tr$$

□

Ο επιτιθέμενος θέλει να μπερδέψει τον Bob ώστε να τον ταυτοποιήσει ως την Alice, οπότε και πρέπει να κάνει μια από τις ακόλουθες δυο ενέργειες:

- Να υπολογίσει το ιδιωτικό κλειδί s της Alice, με το να λύσει το πρόβλημα αναζήτησης της συζυγίας που σχετίζεται με την υποομάδα A ή με το να λύσει το πρόβλημα της διάσπασης για το ζεύγος (w, t) που πάλι σχετίζεται με την υποομάδα A, π.χ. με το να υπολογίσει τα στοιχεία $s_1, s_2 \in A$, έτσι ώστε $t = s_1 w s_2$. Είναι αυτονόητο και δε χρειάζεται να το ελέγξουμε πως για ένα τέτοιο ζεύγος (s_1, s_2), η ισότητα $s_1 w' s_2 = w''$ ικανοποιείται πάντα και κατά συνέπεια το ζεύγος (s_1, s_2) μπορεί να παίξει το ρόλο του ιδιωτικού κλειδιού s της Alice.

- Να υπολογίσει το προσωρινό κλειδί r του Bob με το να επιλύσει το πρόβλημα αναζήτησης της συζυγίας που σχετίζεται με την υποομάδα B ή με το να επιλύσει το πρόβλημα διάσπασης για το ζεύγος (w, w') που σχετίζεται και πάλι με την υποομάδα B και στη συνέχεια να το χρησιμοποιήσει όπως περιγράψαμε πιο πάνω έτσι ώστε να επιτεθεί στο ιδιωτικό κλειδί της Alice.

Η υπολογιστική δυσκολία των πιο πάνω προβλημάτων εξαρτάται από τις μεμονωμένες υποομάδες A και B, οπότε δε χρειάζεται να είναι ίδια και για τα δύο, δηλαδή το A και το B.

Πρωτόκολλο ΙΙΙ.13

Να σημειώσουμε σε αυτό το σημείο ότι το πιο πάνω σύστημα μπορεί εύκολα να τροποποιηθεί έτσι ώστε να βασίζεται στο πρόβλημα της διάσπασης. Πράγματι, έστω ότι A_1, A_2, B_1, B_2 είναι υποομάδες της G, τέτοιες ώστε $[A_1, B_1] = 1$ και $[A_2, B_2] = 1$. Το ιδιωτικό κλειδί της Alice είναι το ζεύγος $(\alpha_1, \alpha_2) \in A_1 \times A_2$ και το δημόσιο της κλειδί είναι το ζεύγος $(w, t) \in G \times G$, όπου το w είναι ένα τυχαίο στοιχείο της G και το $t = \alpha_1 w \alpha_2$. Οπότε και τα βήματα του συστήματος θα τροποποιηθούν αντίστοιχα:

1. Ο Bob επιλέγει τα στοιχεία $b_1 \in B_1, b_2 \in B_2$ και στέλνει στην Alice το «ερώτημα» $w' = b_1 w b_2$.

2. Η Alice στέλνει στον Bob την απάντηση $w'' = a_1 w' a_2$.

3. Ο Bob ελέγχει αν ισχύει $w'' = b_1 t b_2$.

□

Το σύστημα αυτό το οφείλουμε στους Lal και Chaturwedi [40]. Όπως είναι προφανές, δε μπορούμε να χρησιμοποιήσουμε το πρόβλημα αναζήτησης της λέξης έτσι ώστε να επιτεθούμε σε αυτήν την τροποποιημένη εκδοχή του πρωτοκόλλου.

III.8.2 Fiat-Shamir

Μια άλλη πρόταση ενός συστήματος πιστοποίησης με βάση τη χρήση ομάδων οφείλεται στον Sibert [41]. Αν τη μελετήσουμε θα δούμε ότι μας θυμίζει το σύστημα που έχει προταθεί από τους Fiat-Shamir [42], και το οποίο περιλαμβάνει την κατ' εξακολούθηση επανάληψη ενός βήματος στο οποίο έχουμε την πρόκληση για τριπλή επιτυχή απόπειρα πιστοποίησης. Μια από τις μεγάλες διαφορές από το σύστημα των Diffie-Hellman που αναλύσαμε πιο πάνω είναι ότι δε χρειάζεται να επιλέξουμε μεταθετικές υποομάδες A και B.

Πρωτόκολλο ΙΙΙ.14
Όπως και πιο πάνω, το ιδιωτικό κλειδί της Alice είναι ένα στοιχείο $s \in G$ και το δημόσιο κλειδί της είναι ένα ζεύγος (w, t), όπου το w είναι ένα τυχαίο στοιχείο του G και $t = s^{-1}ws$. Το πρωτόκολλο πιστοποίησης θα αναπτυχθεί ως εξής:

1. Η Alice θα επιλέξει ένα τυχαίο $r \in G$ και θα στείλει στον Bob το στοιχείο $x = r^{-1}tr$, που θα αποτελεί τη δέσμευση.

2. Ο Bob θα επιλέξει ένα τυχαίο bit c και θα το στείλει στην Alice.

   - Εάν $c = 0$, τότε η Alice θα στείλει στον Bob το $y = r$ και ο Bob θα ελέγξει εάν ικανοποιείται η ισότητα $x = y^{-1}ty$.

   - Εάν $c = 1$, τότε η Alice θα στείλει στον Bob το $y = sr$ και ο Bob θα ελέγξει εάν ικανοποιείται η ισότητα $x = y^{-1}wy$.

□

Όπως είναι προφανές, μια σωστή απάντηση του "prover" στο δεύτερο βήμα, θα μας οδηγήσει σε αποδοχή του από τον "verifier" και κατά προέκταση σε πιστοποίηση. Όμως, αυτό που δεν είναι τόσο προφανές είναι γιατί χρειαζόμαστε το όλο ζητούμενο που σχετίζεται με τη χρήση του τυχαίου bit. Θα μπορούσε απλά η Alice να αποκαλύψει το $y = sr$, κάτι που δεν αποκαλύπτει το μυστικό s, ενώ επιτρέπει στον Bob να επιβεβαιώσει την ισότητα $x = y^{-1}wy$.

Το θέμα που ανακύπτει σε αυτήν την περίπτωση είναι ότι ο επιτιθέμενος που θέλει να υποκριθεί την Alice μπορεί να πάρει ένα τυχαίο στοιχείο u και να στείλει ως δέσμευση στον Bob το $x = u^{-1}wu$. Τότε, αυτό το u θα μπορούσε να παίξει τον ίδιο ρόλο στις διαδικασίες πιστοποίησης, όπως το $y = sr$. Κατά τον ίδιον τρόπο, εάν ο επιτιθέμενος γνώριζε ότι η Alice επρόκειτο να στείλει $y = r$ ώστε να χρησιμοποιηθεί στις διαδικασίες πιστοποίησης, θα μπορούσε να

χρησιμοποιήσει ένα τυχαίο στοιχείο u στη θέση του r, ως το βήμα της δέσμευσης.

Όμως, όλες αυτές οι σκέψεις που κάνουμε μας δείχνουν ότι θα πρέπει να τρέξουμε το πιο πάνω πρωτόκολλο πιστοποίησης αρκετές φορές έτσι ώστε να πετύχουμε την καλύτερη δυνατή αξιοπιστία, γιατί διαφορετικά, εάν το τρέξουμε μόνον μια φορά, ο επιτιθέμενος μπορεί να υποκριθεί ότι είναι η Alice με πιθανότητα $\frac{1}{2}$. Όμως, εάν το τρέξουμε έστω k φορές, τότε η πιθανότητα πέφτει στο $\frac{1}{2^k}$.

Όπως και στην περίπτωση του συστήματος των Diffie-Hellman, η ασφάλεια του συστήματος που μοιάζει σε αυτό των Fiat-Shamir, εξαρτάται και στηρίζεται στην υπολογιστική δυσκολία που φέρει το πρόβλημα αναζήτησης της συζυγίας στην ομάδα G. Είναι ιδιαιτέρως ενδιαφέρον να αναφέρουμε ότι το πρόβλημα αναζήτησης της διάσπασης δε μπορεί να χρησιμοποιηθεί έτσι ώστε να επιτεθούμε σε αυτό το πρωτόκολλο, επειδή στο τελευταίο βήμα του πρωτοκόλλου, ο Bob αποδέχεται ακριβώς ένα στοιχείο, είτε το r είτε το rs, ανάλογα με την τιμή του c.

ΙΙΙ.8.3 Επικύρωση του προβλήματος αναζήτησης της twisted συζυγίας

Θα μπορούσαμε να τροποποιήσουμε το πιο πάνω σύστημα πιστοποίησης κατά τέτοιον τρόπο ώστε να στηρίζεται στο πρόβλημα της διάσπασης. Σε σχέση με άλλες τροποποιήσεις που έχουμε δει πιο πριν, αυτή για την όποια κάνουμε λόγο τώρα έχει ιδιαίτερο ενδιαφέρον. Έστω ότι έχουμε έναν τυχαίο ενδομορφισμό φ (π.χ. ομομορφισμό ως προς τον εαυτό της) της ομάδας G που επρόκειτο να χρησιμοποιήσουμε. Υποθέτουμε ότι το φ είναι δημοσίως γνωστό, π.χ. θα μπορούσε να αποτελεί μέρος του δημόσιου κλειδιού της Alice.

Πρωτόκολλο ΙΙΙ.15
Το ιδιωτικό κλειδί της Alice είναι ένα στοιχείο $s \in G$ και το δημόσιο κλειδί της είναι ένα ζεύγος (w, t), όπου το w είναι ένα τυχαίο στοιχείο του G και $t = s^{-1}w\varphi(s)$. Το πρωτόκολλο πιστοποίησης θα αναπτυχθεί ως εξής:

1. Η Alice θα επιλέξει ένα στοιχείο $r \in G$ και θα στείλει στον Bob το στοιχείο $x = r^{-1}t\varphi(r)$, που θα αποτελεί τη δέσμευση.

2. Ο Bob θα επιλέξει ένα τυχαίο bit c και θα το στείλει στην Alice.

   - Εάν $c = 0$, τότε η Alice θα στείλει στον Bob το $y = r$ και ο Bob θα ελέγξει εάν ικανοποιείται η ισότητα $x = y^{-1}t\varphi(y)$.

   - Εάν $c = 1$, τότε η Alice θα στείλει στον Bob το $y = sr$ και ο Bob θα ελέγξει εάν ικανοποιείται η ισότητα $x = y^{-1}w\varphi(y)$.

Και σε αυτήν την περίπτωση, εάν ο “prover” δώσει μια σωστή απάντηση στο δεύτερο βήμα, ο “verifier” θα την αποδεχθεί και θα πιστοποιήσει τον “prover”. □

Εάν θέλουμε να επιτεθούμε και να παραβιάσουμε το πρωτόκολλο, είναι αρκετό να βρούμε ένα στοιχείο $s' \in G$, τέτοιο ώστε $t = (s')^{-1}w\varphi(s')$, το οποίο αποτελεί μέρος ενός προβλήματος που είναι γνωστό με το όνομα πρόβλημα αναζήτησης της τροποποιημένης (twisted) συζυγίας και ορίζεται ως εξής:

Ορισμός ΙΙΙ.9
Έστω ότι έχουμε μια ομάδα G. Για κάθε $\varphi \in Aut(G)$ και για κάθε ζεύγος στοιχείων $w, t \in G$, θα πρέπει να βρούμε έναν τροποποιημένο (twisted) συζεύκτη για τα w και t (π.χ. ένα στοιχείο $s \in G$ τέτοιο ώστε $t = s^{-1}w\varphi(s)$, δεδομένου φυσικά ότι υπάρχει τουλάχιστον ένα τέτοιο s). □

Το πρόβλημα απόφασης του πιο πάνω προβλήματος είναι σχετικά καινούργιο στη θεωρία ομάδων. Αποτελεί μη-τετριμμένη περίπτωση, ακόμη και για τις ελεύθερες ομάδες. Μια άλλη κλάση ομάδων στις οποίες μπορούμε να επικαλεστούμε το πιο πάνω πρόβλημα είναι η κλάση των πολυκυκλικών πεπερασμένων ομάδων.

Ολοκληρώνοντας, αξίζει να αναφέρουμε πως δύο πρόσφατες γενικές προτάσεις ως προς το πώς μπορούμε να χρησιμοποιήσουμε την ιδέα των Fiat-Shamir έχουν προταθεί στο [43], όπου θα δούμε ότι με την κατάλληλη εφαρμογή του συστήματος πιστοποίησης των Fiat-Shamir, μπορούμε να αναγκάσουμε τον επιτιθέμενο (που θέλει να υποκριθεί) να πρέπει να αντιμετωπίσει ένα πρόβλημα NP-hard.

III.9
Το πρωτόκολλο KLCHKP
(Ko-Lee-Cheon-Han-Kang-Park)

Περίληψη

Δε θα επεκταθούμε ιδιαίτερα στο πρωτόκολλο καθότι το έχουμε ήδη συζητήσει εκτενώς. Πρόκειται για σύστημα ανταλλαγή κλειδιών και οφείλεται στους Ko-Lee-Cheon-Han-Kang-Park (2000) [3], ενώ βασίζεται στο σύστημα των Diffie-Hellman. Άλλωστε το είδαμε και στην 1η Ενότητα του Κεφαλαίου.

Πρωτόκολλο III.16
Ας δούμε λίγο περιληπτικά το πρωτόκολλο, επειδή αξίζει να συμπεριληφθεί στο σύνολο του παρόντος Κεφαλαίου.

1. Έστω ότι έχουμε μια δημόσια ομάδα G, με $G = \langle X|R\rangle$, ένα δημόσιο $w \in G$ και δύο υποομάδες $A, B \subseteq G$ τέτοιο ώστε $[a, b] = 1, \forall a \in A, \forall b \in B$.

2. Η Alice θα επιλέξει ένα τυχαίο $a \in A$ και θα στείλει στον Bob το $a^{-1}wa = w^a$.

3. Ο Bob θα επιλέξει ένα τυχαίο $b \in B$ και θα στείλει στην Alice το $b^{-1}wb = w^b$.

4. Οπότε το κοινό μυστικό που θα πάρουν και οι δύο, Alice και Bob, είναι:

   - Alice: $a^{-1}(b^{-1}wb)a = w^{ba}$
   - Bob: $b^{-1}(a^{-1}wa)b = w^{ab}$

5. Ο επιτιθέμενος γνωρίζει τα w, w^a, w^b και χρειάζεται να μάθει το w^{ab}. Όμως για να το μάθει, πρέπει να λύσει το πρόβλημα αναζήτησης της συζυγίας για το A ή για το B.

   Ή το παρακάτω φαινομενικά ακόμη πιο εύκολο πρόβλημα της διάσπασης:

   Έστω ότι έχουμε τα $w, w' \in G$, και θέλουμε να βρούμε τα $a_1, a_2 \in A$ τέτοια ώστε $w' = a_1 w a_2$.

Τώρα ο επιτιθέμενος γνωρίζει τα w, w^a, w^b και υποθέτουμε ότι μπορεί να υπολογίσει τα $a_1, a_2 \in A$, τέτοια ώστε:

$$w^a = a_1 w a_2.$$

Τότε όμως θα έχουμε:

$$a_1 w^b a_2 = a_1(b^{-1}wb)a_2 = b^{-1}(a_1 w a_2)b = b^{-1}w^a b = w^{ab}$$

οπότε και θα βρει το μυστικό.

□

III.10
Σχέσεις μεταξύ των διαφόρων προβλημάτων

Εισαγωγή

Σε αυτήν την τελευταία ενότητα του Κεφαλαίου, θα δούμε διάφορες σχέσεις που υπάρχουν ανάμεσα στα διάφορα προβλήματα και πρωτόκολλα που αναπτύξαμε σε όλες τις προηγούμενες ενότητες.

Πρόβλημα αναζήτησης της συζυγίας (Ko-Lee)

Ας ξεκινήσουμε με το πολυσυζητημένο πρόβλημα αναζήτησης της συζυγίας, το οποίο το είδαμε και στην αρχή του Κεφαλαίου. Αν θα θέλαμε να του δώσουμε ένα όνομα που θα του ταίριαζε ακόμη καλύτερα, μπορούμε να το αποκαλέσουμε και πρόβλημα αναζήτησης της συζυγίας για συγκεκριμένες υποομάδες. Έτσι έχουμε:

Ορισμός III.10
Έστω ότι έχουμε δύο στοιχεία w, h μιας ομάδας G, μια υποομάδα $A \leq G$ και ότι ισχύει $w^a = h$ για κάποιο $a \in A$. Το ζητούμενο είναι να βρούμε ένα τέτοιο στοιχείο a. □

Αναφορικά με το πρωτόκολλο των Ko-Lee που έχουμε συναντήσει πολλές φορές, η Alice θα στείλει στον Bob το w^a για κάποιο ιδιωτικό $a \in A$ και ο Bob θα στείλει στην Alice το w^b για κάποιο ιδιωτικό $b \in B$, όπου οι υποομάδες A και B έχουμε μεταθετικά στοιχεία, π.χ. $ab = ba, \forall a \in A, \forall b \in B$.

Τώρα ας υποθέσουμε ότι ο επιτιθέμενος βρίσκει τα $a_1, a_2 \in A$, τέτοια ώστε $a_1 w a_2 = a^{-1} w a$ και $b_1, b_2 \in B$ τέτοια ώστε $b_1 w b_2 = b^{-1} w b$. Οπότε στη συνέχεια ο επιτιθέμενος μπορεί να βρει το μυστικό κλειδί:

$$a_1 b_1 w b_2 a_2 = a_1 b^{-1} w b a_2 = b^{-1} a_1 w a_2 b = b^{-1} a^{-1} w a b = K$$

Να σημειώσουμε σε αυτό το σημείο ότι τα προαναφερθέντα a_1, a_2 και b_1, b_2 δε συσχετίζονται με τα ιδιωτικά στοιχεία που αρχικώς επέλεξαν η Alice και ο Bob, κάτι που απλοποιεί σημαντικά την αναζήτηση. Επίσης, είναι

αξιοσημείωτο πως ο επιτιθέμενος μπορεί να βρει το μυστικό κλειδί και με μόνον ένα από τα ζευγάρια, έστω το $a_1, a_2 \in A$. Τότε έχουμε:

$$a_1(b^{-1}wb)a_2 = b^{-1}a_1wa_2b = b^{-1}a^{-1}wab = K$$

Όπως είπαμε και στην Ενότητα ΙΙΙ.9 πιο πάνω, ο επιτιθέμενος δε χρειάζεται να λύσει το πρόβλημα αναζήτησης της συζυγίας για συγκεκριμένη υποομάδα, έτσι ώστε να βρει το μυστικό κλειδί K. Αρκεί να λύσει κάτι αρκετά πιο εύκολο, δηλαδή το πρόβλημα αναζήτησης της διάσπασης για συγκεκριμένη υποομάδα. Δε θα επεκταθούμε περισσότερο σε αυτό το σημείο, επειδή το έχουμε αναλύσει στην ακριβώς προηγούμενη ενότητα.

Γενίκευση του προβλήματος αναζήτησης της διάσπασης (Shpilrain-Ushakov)

Το πρωτόκολλο που οφείλουμε στους Shpilrain και Ushakov στηρίζεται σε μια πιο γενική εκδοχή του προβλήματος αναζήτησης της διάσπασης, όπου έχουμε δύο διαφορετικές υποομάδες. Πιο συγκεκριμένα:

Ορισμός ΙΙΙ.11
Έστω, ότι έχουμε δύο στοιχεία w και w' μιας ομάδας G και δύο υποομάδες $A, B \leq G$. Πρέπει να βρούμε δύο στοιχεία $a \in A$ και $b \in B$ που να ικανοποιούν τη σχέση $a \cdot w \cdot b = w'$, δεδομένου ότι υπάρχει τουλάχιστον ένα τέτοιο ζεύγος. □

Τώρα, μπορούμε να εφαρμόσουμε ένα επιπλέον τέχνασμα έτσι ώστε να αναγάγουμε το πρόβλημα αναζήτησης της διάσπασης σε μια ειδική περίπτωση όπου $w = 1$. Δηλαδή, έστω ότι έχουμε το $w' = a \cdot w \cdot b$ και θα το πολλαπλασιάσουμε από αριστερά με το w^{-1} (που είναι το αντίστροφο του δημόσιου στοιχείου w), έτσι ώστε να λάβουμε το:

$$w'' = w^{-1}a \cdot w \cdot b = (w^{-1}a \cdot w) \cdot b$$

Οπότε, ονομάζοντας με A^w την υποομάδα που είναι συζυγής με το A μέσω του στοιχείου w, το πρόβλημα που θα έχει να αντιμετωπίσει πλέον ο επιτιθέμενος, γίνεται πλέον πρόβλημα αναζήτησης της παραγοντοποίησης και μπορεί να οριστεί ως εξής:

Έστω ότι έχουμε ένα στοιχείο w' μιας ομάδας G και δύο υποομάδες A^w, $B \leq G$. Πρέπει να βρούμε δύο στοιχεία $a \in A^w$ και $b \in B$ που να ικανοποιούν τη σχέση $a \cdot b = w'$, δεδομένου ότι υπάρχει τουλάχιστον ένα τέτοιο ζεύγος.

Στο αυθεντικό πρωτόκολλο των Ko-Lee, ισχύει $A = B$, κάτι που μας οδηγεί στην ακόλουθη ενδιαφέρουσα παρατήρηση:

Εάν στο πρωτόκολλο αυτό το A είναι μια κανονική υποομάδα της G, τότε θα έχουμε $A^w = A$ και οπότε το πιο πάνω πρόβλημα θα διαμορφωθεί ως εξής: Έστω ότι έχουμε $w' \in A$. Πρέπει να βρούμε δύο στοιχεία $a_1, a_2 \in A$ τέτοια ώστε $w' = a_1 a_2$.

Το πρόβλημα αυτό θα είναι τετριμμένο επειδή το a_1 θα μπορούσε να είναι οποιοδήποτε στοιχείο του A και οπότε θα έχουμε $a_2 = {a_1}^{-1} w'$.

Για τον λόγο αυτόν, σε πρωτόκολλα σαν τα πιο πάνω, προκειμένου να τους αυξήσουμε την ασφάλεια, θα πρέπει να αποφευχθεί η επιλογή κανονικών υποομάδων.

Αναγωγή προβλήματος αναζήτησης της διάσπασης σε πρόβλημα αναζήτησης της συζυγίας

Μπορούμε να προσεγγίσουμε και να επιτεθούμε σε ένα πρωτόκολλο που βασίζεται στο πρόβλημα αναζήτησης της διάσπασης εφαρμόζοντας εναλλακτικό τέχνασμα, προβαίνοντας σε αναγωγή στο πρόβλημα αναζήτησης της συζυγίας.

Έστω ότι έχουμε μια ομάδα G και $w' = awb$ ένα στοιχείο της G. Τώρα ο επιτιθέμενος πρέπει να βρει τα στοιχεία $a \in A$ και $b \in B$, όπου A, B είναι μεταθετικές ομάδες της G. Σε αυτήν την περίπτωση ο επιτιθέμενος θα επιλέξει τυχαία ένα $b_1 \in B$ και πρέπει να υπολογίσει το στοιχείο:

$$[awb, b_1] = b^{-1}w^{-1}a^{-1}{b_1}^{-1}awbb_1 = b^{-1}w^{-1}{b_1}^{-1}wbb_1 = (b_1^{-1})^{wb}b_1 = ((b_1^{-1})^w)^b b_1$$

Πλέον ο επιτιθέμενος γνωρίζει το στοιχείο b_1, οπότε και μπορεί να πολλαπλασιάσει το στοιχείο $((b_1^{-1})^w)^b b_1$ με το b_1^{-1} από δεξιά, οπότε και θα πάρει τοι στοιχείο:

$$w'' = ((b_1^{-1})^w)^b$$

Άρα, το πρόβλημα πλέον θα έχει μετατραπεί στο εξής:

Θα πρέπει να βρεθεί ένα στοιχείο $b \in B$ από τα στοιχεία $w'' = ((b_1^{-1})^w)^b$ και $(b_1^{-1})^w$.

Κατά τον ίδιο τρόπο, προκειμένου ο επιτιθέμενος να εντοπίσει το στοιχείο $a \in A$, θα επιλέξει ένα στοιχείο $a_1 \in A$ και θα υπολογίσει το στοιχείο:

$$[(awb)^{-1}, (\alpha_1)^{-1}] = awb\alpha_1 b^{-1}w^{-1}a^{-1}{a_1}^{-1} = awa_1w^{-1}a^{-1}{a_1}^{-1}$$
$$= (\alpha_1)^{w^{-1}a^{-1}}{a_1}^{-1} = ((\alpha_1)^{w^{-1}})^{a^{-1}}{a_1}^{-1}$$

Στη συνέχεια, ο επιτιθέμενος θα πολλαπλασιάσει το πιο πάνω αποτέλεσμα με το γνωστό στοιχείο a_1 από δεξιά και θα λάβει το στοιχείο:

$$w''' = ((\alpha_1)^{w^{-1}})^{a^{-1}}$$

Οπότε και το πρόβλημα θα μετατραπεί στο εξής:

Θα πρέπει να βρεθεί ένα στοιχείο $\alpha \in A$ από τα στοιχεία $w''' = ((\alpha_1)^{w^{-1}})^{a^{-1}}$ και $(\alpha_1)^{w^{-1}}$.

Σε αυτό το σημείο θα πρέπει να σημειώσουμε πως η λύση του προβλήματος αναζήτησης της συζυγίας για συγκεκριμένη υποομάδα δεν είναι πάντα μοναδική. Κατά συνέπεια, αν προσπαθήσουμε να επιλύσουμε τις δύο πιο πάνω περιπτώσεις του προβλήματος, ενδέχεται να μη λάβουμε πάντα τη σωστή λύση του αυθεντικού προβλήματος διάσπασης. Παρ' όλα αυτά, οι όποιες δύο λύσεις, έστω b' και b'', του πρώτου προβλήματος αναζήτησης της συζυγίας διαφέρουν κατά ένα στοιχείο του κεντροποιητή του $(b_1^{-1})^w$. Και όπως είναι αυτονόητο, ο προαναφερθέν κεντροποιητής δε φέρεται να έχει μια μη-τετριμμένη διχοτόμηση με το B.

Αναγωγή προβλήματος παραγοντοποίησης
σε πρόβλημα αναζήτησης της συζυγίας

Ένας παρόμοιος υπολογισμός μας δείχνει ότι εάν εφαρμόσουμε το ίδιο τέχνασμα, μπορούμε να αναγάγουμε και το πρόβλημα αναζήτησης της παραγοντοποίησης σε πρόβλημα αναζήτησης της συζυγίας για μια συγκεκριμένη υποομάδα. Έστω ότι έχουμε το $w' = ab$ και θέλουμε να ανακτήσουμε τα $\alpha \in A$ και $b \in B$, όπου τα A και B είναι δύο υποομάδες της ομάδας G με μεταθετικά στοιχεία μεταξύ τους.

Θα επιλέξουμε ένα $b_1 \in B$ και θα υπολογίσουμε το:

$$[ab, b_1] = b^{-1}a^{-1}{b_1}^{-1}abb_1 = ({b_1}^{-1})^b b_1$$

Καθότι γνωρίζουμε το b_1, μπορούμε να πολλαπλασιάσουμε το πιο πάνω αποτέλεσμα με ${b_1}^{-1}$ από δεξιά έτσι ώστε να λάβουμε:

$$w'' = (b_1^{-1})^b$$

Αυτό όμως είναι το πρόβλημα αναζήτησης της συζυγίας για συγκεκριμένη υποομάδα. Εάν μπορούμε να την επιλύσουμε, μπορούμε να ανακτήσουμε και το $b \in B$.

Εφαρμόζοντας και πάλι το γνωστό πλέον τέχνασμα, μπορούμε να επιτεθούμε κατά τον ίδιο τρόπο και στο πρόβλημα αναζήτησης της συζυγίας για μια συγκεκριμένη υποομάδα. Έτσι, έστω ότι έχουμε $w' = \alpha^{-1}wa$ και θα πρέπει να ανακτήσουμε το $\alpha \in A$. Θα επιλέξουμε κάποιο b από τον κεντροποιητή του A.

Γνωρίζουμε ότι υπάρχει μια δημόσια υποομάδα B που είναι μεταθετική προς την A ως προς τα στοιχεία τους και στη συνέχεια θα επιλέξουμε ένα $b \in B$. Οπότε μετά πρέπει να υπολογίσουμε το:

$$[w', b] = [a^{-1}wa, b] = a^{-1}w^{-1}ab^{-1}a^{-1}wab = a^{-1}w^{-1}b^{-1}wab = (b^{-w})^a b$$

Στη συνέχεια, θα πολλαπλασιάσουμε το αποτέλεσμα που θα πάρουμε με το b^{-1} από δεξιά έτσι ώστε να πάρουμε $(b^{-w})^a$, οπότε και το πρόβλημα πλέον θα είναι να ανακτήσουμε το $\alpha \in A$ από τα $(b^{-w})^a$ και b^{-w}.

Το πρόβλημα αυτό που προκύπτει πιθανόν να είναι ευκολότερο από το αρχικό πρόβλημα επειδή έχουμε την ευελιξία ως προς την επιλογή του $b \in B$. Πιο συγκεκριμένα, εάν θέλουμε να αποπειραθούμε μια πετυχημένη επίθεση θα πρέπει να επιλέξουμε αρκετά $b \in B$ και να προσπαθήσουμε να λύσουμε το πρόβλημα αναζήτησης της συζυγίας για κάθε ένα από αυτά παράλληλα, χρησιμοποιώντας κάποια γενικευμένη μέθοδος, όπως την επίθεση ως προς το μήκος. Πιθανολογώντας, η επίθεση μας θα πρέπει να είναι πετυχημένη για τουλάχιστον ένα από τα b που θα επιλέξουμε.

ΚΕΦΑΛΑΙΟ IV

ΠΡΟΒΛΗΜΑΤΑ ΑΠΟΦΑΣΗΣ ΚΑΙ ΚΡΥΠΤΟΓΡΑΦΙΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

IV.1
Ορισμοί και Βασικές Έννοιες

Εισαγωγή

Σε αυτό το κεφάλαιο θα συναντήσουμε κάτι που θα φανεί οικείο σε όσους έχουν ασχοληθεί με την παραδοσιακή κρυπτογραφία. Πιο συγκεκριμένα, θα δούμε πως μπορούμε να χρησιμοποιήσουμε προβλήματα απόφασης από τη Συνδυαστική Θεωρία Ομάδων, ως το κύριο εργαλείο στην εγκατάσταση ή στα κρυπτοσυστήματα δημοσίου κλειδιού.

Ορισμός IV.1
Τα προβλήματα απόφασης έχουν την ακόλουθη μορφή:

Έστω ότι έχουμε μια ιδιότητα $\mathcal{P}$ κι ένα αντικείμενο $\mathcal{O}$ και πρέπει να βρούμε αν το αντικείμενο $\mathcal{O}$ έχει την ιδιότητα $\mathcal{P}$ ή όχι. □

Τα προβλήματα απόφασης μπορούν να μας δώσουν τη δυνατότητα να προσεγγίσουμε μέχρι κάποιο βαθμό, το ακόλουθο πρόβλημα της κρυπτογραφίας δημοσίου κλειδιού, στο οποίο επιθυμούμε να σχεδιάσουμε ένα κρυπτοσύστημα που θα είναι ασφαλές απέναντι σε (μερικές τουλάχιστον) “brute force” επιθέσεις, πίσω από τις οποίες θα βρίσκεται κάποιος επιτιθέμενος που θα διαθέτει ανεξάντλητες υπολογιστικές δυνατότητες.

Το πρόβλημα της λέξης αποτελεί ένα πιο συγκεκριμένο πρόβλημα απόφασης. Σε αυτό θα πάρουμε μια αναδρομική παράσταση μιας ομάδας G κι ένα στοιχείο $g \in G$ και θα ψάξουμε να βρούμε αν το $g = 1$ ανήκει στη G ή όχι.

Από την περιγραφή του πιο πάνω προβλήματος, διαπιστώνουμε ότι απαρτίζεται από δύο περιπτώσεις, να ανήκει το $g = 1$ στη G ή να μην ανήκει. Θα τις ονομάσουμε ως τις περιπτώσεις «ΝΑΙ» και «ΟΧΙ» αντίστοιχα. Εάν έχουμε μια ομάδα με αναδρομική παράσταση, ως προς τους γεννήτορες και τις σχέσεις, τότε η περίπτωση του «ΝΑΙ» του προβλήματος της λέξης θα έχει αναδρομική λύση, γιατί κάποιος θα μπορεί να αριθμήσει όλα τα παράγωγα των οριζουσών σχέσεων, των αντίστροφών τους και των συζυγών τους.

Παρ’ όλα αυτά, σε ένα τέτοιο γινόμενο, ο αριθμός των παραγόντων που απαιτούνται για την παράσταση μιας λέξης μήκους n, ίση με 1, στη G, θα

μπορούσε να είναι ιδιαιτέρως μεγάλη σε σχέση με το n. Ακόμη πιο συγκεκριμένα, γνωρίζουμε πως υπάρχουν ομάδες G στις οποίες το πρόβλημα της λέξης επιλύεται αποτελεσματικά και στις οποίες θα συναντήσουμε λέξεις w μήκους n ίσο με 1 (στην ομάδα G), τέτοιες ώστε ο αριθμός των παραγόντων στην οποιαδήποτε παραγοντοποίηση του w σε γινόμενο διακεκριμένων σχέσεων, αντιστρόφων και συζυγών, να μην είναι φραγμένο από κάποια εκθετική σχέση στο n. Τώρα, εάν σε κάποια ομάδα G, το πρόβλημα της λέξης δεν επιλύεται αναδρομικά, τότε και το μήκος της απόδειξης που μας δείχνει ότι το $g = 1$ στη G, δε θα είναι φραγμένο από κάποια αναδρομική συνάρτηση με μήκος το μήκος του w.

Επίσης, αξίζει να σημειώσουμε ότι η περίπτωση « ΟΧΙ» δε μπορεί να επιλυθεί αναδρομικά σε αρκετές ομάδες. Για τον λόγο αυτόν, μια περίπτωση “brute force” επίθεσης δε θα είναι αποτελεσματική. Σε αυτό το σημείο, δε θα πρέπει να αμελήσουμε να αναφέρουμε ότι δεν υπάρχει κάποια ομάδα (ή ημιομάδα), που να παριστάνεται αναδρομικά και να έχει συγχρόνως και τις δύο περιπτώσεις του προβλήματος της λέξης, τη «ΝΑΙ» και την «ΟΧΙ», μη-επιλύσιμες αναδρομικά.

IV.2
Shpilrain-Zapata

Εισαγωγή

Σε αυτήν την Ενότητα θα έχουμε την ευκαιρία να γνωρίσουμε καλύτερα ένα κρυπτογραφικό πρωτόκολλο [14] που χρησιμοποιεί την υπολογιστική δυσκολία που παρουσιάζει το πρόβλημα της λέξης στις ομάδες. Σε αυτό το πρωτόκολλο, ο Bob στέλνει στην Alice μια κρυπτογραφημένη δυαδική ακολουθία και η Alice από την πλευρά της θα προσπαθήσει να την αποκρυπτογραφήσει με πιθανότητα επιτυχίας πολύ κοντά στη μονάδα «1».

Vladimir Shpilrain

Φωτογραφία IV.1

Παλαιότερα είχαν γίνει προσπάθειες να χρησιμοποιηθεί το πρόβλημα της λέξης στην κρυπτογραφία δημόσιου κλειδιού [44], αλλά για πολλούς και διάφορους λόγους, η απόπειρα δεν στέφθηκε με επιτυχία. Ο ένας από τους λόγους αυτούς [45] ήταν κι ο εξής:

Το πρόβλημα που χρησιμοποιήθηκε στο [44], δεν είναι ακριβώς το πρόβλημα της λέξης, αλλά έχει μια ανεπαίσθητη διαφοροποίηση ως προς τη διατύπωση. Έτσι, μπορούμε να πούμε ότι πρόκειται για το πρόβλημα επιλογής της λέξης, στο οποίο έστω ότι έχουμε $g, w_1, w_2 \in G$ και θέλουμε να βρούμε αν $g = w_1$ ή $g = w_2$ στη G, δεδομένου ότι μια από τις δύο ισότητες ισχύει. Σε αυτήν την

εκδοχή του προβλήματος, για κάθε ομάδα G που θα χρησιμοποιήσουμε και η οποία μπορεί να παρασταθεί αναδρομικά, και τα δύο μέρη του είναι επιλύσιμα αναδρομικά. Ο λόγος είναι ότι και τα δύο μέρη ανήκουν στη θετική «ΝΑΙ» έκβαση του προβλήματος της λέξης, οπότε και η προαναφερθείσα εκδοχή του προβλήματος επιλογής της λέξης, δε μπορεί να χρησιμοποιηθεί για το σκοπό μας.

Κατά συνέπεια δεν πρέπει να συγχέουμε τη λογική του πιο κάτω πρωτοκόλλου [14] που θα αναλύσουμε, με αυτό που χρησιμοποιήθηκε στο [44], διότι δεν ταυτίζονται. Αντιθέτως, το πιο κάτω φαίνεται να είναι και η πρώτη απόπειρα να χρησιμοποιηθεί ένα πρόβλημα απόφασης.

IV.2.1 Το Πρωτόκολλο

Πρωτόκολλο IV.1
Ένα γενικό περίγραμμα του πρωτοκόλλου [14] για το οποίο θα μιλήσουμε είναι το πιο κάτω. Θα έχουμε την ευκαιρία να το δούμε αναλυτικότερα και πιο κάτω:

Βήματα

1. Έστω ότι έχουμε μερικές παραστάσεις δημόσιων ομάδων που έχουν το πρόβλημα της λέξης επιλύσιμο (π.χ. ας θεωρήσουμε ότι είναι μέρος του λογισμικού της Alice).

2. Η Alice επιλέγει τυχαία μια συγκεκριμένη παράσταση Γ από τις πιο πάνω διαθέσιμες, τη διαφοροποιεί με μετασχηματισμούς που διατηρούν τον ισομορφισμό, έτσι ώστε να πάρει μια διαφοροποιημένη παράσταση Γ', απορρίπτοντας μερικές από τις σχέσεις και δημοσιοποιεί τη συντομευμένη διαφοροποιημένη παράσταση $\hat{\Gamma}$.

3. Ο Bob θα στείλει την ιδιωτική δυαδική ακολουθία στην Alice με την εκπομπή ενός στοιχείο ίσο προς το 1 στη $\hat{\Gamma}$ (οπότε και στη Γ'), αντί του «1» κι ένα στοιχείο διάφορο από το 1 στη Γ', στη θέση του «0».

4. Η Alice θα ανακτήσει τη δυαδική ακολουθία του Bob με το να μετατρέψει τα στοιχεία του Γ' (χρησιμοποιώντας τον ισομορφισμό που γνωρίζει) στα αντίστοιχα του Γ, και κατά συνέπεια θα επιλύσει το πρόβλημα της λέξης στη Γ.

Τα πιο πολλά μέρη αυτού του πρωτοκόλλου είναι μη-τετριμμένα και ανοίγουν πολλά και ενδιαφέροντα πεδία έρευνας. Θα δούμε πιο αναλυτικά τα βήματα 1, 2 και 3 στις παρακάτω ενότητες IV.2.2, IV.2.3, IV.2.4 αντίστοιχα.

Εκ πρώτης όψεως, φαίνεται ότι το πλέον μη-τετριμμένο μέρος είναι η εύρεση ενός στοιχείου που δε θα είναι ίσο με το 1 στη Γ', αφού ο Bob δε γνωρίζει την παράσταση Γ'. Θα προσπαθήσουμε να επιλύσουμε το πρόβλημα μέσω της «περπατημένη», δηλαδή θα αφήσουμε τον Bob να επιλέξει μια τυχαία (σχεδόν τυχαία) λέξη ικανοποιητικά μεγάλου μήκους και θα δείξει μέσω της συντριπτικής πιθανότητας, ότι ένα τέτοιο στοιχείο δεν είναι ίσο προς το 1 στη Γ'.

Σε αυτό το σημείο ας επισημάνουμε και πάλι ποια είναι η καινοτομία που παρουσιάζει το συγκεκριμένο πρωτόκολλο, σε σύγκριση με τα ήδη υπάρχοντα. Το ζητούμενο είναι να στερήσει από τον επιτιθέμενο τη δυνατότητα να επιτεθεί στο πρωτόκολλο μέσω μια εκτεταμένης και εξαντλητικής αναζήτησης των διαθέσιμων δημόσιων κλειδιών του αποστολέα, κάτι που είναι και ο πλέον προφανής (αν και μερικές φορές «υπολογιστικά αδύνατο) τρόπος επίθεσης σε όλα τα υπάρχοντα πρωτόκολλα δημοσίου κλειδιού.

Ο τρόπος μέσω του οποίου σχεδιάζουμε να πετύχουμε το στόχο μας είναι παρεμφερής με το βήμα 3 του πιο πάνω πρωτοκόλλου, και πιο συγκεκριμένα, την επίλυση του προβλήματος της λέξης στη $\hat{\Gamma}$. Εάν ο Bob στείλει ένα στοιχείο g ίσο με 1, στη $\hat{\Gamma}$, τότε ο επιτιθέμενος ίσως να μπορέσει να το εντοπίσει με το να διατρέξει όλα τα προϊόντα των συζυγών σχέσεων και των αντίστροφών τους. Το σύνολο αυτό είναι αναδρομικό, αλλά όπως έχουμε πει και στην Εισαγωγή, υπάρχουν ομάδες G με επιλύσιμο το πρόβλημα της λέξης και με λέξεις w μήκους n ίσές με 1 στη G, τέτοιες ώστε το μήκος της απόδειξης που πιστοποιεί ότι $w = 1$ στη G δεν είναι φραγμένο από κάποια εκθετική σχέση στο n.

Επιπλέον, εάν ο Bob μεταδώσει ένα στοιχείο g άνισο προς το 1, στη $\hat{\Gamma}$, τότε ο εντοπισμός του από τον επιτιθέμενο θα γίνει ακόμη πιο δύσκολος. Σε γενικές γραμμές, θα μπορούσαμε να πούμε ότι είναι και αδύνατο. Στη καλύτερη των περιπτώσεων, η ελπίδα του επιτιθέμενου είναι αν βρει κάποια ομάδα παραγόντων της $\hat{\Gamma}$, στην οποία το πρόβλημα της λέξης είναι επιλύσιμο, και κατά συνέπεια, στην πιο πάνω ομάδα παραγόντων, θα έχουμε ότι $g \neq 1$. Αυτού του είδους την επίθεση την ονομάζουμε και «Επίθεση Πηλίκου».

Τώρα, ας δούμε λίγο καλύτερα τον τρόπο επίθεσης που χρησιμοποιεί ο επιτιθέμενος:

Ο επιτιθέμενος παράγει συνεχώς κλειδιά και κάθε φορά χρησιμοποιεί και μια εντελώς νέα τυχαιότητα, μέχρι που θα πάρει τη μετάδοση στην οποία θέλει να επιτεθεί. Αυτό συμβαίνει με συντριπτική πιθανότητα. Η ορθότητα του πιο πάνω συστήματος εξασφαλίζει ότι το αντίστοιχο μυστικό κλειδί που προκύπτει από την αλλεπάλληλη παραγωγή κλειδιών, μας επιτρέπει την παράνομη αποκρυπτογράφηση.

Όντως, αυτό θα ήταν εφικτό εάν η ορθότητα της όποιας αποκρυπτογράφησης από την Alice ήταν τέλεια. Όμως, στην περίπτωσή μας, αυτού του είδους η επίθεση θα μπορούσε και να μην αποδώσει για μια γενική $\hat{\Gamma}$. Ας υποθέσουμε ότι ο επιτιθέμενος κατασκευάζει δύο λίστες που αντιστοιχούν σε δύο πιθανές κρυπτογραφήσεις «$0 \to w \neq 1$ στη $\hat{\Gamma}$» ή «$1 \to w = 1$ στη $\hat{\Gamma}$» του Bob. Η πρώτη μας παρατήρηση είναι ότι η λίστα που αντιστοιχεί στο «$0 \to w \neq 1$» θα είναι άχρηστη στον επιτιθέμενο, επειδή θα περιέχει όλες τις λέξεις στο αλφάβητο $X = \{x_1, \dots, x_n, x_1^{-1}, \dots x_n^{-1}\}$, καθώς ο Bob επιλέγει τυχαία τη λέξη w. Για τον λόγο αυτόν, ο επιτιθέμενος θα μπορούσε να αγνοήσει τη λίστα αυτή και να ασχοληθεί με την άλλη που αντιστοιχεί στο «$1 \to w = 1$».

Η όλη κατάσταση μας οδηγεί στο ακόλουθο:

Εάν μια λέξη w που μεταδίδει ο Bob εμφανιστεί στη λίστα, τότε θα είναι ίση με 1 στη G. Εάν δεν εμφανιστεί, τότε δε θα είναι ίση. Το μόνο πρόβλημα είναι ότι:

Πώς μπορεί ο επιτιθέμενος να αποφανθεί ότι η w δεν εμφανίζεται στη λίστα, εάν η λίστα είναι άπειρη; Κάποιος θα μπορούσε να πει ότι κάποια στιγμή ο επιτιθέμενος θα σταματήσει και θα θεωρήσει πως με συντριπτική πιθανότητα ισχύει πως $w \neq 1$, ακριβώς με τον ίδιο τρόπο που το κάνει και η Alice. Το θέμα μας όμως είναι ότι αυτή η πιθανότητα μπορεί να μην είναι το ίδιο συντριπτική με την πιθανότητα που έχει η Alice να προβεί σε σωστή αποκρυπτογράφηση.

Η σύγκριση γίνεται μεταξύ των:

1. Για την Alice, το να προβεί στη σωστή αποκρυπτογράφηση, η πιθανότητα $P_1(N)$ για μια τυχαία λέξη w, μήκους N, να μην είναι ίση με το 1, θα συγκλίνει σχετικά γρήγορα προς το 1, καθώς το N τείνει στο άπειρο.

2. Για τον επιτιθέμενο, το να έχει μια σωστή αποκρυπτογράφηση με υψηλή πιθανότητα, σημαίνει πως η πιθανότητα $P_2(N, f(N))$ για μια

τυχαία λέξη w, μήκους N, η οποία θα είναι ίση με 1, να έχει μια απόδειξη μήκους $\leq f(N)$ που να πιστοποιεί ότι $w = 1$, θα συγκλίνει γρήγορα στο 1, καθώς το N τείνει στο άπειρο. Να επεξηγήσουμε σε αυτό το σημείο ότι το $f(N)$ παριστάνει την υπολογιστική ισχύ του επιτιθέμενου. Πρόκειται για μια συνάρτηση που θα μπορούσε να είναι τυχαία, αλλά πάντα σταθερή.

Εύκολα παρατηρούμε πως οι συναρτήσεις $P_1(N)$ και $P_2(N, f(N))$ έχουν έντονες διαφορές μεταξύ τους και κατά συνέπεια, η όποια συσχέτιση μεταξύ τους δεν ευσταθεί.

Να σημειώσουμε σε αυτό το σημείο ότι η συνάρτηση $P_1(N)$, γενικά είναι ευκολότερα αντιληπτή και πιο συγκεκριμένα, γνωρίζουμε πως σε κάθε άπειρη ομάδα G, το $P_1(N)$ όντως συγκλίνει σχετικά γρήγορα προς το 1, καθώς το N τείνει στο άπειρο. Από την άλλη, οι συναρτήσεις $P_2(N, f(N))$ είναι πιο σύνθετες. Αποτελούν αντικείμενο μελέτης και ερευνών και θα μπορούσε να αποδειχθεί πως για κάθε $f(N)$, υπάρχουν ομάδες στις οποίες οι $P_2(N, f(N))$ δε συγκλίνουν ποτέ στο 1. Αλλά δε θα επεκταθούμε περαιτέρω σε αυτό το σημείο.

Ολοκληρώνοντας την ενότητα, θα μπορούσαμε να πούμε πως η κρυπτογράφηση του ενός bit σε αυτό το πρωτόκολλο είναι κάτι παραπάνω από αποτελεσματική. Κι ο λόγος είναι επειδή θα χρειαστεί τετραγωνικό χρόνο ως προς το μήκος της μεταδιδόμενης λέξης. Επίσης, είναι προφανές και αξίζει να παρατηρήσουμε ότι ο χρόνος που χρειάζεται η Alice για να αποκρυπτογραφήσει κάθε μεταδιδόμενη λέξη w είναι φραγμένος από $C \cdot |w|$, όπου $|w|$ είναι το μήκος της λέξης w και C είναι μια σταθερά που συσχετίζεται με τον ιδιωτικό ισομορφισμό της Alice για τα Γ, Γ'.

Το γεγονός πως η Alice, που είναι ο παραλήπτης, κι ο επιτιθέμενος διαφοροποιούνται ως προς την ισχύ, οφείλεται κυρίως στο ότι η Alice γνωρίζει τον ιδιωτικό της ισομορφισμό μεταξύ των Γ και Γ'. Μην ξεχνάμε ότι ο Bob δε χρειάζεται να γνωρίζει αυτόν τον ισομορφισμό για να προβεί στην κρυπτογράφηση.

Θα πρέπει όμως να παραδεχθούμε ένα μεγάλο αρνητικό που έχει αυτό το πρωτόκολλο, συγκρινόμενο με τα υπόλοιπα, ευρέως διαδεδομένα πρωτόκολλα δημοσίου κλειδιού. Πρόκειται για μια κρυπτογράφηση με ιδιαίτερα μεγάλο συντελεστή διαστολής. Πρόχειροι πειραματισμοί με τη χρήση υπολογιστή, έχουν δείξει πως για συγκεκριμένες παραμέτρους, ένα bit από το μήνυμα του Bob, θα κρυπτογραφηθεί σε μια λέξη μήκους περίπου 150 κατά μέσο όρο. Αυτό μας δημιουργεί πρόβλημα, εάν δώσουμε πολύ μεγάλη υπολογιστική ισχύ στον επιτιθέμενο.

IV.2.1 Πλήθος παραστάσεων ομάδας

Υπάρχουν πολλές κλάσεις ομάδων με πεπερασμένη παράσταση, οι οποίες έχουν επιλύσιμο το πρόβλημα της λέξης. π.χ. ομάδες μιας σχέσης, υπερβολικές ομάδες και μετα-αβελιανές ομάδες. Όμως, η Alice θα πρέπει να είναι σε θέση να επιλέξει αποτελεσματικά μια τυχαία παράσταση ανάμεσα από τις υπόλοιπες, κάτι που συνεπάγεται κάποιους περιορισμούς στις κλάσεις των παραστάσεων που θα μπορούσαν να χρησιμοποιηθούν γι' αυτόν τον σκοπό. Εμείς θα προτείναμε την κλάση των ομάδων που παριστάνονται πεπερασμένα και ονομάζονται ομάδες περιορισμένης ακύρωσης.

Οι ομάδες περιορισμένης ακύρωσης έχουν σχέσεις που ικανοποιούν μια απλή και αποτελεσματικά πιστοποιήσιμη «κατάσταση». Πιο συγκεκριμένα, έστω ότι έχουμε την ελεύθερη ομάδα $F(X)$ με βάση το $X = \{x_i | i \in I\}$, όπου το I είναι το ταυτοτικό σύνολο. Έστω ότι $\varepsilon_k \in \{\pm 1\}$, όπου $1 \leq k \leq n$. Μια λέξη $w(x_1, \dots, x_n) = x_{i_1}^{\varepsilon_1} x_{i_2}^{\varepsilon_2} \dots x_{i_n}^{\varepsilon_n}$ στην $F(X)$, με όλα τα x_{i_k} να μην είναι κατά ανάγκη διακεκριμένα, θα είναι μια X-λέξη που θα μπορεί να αναχθεί αν $x_{i_k}^{\varepsilon_k} \neq x_{i_{k+1}}^{-\varepsilon_{k+1}}$, για $1 \leq k \leq n-1$. Επιπροσθέτως, η λέξη $w(x_1, \dots, x_n)$ μπορεί να αναχθεί κυκλικά, εάν είναι μια X-λέξη που ανάγεται και ισχύει $x_{i_1}^{\varepsilon_1} \neq x_{i_n}^{-\varepsilon_n}$. Ένα σύνολο R, που περιέχει λέξεις από το $F(X)$, οι οποίες μπορούν να ανάγονται κυκλικά, θα είναι συμμετρικό εάν είναι κλειστό ως προς τις κυκλικές μεταθέσεις και δέχεται αντίστροφες.

Έστω ότι έχουμε μια ομάδα G, με παράσταση $\langle X; R \rangle$. Μια μη κενή λέξη $u \in F(X)$ θα ονομάζεται «τμήμα», εάν υπάρχουν δύο διακεκριμένες σχέσεις $r_1, r_2 \in R$ της G, τέτοιες ώστε $r_1 = uv_1$ και $r_2 = uv_2$ για κάποια $v_1, v_2 \in F(X)$, χωρίς να υπάρχει κάποια ακύρωση μεταξύ των u και v_1 ή μεταξύ των u και v_2. Η ομάδα G ανήκει στην κλάση $C(p)$, εάν κανένα στοιχείο της R δεν είναι προϊόν με λιγότερα από p τμήματα. Επίσης, η ομάδα G ανήκει στην κλάση $C'(\lambda)$ αν για κάθε $r \in R$, τέτοιο ώστε $r = uv$ όπου u είναι τμήμα, έχουμε $|u| < \lambda |r|$.

Πιο συγκεκριμένα, εάν η G ανήκει στην κλάση $C'(\frac{1}{6})$, τότε μπορούμε να επιλύσουμε αποτελεσματικά το πρόβλημα της λέξης με τον αλγόριθμο του Dehn. Αυτός ο αλγόριθμος θα έχει πολυπλοκότητα τετραγωνικού χρόνου ως προς το μήκος της λέξης w που εισάγουμε.

Επίσης παρατηρούμε πως γενικώς, μια ομάδα που παριστάνεται πεπερασμένα είναι και μια ομάδα περιορισμένης ακύρωσης. Για τον λόγο αυτό, προκειμένου να επιλέξει μια ομάδα περιορισμένης ακύρωσης, η Alice επιλέγει απλώς μερικές τυχαίες λέξεις και ελέγχει εάν το αντίστοιχο συμμετρικό σύνολο ικανοποιεί τη συνθήκη για $C'(\frac{1}{6})$. Αν όχι, το επαναλαμβάνει εκ νέου.

Πρωτόκολλο IV.2

Ολοκληρώνοντας και αυτήν την ενότητα, θα δώσουμε ένα πιο συγκεκριμένο σύστημα, με παραδειγματικές παραμέτρους, έτσι ώστε η Alice να μπορέσει να παράγει μια παράσταση Γ για το πρωτόκολλο:

1. Η Alice θα επιλέξει ένα αριθμό k, με $10 \leq k \leq 20$, από γεννήτορες στην παράσταση της Γ. Οπότε η Γ παράστασή της, θα έχει τους γεννήτορες $x_1, \dots, x_k$.

2. Η Alice θα επιλέξει m τυχαίες λέξεις $r_1, \dots, r_m$ εκ των γεννητόρων $x_1, \dots, x_k$. Ισχύει ότι $10 \leq m \leq 30$ και τα μήκη l_i των r_i είναι τυχαίοι ακέραιοι από το διάστημα $L_1 \leq l_i \leq L_2$. Μερικές πιο συγκεκριμένες τιμές που θα προτείναμε είναι οι: $L_1 = 12, L_2 = 20$.

3. Μόλις η Alice επιλέξει την συντομευμένη παράσταση $\hat{\Gamma}$, θα προσθέσει σε αυτήν την ακόλουθη σχέση:

$$x'_i = \prod_{j=1}^{M} [x'_i, w_j]$$

όπου x'_i είναι ένας γεννήτορας που επιλέγεται τυχαία από τη $\hat{\Gamma}$, τα w_j είναι τυχαία στοιχεία μήκους 1 ή 2 εκ των γεννητόρων $x'_1, x'_2, \dots$, και $M = 10$. Στη συνέχεια, η Alice θα βρει μια πρώτη εικόνα τις προαναφερθείσας σχέσης συναρτήσει του ισομορφισμού μεταξύ των Γ και $\hat{\Gamma}$ και θα προσθέσει αυτήν την πρώτη εικόνα στις ορισμένες σχέσεις της Γ. Για τον λόγο αυτόν, η Γ έχει k γεννήτορες και $m + 1$ ορισμένες σχέσεις.

4. Τελικώς, η Alice θα ελέγξει εάν η ιδιωτική της παράταση Γ, ικανοποιεί τη συνθήκη περιορισμένης ακύρωσης $C'(\frac{1}{6})$. Εάν δεν την ικανοποιεί, θα ξεκινήσει και πάλι από την αρχή.

□

IV.2.3 Μετασχηματισμοί Tietze - Στοιχειώδεις ισομορφισμοί

Σε αυτήν την ενότητα θα εξηγήσουμε τι θα χρησιμοποιήσει η Alice ώστε να μπορέσει να εφαρμόσει το Βήμα 2 του πρωτοκόλλου που παρουσιάσαμε στην αρχή του Κεφαλαίου. Για να το κάνουμε αυτό, πρέπει πρώτα να δούμε ποιοι είναι οι μετασχηματισμοί Tietze. Πρόκειται για στοιχειώδεις ισομορφισμούς. Με άλλα λόγια, κάθε ισομορφισμός μεταξύ ομάδων που παριστάνονται πεπερασμένα είναι μια σύνθεση μετασχηματισμών Tietze. Αυτό που είναι σημαντικό για εμάς είναι ότι κάθε μετασχηματισμός Tietze μπορεί εύκολα να αντιστραφεί, και κατά συνέπεια η Alice μπορεί να υπολογίσει τον αντίστροφο ισομορφισμό που θα την οδηγήσει από το Γ' στο Γ.

Θεώρημα IV.1
Ο Tietze εισήγαγε για τους στοιχειώδεις μετασχηματισμούς που διατηρούν τον ισομορφισμό πως μπορούν να εφαρμοστούν σε ομάδες που παριστάνονται από γεννήτορες και σχέσεις. Αυτοί θα έχουν την ακόλουθη μορφή:

1. (T1)
   Εισάγοντας έναν νέο γεννήτορα:
   Θα αντικαταστήσουμε τα:
   $$\langle x_1, x_2, \dots | r_1, r_2, \dots \rangle \text{ με } \langle y, x_1, x_2, \dots | y s^{-1}, r_1, r_2, \dots \rangle,$$
   όπου $s = s(x_1, x_2, \dots)$ είναι ένα τυχαίο στοιχείο εκ των γεννητόρων $x_1, x_2, \dots$

2. (T2)
   Η ακύρωση ενός γεννήτορα (πρόκειται για το αντίστροφο της (T1)):
   Εάν έχουμε μια παράσταση τη μορφής $\langle y, x_1, x_2, \dots | q, r_1, r_2, \dots \rangle$, όπου το q είναι της μορφής $y s^{-1}$ και τα $s, r_1, r_2, \dots$ ανήκουν σε μια ομάδα που προκύπτει από τα $x_1, x_2, \dots$, τότε θα αντικαταστήσουμε αυτήν την παράσταση με $\langle x_1, x_2, \dots | r_1, r_2, \dots \rangle$.

3. (T3)
   Εφαρμόζοντας έναν αυτομορφισμό:
   Θα εφαρμόσουμε ένα αυτομορφισμό της ελεύθερης ομάδας που παράγεται από τα $x_1, x_2, \dots$, σε όλες τις σχέσεις $r_1, r_2, \dots$

4. (T4)
   Αλλάζοντας τις ορισμένες σχέσεις:
   Θα αντικαταστήσουμε το σύνολο $r_1, r_2, \dots$ των ορισμένων σχέσεων με ένα άλλο σύνολο $r'_1, r'_2, \dots$ με το ίδιο κανονικό κλείσιμο. Αυτό σημαίνει ότι κάθε ένα από τα $r'_1, r'_2, \dots$ θα πρέπει να ανήκει στην κανονική υποομάδα που παράγεται από τα $r_1, r_2, \dots$ και αντιστρόφως.

□

Ο Tietze απέδειξε ότι δύο ομάδες $\langle x_1, x_2, \dots | r_1, r_2, \dots \rangle$ και $\langle x_1, x_2, \dots | s_1, s_2, \dots \rangle$ είναι ισόμορφες αν και μόνον αν κάποιος μπορεί να μεταβεί από την μια παράσταση στην άλλη, ύστερα από μια ακολουθία μετασχηματισμών (Τ1)-(Τ4).

Δε θα επεκταθούμε περαιτέρω ως προς το πώς η Alice χρησιμοποιεί τους προαναφερθέντες μετασχηματισμούς Tietze, καθότι πρόκειται για πολύ λεπτομερή ανάλυση, που ξεφεύγει από τα όρια ενδιαφέροντος της παρούσας εργασίας.

IV.2.4 Παράγοντας τυχαία στοιχεία σε πεπερασμένες παραστάσεις ομάδων

Σε αυτήν την ενότητα θα δούμε μερικά πράγματα που αφορούν την εφαρμογή του Βήματος 3, του πρωτοκόλλου που παρουσιάσαμε στην αρχή του Κεφαλαίου.

Έτσι, όταν ο Bob θέλει να μεταδώσει ένα στοιχείο ίσο με το 1, στη $\hat{\Gamma}$, θα πρέπει να κατασκευάσει μια λέξη, που να δείχνει όσο γίνεται πιο τυχαία, στις σχέσεις $\hat{r}_1, \dots, \hat{r}_l$ και στα συζυγή τους. Όμως, όταν θα θέλει να μεταδώσει ένα στοιχείο που δε θα είναι ίσο με το 1, στη $\hat{\Gamma}$, θα επιλέξει μια τυχαία λέξη με αρκετά μεγάλο μήκος. Έχει αποδειχθεί με συντριπτική πιθανότητα, ότι ένα τέτοιο στοιχείο δεν είναι ίσο προς το 1, στη Γ'.

Θα ξεκινήσουμε την αναφορά μας με μια περιγραφή της πιθανής τακτικής που θα εφαρμόσει ο Bob για τη διαμόρφωση των παραγόμενων στοιχείων που θα είναι ίσα με 1, στη $\hat{\Gamma}$. Όταν ο Bob θα στείλει μια λέξη w ίση προς το 1, στη $\hat{\Gamma}$, θα ήθελε να τη διαμορφώσει κατά τέτοιον τρόπο ώστε μεγάλα τμήματα των ορισμένων σχέσεων να μη μπορούν να θεαθούν στη w. Σε ορισμένες ομάδες (π.χ. στις ομάδες πλεξίδων), η προαναφερθείσα διαμόρφωση θα παρέχεται από μια «κανονική μορφή», η οποία θα είναι η συλλογή συμβόλων που αντιστοιχούν κατά μοναδικό τρόπο σε ένα δεδομένο στοιχείο της ομάδας. Η ύπαρξη τέτοιων κανονικών μορφών οφείλεται συνήθως σε κάποιες ειδικές αλγεβρικές ή γεωμετρικές ιδιότητες μιας δεδομένης ομάδας.

Παρ' όλα αυτά, καθότι ο Bob δε γνωρίζει τυχόν σημαντικές ιδιότητες της ομάδας που ορίζεται από την παράσταση $\hat{\Gamma}$ που του δίνεται, δε θα μπορέσει να εφαρμόσει τυχόν κανονικές μορφές κατά τον συνήθη τρόπο. Η μόνη χρήσιμη ιδιότητα που έχει η παράσταση $\hat{\Gamma}$ είναι το γεγονός ότι οι περισσότερες εκ των σχέσεων της έχουν μήκος 3 ή 4. Θα εκμεταλλευτούμε την ιδιότητα αυτή με τον ακόλουθο τρόπο, που θα τον ονομάσουμε και «ανακάτεμα»:

1. Θα πάρουμε το γινόμενο της μορφής $u = s_1 \cdots s_p$, όπου το κάθε s_i επιλέγεται τυχαία ανάμεσα από τις ορισμένες σχέσεις $\hat{r}_1, \hat{r}_2, \dots$, μήκους 3 ή 4, τα αντίστροφά τους και τις συζυγείς λέξεις κατά ένα ή δύο γράμματα στο $x'_1, x'_2, \dots$. Ο αριθμός p των παραγόντων θα πρέπει να είναι αρκετά μεγάλος, τουλάχιστον 10 φορές πιο μεγάλος από τον αριθμό των ορισμένων σχέσεων στη $\hat{\Gamma}$.

2. Θα εισάγουμε περίπου $\frac{2p}{k}$ εκφράσεις της μορφής $x'_j (x'_j)^{-1}$ ή $(x'_j)^{-1} x'_j$ σε τυχαία σημεία της λέξης u (με το k να είναι ο αριθμός των γεννητόρων x'_i της $\hat{\Gamma}$), για τυχαίες τιμές του j.

3. Πηγαίνοντας από αριστερά προς τα δεξιά στη λέξη u, θα αναζητήσουμε υπο-λέξεις με δύο γράμματα που θα είναι μέρη των ορισμένων σχέσεων $\hat{r}_i$ μήκους 3 ή 4. Μόλις εντοπίσουμε μια τέτοια υπολέξη, θα την αντικαταστήσουμε με το αντίστροφο του αυξανόμενου μέρους της ίδιας ορισμένης σχέσης και θα συνεχίσουμε. Για παράδειγμα, έστω ότι υπάρχει μια σχέση $\hat{r}_i = x'_1 x'_2 x'_3 x'_4$ και έστω ότι εντοπίσαμε μια τέτοια υπολέξη $x'_1 x'_2$ στη u. Τότε θα την αντικαταστήσουμε με $(x'_4)^{-1}(x'_3)^{-1}$. Είναι προφανές πως στην ομάδας μας θα έχουμε $x'_1 x'_2 = (x'_4)^{-1}(x'_3)^{-1}$. Εάν τώρα εντοπίσουμε την υπολέξη $x'_2 x'_3$ στη w, θα την αντικαταστήσουμε με $(x'_1)^{-1}(x'_4)^{-1}$. Τέλος, εάν έχουμε περισσότερες από μια επιλογές για αντικατάσταση, θα επιλέξουμε μια εκ αυτών κατά τυχαίο τρόπο.

4. Θα ακυρώσουμε τυχόν εναπομείναντες υπολέξεις της μορφής $x'_j(x'_j)^{-1}$ ή $(x'_j)^{-1}x'_j$.

Για να πετύχουμε ένα καλό ανακάτεμα, θα πρέπει να τρέξουμε τα βήματα (2)-(4) περίπου p φορές.

Δε θα αναλύσουμε περαιτέρω τη συγκεκριμένη ενότητα, καθότι ξεφεύγει από τα όρια ενδιαφέροντος της παρούσας εργασίας.

IV.2.5 Επίθεση Ισομορφισμού

Σε αυτήν την ενότητα θα συζητήσουμε σε θεωρητικό επίπεδο για πιθανή «brute force» επίθεση στο πρωτόκολλο που αναλύσαμε στην αρχή του Κεφαλαίου.

Εάν ο επιτιθέμενος γνωρίζει τις παραστάσεις ομάδων εκ των οποίων η Alice θα επιλέξει την ιδιωτική της παράσταση Γ, θα προσπαθήσει να αυξήσει τη δημόσια παράσταση $\hat{\Gamma}$ σε μια παράσταση που θα είναι ισόμορφη προς κάποια από αυτές που διατίθενται στην Alice. Μιλώντας θεωρητικά, αυτό είναι εφικτό καθότι το σύνολο των δοσμένων παραστάσεων είναι αναδρομικό και επειδή και το σύνολο των πεπερασμένων παραστάσεων που είναι ισομορφικές προς μια δοσμένη είναι επίσης αναδρομικό. Όμως, μια τέτοια απόπειρα θα απαιτούσε τεράστια μεγέθη ισχύος. Ας προσπαθήσουμε όμως να το δούμε λίγο καλύτερα.

Ο επιτιθέμενος μπορεί να προσθέσει στη $\hat{\Gamma}$ ένα στοιχείο κάθε φορά και να ελέγξει εάν η τελική παράσταση, έστω η $\hat{\Gamma}_+$, είναι ισομορφική προς μια από τις παραστάσεις που είναι διαθέσιμες στην Alice. Για να το πετύχει αυτό ακολουθεί τα εξής. Έστω ότι ο επιτιθέμενος θέλει να ελέγξει εάν η $\hat{\Gamma}_+$ είναι ισομορφική προς κάποια Γ_i. Θα προσπελάσει όλες τις αντιστοιχήσεις από το Γ_i στο $\hat{\Gamma}_+$, μια κάθε φορά, ορισμένη εκ των γεννητόρων της Γ_i. Την ίδια στιγμή, θα προσπελάσει και όλες τις αντιστοιχήσεις από το $\hat{\Gamma}_+$ στο Γ_i που ορίζονται από τους γεννήτορες της $\hat{\Gamma}_+$.

Κατά αυτόν τον τρόπο, ο επιτιθέμενος θα δημιουργήσει διάφορα ζεύγη με τέτοιες αντιστοιχήσεις και θα ελέγξει:

1. Εάν θα πάρει την ταυτοτική αντιστοίχιση της Γ_i, και

2. Εάν και οι δύο αντιστοιχήσεις σε ένα τέτοιο ζεύγος είναι ισομορφισμοί.

Εάν έχουμε το πρόβλημα της λέξης επιλύσιμο στη Γ_i, τότε ο πιο πάνω έλεγχος θα είναι περισσότερο αποτελεσματικός. Όμως, στην πραγματικότητα δεν είναι και απαραίτητο, γιατί αυτό που μας ενδιαφέρει σε αυτήν την περίπτωση είναι το μέρος του «ΝΑΙ» του προβλήματος της λέξης, το οποίο είναι πάντα αναδρομικό.

Τώρα, ας συγκεντρωθούμε στο μέρος του όλου εγχειρήματος, στο οποίο ο επιτιθέμενος δουλεύει με μια συγκεκριμένη παράσταση Γ_i από αυτές που είναι διαθέσιμες προς την Alice. Ας υποθέσουμε ότι η Γ_i δεν είναι ισόμορφη προς την $\hat{\Gamma}_+$. Επειδή το μέρος «ΟΧΙ» του προβλήματος ισομορφισμού μεταξύ

των $\hat{\Gamma}_+$ και Γ_i δεν είναι αναδρομικό, ο επιτιθέμενος θα πρέπει να δοκιμάσει διάφορα ζεύγη αντιστοιχίσεων μεταξύ των $\hat{\Gamma}_+$ και Γ_i επ' αόριστόν. Για τον λόγο αυτόν ο επιτιθέμενος θα πρέπει να βρει κάποια αποθέματα υπολογιστικής μνήμης ώστε να ελέγξει το προαναφερθέν συγκεκριμένο Γ_i. Όμως, καθότι ο αριθμός των Γ_i αυξάνει εκθετικά με το μέγεθος της παράστασης (που είναι το συνολικό μήκος των σχέσεων), ο επιτιθέμενος θα χρειαστεί κατ' ουσία ανεξάντλητα αποθέματα χώρου αποθήκευσης, κάτι που συνεπάγεται ότι αργά ή γρήγορα θα εξαντλήσει όλα τα αποθεματικά του.

Τέλος, ολοκληρώνοντας την ενότητα, θα θέλαμε να πούμε ότι ίσως και να υπάρχουν πιο έξυπνοι τρόποι για να βρούμε μια παράσταση περιορισμένης ακύρωσης που να είναι ισομορφική προς τη $\hat{\Gamma}_+$, αλλά ελπίζουμε ότι έχουμε πείσει τον αναγνώστη ότι (τουλάχιστον, στη χειρότερη περίπτωση), αυτή η αναζήτηση θα απαιτήσει ουσιαστικά απεριόριστη υπολογιστική ισχύ.

IV.3
Κρυπτογράφηση Δημοσίου κλειδιού και επιθέσεις κρυπτογραφικής προσομοίωσης

Εισαγωγή

Σε αυτήν την Ενότητα θα συνεχίσουμε να μελετάμε το πως η μη-αναδρομικότητα ενός προβλήματος απόφασης θα μπορούσε να χρησιμοποιηθεί στην κρυπτογραφία δημοσίου κλειδιού. Θα ακολουθήσουμε την αναφορά στο [46].

Θα διερευνήσουμε την επίθεση «encryption emulation (κρυπτογράφηση μίμησης)» πάνω στις μεταδόσεις που κάνει ο αποστολέας, δηλαδή ο Bob. Θα δείξουμε ότι η κρυπτογραφία του Bob μπορεί να γίνει αρκετά ασφαλή απέναντι στις επιθέσεις «encryption emulation (κρυπτογράφησης μίμησης)», από έναν επιτιθέμενο που έχει απεριόριστη υπολογιστική ισχύ, με μια όμως προϋπόθεση: ότι ο νόμιμος παραλήπτης θα μπορεί να αποκρυπτογραφήσει σωστά με πιθανότητα που μπορεί να προσεγγίσει το 1, αλλά δε γίνεται ποτέ ίση με 1.

Κατ' αρχάς, πρέπει να θυμηθούμε από το όσα έχουμε πει στην αρχή του Κεφαλαίου, ότι η επίθεση «encryption emulation (με κρυπτογράφηση μίμησης» θα μπορούσε να δουλέψει τέλεια (τουλάχιστον για έναν επιτιθέμενο με απεριόριστη υπολογιστική ισχύ), εάν η ορθότητα του συστήματος ήταν τέλεια. Όμως, αν υπάρχει κάποιο κενό, χωρίς να έχει σημασία πόσο μικρό είναι, μεταξύ του 1 και της πιθανότητας της πετυχημένης αποκρυπτογράφησης από τον νόμιμο παραλήπτη, τότε αυτό το κενό μπορεί να ενισχυθεί σημαντικά για τον επιτιθέμενο, κάνοντας την πιθανότητα επιτυχίας της παράνομης αποκρυπτογράφησης να φέρει συντριπτική πλειοψηφία.

Σε αυτό το σημείο θα πρέπει να τονίσουμε ότι στο πρωτόκολλο που έχουμε περιγράψει δεν έχουμε κάνει αναφορά στην ασφάλεια απέναντι στην επίθεση «encryption emulation (κρυπτογράφηση μίμησης» ή απέναντι σε όποια άλλη επίθεση που γίνεται στο δημόσιο κλειδί του παραλήπτη, από έναν επιτιθέμενο με απεριόριστη υπολογιστική ισχύ. Αυτό που ισχυριζόμαστε αφορά μόνον την ασφάλεια εναντίον της επίθεσης «encryption emulation (κρυπτογράφηση μίμησης» που γίνεται στη μετάδοση του αποστολέα. Όμως, στις διάφορες εφαρμογές, όπως το Ίντερνετ και οι On-line συναλλαγές, υποθέτουμε πως οι

αλγόριθμοι και των δύο (αποστολέα και παραλήπτη) είναι γνωστοί στον επιτιθέμενο, με αυτούς του παραλήπτη να είναι πιο ευάλωτοι. Όμως, σε μερικές άλλες εφαρμογές, όπως οι ψηφιακές υπογραφές, οι αλγόριθμοι αποκρυπτογράφησης ή οι αλγόριθμοι για την παραγωγή δημόσιων κλειδιών (από τον παραλήπτη), δεν πρέπει να είναι δημόσιοι, ενώ οι αλγόριθμοι κρυπτογράφησης (από τον αποστολέα) είναι πάντα.

Για τον λόγο αυτό θα παρουσιάσουμε πιο κάτω ένα πρωτόκολλο που είναι ασφαλές απέναντι στην επίθεση «encryption emulation (κρυπτογράφηση μίμησης)» που μπορεί να δεχθεί η μετάδοση του αποστολέα από έναν επιτιθέμενο που έχει απεριόριστη υπολογιστική ισχύ και πλήρη γνώση των αλγορίθμων και του υλικού (hardware) που χρησιμοποιεί ο αποστολέας για την κρυπτογράφηση. Πιο συγκεκριμένα, στο πρωτόκολλό μας, ο αποστολέας θα μεταδώσει την ιδιωτική του ακολουθία από bits, με το να κρυπτογραφεί ένα bit τη φορά κι ο παραλήπτης αποκρυπτογραφεί κάθε bit σωστά με πιθανότητα που μπορεί να προσεγγίσει αυθαίρετα το 1, αλλά ποτέ δε θα είναι ίση με 1. Την ίδια στιγμή, ο επιτιθέμενος αποκρυπτογραφεί σωστά κάθε bit με πιθανότητα το πολύ $\frac{3}{4}$, με το να μιμείται τον αλγόριθμο κρυπτογράφησης του αποστολέα.

Ουσιαστικά δεν υπάρχουν κάποιες απαιτήσεις ως προς την υπολογιστική ικανότητα του αποστολέα. Στην πραγματικότητα, η κρυπτογράφηση μπορεί να γίνει ακόμη και με το χέρι, κάτι που μπορεί να αποτελεί μεγάλο πλεονέκτημα σε κάποιες περιπτώσεις. Για παράδειγμα, κάποιος από το πεδίο λειτουργίας, μπορεί να λάβει ένα δημόσιο κλειδί από ένα κέντρο ελέγχου και να μεταδώσει την κρυπτογραφημένη πληροφορία από το τηλέφωνο, χωρίς καν να χρησιμοποιήσει τον υπολογιστή.

Πρωτόκολλο IV.3

Κρυπτογράφηση:

Τώρα, θα περιγράψουμε περιληπτικά ένα πρωτόκολλο κρυπτογράφησης με τα ακόλουθα χαρακτηριστικά:

1. Ο Bob κρυπτογραφεί το μυστικό του bit με μια λέξη σε ένα δημόσιο αλφάβητο X.

2. Η Alice (παραλήπτης) αποκρυπτογραφεί τη μετάδοση του Bob σωστά με πιθανότητα που μπορεί να προσεγγίσει αυθαίρετα το 1, αλλά δε θα γίνει ποτέ ίση με 1.

3. Ο επιτιθέμενος, υποθέτουμε ότι δεν έχει κάποιον περιορισμό ως προς την υπολογιστική του ισχύ (ταχύτητα) ή τους χώρους αποθήκευσης.

4. Υποθέτουμε ότι ο επιτιθέμενος έχει πλήρη γνώση των αλγορίθμων και του υλικού (hardware) που ο Bob θα χρησιμοποιήσει για την κρυπτογραφία. Παρ' όλα αυτά, ο επιτιθέμενος δε μπορεί να προβλέψει τα αποτελέσματα που παίρνει ο Bob από την παραγωγή τυχαίων αριθμών.

5. Ο επιτιθέμενος δεν έχει κάποια πληροφορία σχετικά με τον αλγόριθμο που χρησιμοποιεί η Alice για να παίρνει τα δημόσια κλειδιά.

6. Ο επιτιθέμενος δε μπορεί να αποκρυπτογραφήσει σωστά το μυστικό bit του Bob με πιθανότητα $> \frac{3}{4}$, σε μια προσπάθεια μίμησης του αλγορίθμου κρυπτογράφησης του Bob.

Σε αυτό το σημείο αξίζει να τονίσουμε ότι το πρωτόκολλο που παρουσιάζουμε πιο πάνω ίσως να μην είναι και το καλύτερο για εμπορικές εφαρμογές, επειδή απαιτείται πολύ δουλειά από την Alice για να λάβει μόνον ένα bit από τον Bob. Από την άλλη, ο Bob, ίσως να μη χρειαστεί καν υπολογιστή για την κρυπτογράφηση.

ΣΥΜΠΕΡΑΣΜΑΤΑ
«ΕΠΙΛΟΓΟΣ»

Ολοκληρώνοντας την παρούσα Διπλωματική Εργασία, αξίζει να αναφέρουμε μερικά συμπεράσματα που μας δημιουργήθηκαν και που ίσως να αποτελέσουν και πεδίο περαιτέρω έρευνας στον μέλλον.

Αναλύσαμε εκτενώς τις ανάγκες των κρυπτογραφικών πρωτοκόλλων και ποιες ομάδες μπορούν να ανταποκριθούν επάξια. Η λίστα από αυτές της ομάδες είναι μεγάλη και ατελείωτη. Όμως, δεν είναι όλες τους στον ίδιο βαθμό δόκιμες για να ανταπεξέρθουν στις προσδοκίες μας. Για τον λόγο αυτόν θα πρέπει να προβούμε σε εκτενέστερη μελέτη των ιδιοτήτων και των συμπεριφορών που επιδεικνύουν, έτσι ώστε να οδηγηθούμε σε καλύτερη κατάταξή τους, δεδομένου του επιπέδου ασφαλείας που μπορούν να μας διασφαλίσουν, χωρίς βεβαίως να αγνοούμε τα αποθέματα υπολογιστικής ισχύος, σε μνήμη και ταχύτητα προσπέλασης, που απαιτούνται και τα οποία θα πρέπει να φροντίσουμε να δαπανήσουμε στο λιγότερο δυνατόν.

Αυτό μας δίνει πάτημα για να κάνουμε αναφορά και στην ανάγκη που υπάρχει για περαιτέρω βελτιστοποίηση των περισσοτέρων μοντέλων, στα πλαίσια της πολυπλοκότητας και της αποδοτικότητας. Είναι περιττό να αναφέρουμε ότι για να είναι κάτι λειτουργικό και υλοποιήσιμο, θα πρέπει να πετύχουμε καλύτερες ταχύτητες προσπέλασης, ορθότερα αποτελέσματα και φυσικά αποταμίευση πόρων.

Επειδή τα Μαθηματικά είναι αρρήτως παντρεμένα και με πολλές άλλες εκφάνσεις του Επιστημονικού εύρους, οι προσπάθειες πρέπει να συνεχίσουν για την εύρεση ασφαλέστερων πρωτοκόλλων, με περαιτέρω έρευνα στη Θεωρία Ομάδων κι όχι μόνον.

Βιβλιογραφικές Αναφορές

[1] I. Anshel, M. Anshel και D. Goldfeld - «An algebraic method for public-key cryptography, Math. Res. Lett. 6 (1999), pp. 287–291».

[2] D. B. A. Epstein, J. W. Cannon, D. F. Holt, S. V. F. Levy, M. S. Paterson, and W. P. Thurston, Word processing in groups. Jones and Bartlett Publishers, 1992.

[3] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. Kang, and C. Park, New public-key cryptosystem using braid groups. Advances in Cryptology – CRYPTO 2000, Lecture Notes in Computer Science 1880, pp. 166–183. Springer, Berlin, 2000.

[4] J. Birman, Braids, Links and Mapping Class Groups, Annals of Math. Studies. Princeton University Press, 1974.

[5] D. B. A. Epstein, J. W. Cannon, D. F. Holt, S. V. F. Levy, M. S. Paterson, and W. P. Thurston, Word processing in groups. Jones and Bartlett Publishers, 1992.

[6] A fast method for comparing braids, Adv. Math. 125 (1997), pp. 200–235.

[7] D. Collins, Relations among the squares of the generators of the braid group, Invent. Math. 117 (1994), pp. 525–529.

[8] A. M. Vershik, S. Nechaev, and R. Bikbov, Statistical properties of braid groups with application to braid groups and growth of heaps, Commun. Math. Phys. 212 (2000), pp. 469–501.

[9] P. Dehornoy, I. Dynnikov, D. Rolfsen, and B. Wiest, Why are braids orderable?. Societe Mathematique De France, 2002.

[10] Shavgulidze, E. (2009), "The Thompson group F is amenable", Inf. Dimen. Anal. Quantum Probab. Relat. Top. 12: 173–191

[11] J. C. Lagarias, The 3x + 1 problem and its generalizations, Amer. Math. Monthly 92 (1985), pp. 3–23.

[12] J.-P. Tillich and G. Z´emor, Hashing with SL2. Advances in Cryptology – CRYPTO 1994, Lecture Notes in Computer Science 839, pp. 40–49. Springer, 1994.

[13] Hashing with polynomials. Information Security and Cryptology – ICISC 2006, Lecture Notes in Computer Science 4296, pp. 22–28. Springer, 2006.

[14] V. Shpilrain and G. Zapata, Using decision problems in public key cryptography, preprint. Available at http://www.sci.ccny.cuny.edu/shpil/res.html.

[15] Using the subgroup membership search problem in public key cryptography. Algebraic Methods in Cryptography, Contemporary Mathematics 418, pp. 169–179. American Mathematical Society, 2006

[16] Combinatorial group theory and public key cryptography, Appl. Algebra Engrg. Comm. Comput. 17 (2006), pp. 291–302.

[17] K. Appel and P. Schupp, Artin groups and infinite Coxeter groups, Invent. Math. 72 (1983), pp. 201–220.

[18] D. Peifer, Artin groups of extra-large type are automatic, J. Pure Appl. Algebra 110 (1996), pp. 15–56.

[19] I. Kapovich, A. G. Miasnikov, P. Schupp, and V. Shpilrain, Generic-case complexity, decision problems in group theory and random walks, J. Algebra 264 (2003), pp. 665–694.

[20] Alexei Myasnikov, Vladimir Shpilrain, Alexander Ushakov - Group-based Cryptography

[21] F. A. Garside – The Braid Group and other Groups, October 2, 1967

[22] David Graber – Tutorials: Braid Group Cryptography, Singapore, June 2007, Department of Applied Mathematics, School of Sciences, Holon Institute of Technology Holon, Israel

[23] John B. Fraleigh – A First Course in Abstract Algebra, 7th Edition

[24] Apostolos Giannopoulos – Θεωρία Ομάδων (Group Theory), 2013

[25] Dimitrios Varsos, Dimitrios Deriziotis, Ioannis Emmanouil, Michail Maliakas, Olympia Talelli – Μια Εισαγωγή στην Άλγεβρα, Δεύτερη Έκδοση

[26] Epameinondas Kechagias – Εισαγωγή στη Θεωρία Ομάδων

[27] Theodora Theochari-Apostolidi – Εισαγωγή στη Θεωρία Ομάδων, 2015

[28] Simon Singh – The Code Book, 2002

[29] Clay Mathematical Institute, http://www.claymath.org/prizeproblems/pvsnp.htm.

[30] C. F. Miller III, Decision problems for groups – survey and reflections. Algorithms and Classification in Combinatorial Group Theory, pp. 1–60. Springer, 1992.

[31] V. Shpilrain and A. Ushakov, Thompson's group and public key cryptography. Applied Cryptography and Network Security – ACNS 2005, Lecture Notes in Computer Science 3531, pp. 151–164. Springer, 2005.

[32] A new key exchange protocol based on the decomposition problem. Algebraic Methods in Cryptography, Contemporary Mathematics 418, pp. 161–167. American Mathematical Society, 2006.

[33] Y. Kurt, A New Key Exchange Primitive Based on the Triple Decomposition Problem, preprint. Available at http://eprint.iacr.org/2006/378.

[34] E. Stickel, A New Method for Exchanging Secret Keys. Proceedings of the Third International Conference on Information Technology and Applications (ICITA05), Contemporary Mathematics 2, pp. 426–430. IEEE Computer Society, 2005.

[35] Cryptanalysis of Stickel's key exchange scheme. Computer Science in Russia 2008, Lecture Notes in Computer Science 5010, pp. 283–288. Springer, 2008.

[36] M. Sramka, On the Security of Stickel's Key Exchange Scheme, preprint.

[37] K. A. Mihailova, The occurrence problem for direct products of groups, Dokl. Akad. Nauk SSSR 119 (1958), pp. 1103–1105.

[38] D. Garber, S. Kaplan, M. Teicher, B. Tsaban, and U. Vishne, Probabilistic solutions of equations in the braid group, Adv. Appl. Math. 35 (2005), pp. 323–334.

[39] J. Hughes and A. Tannenbaum, Length-based attacks for certain group based encryption rewriting systems, preprint. Available at: http://front.math.ucdavis.edu/0306.6032

[40] S. Lal and A. Chaturvedi, Authentication Schemes Using Braid Groups, preprinet. Available at http://arxiv.org/abs/cs/0507066, 2005.

[41] H. Sibert, P. Dehornoy, and M. Girault, Entity authentication schemes using braid word reduction, Discrete Appl. Math. 154 (2006), pp. 420–436.

[42] U. Feige, A. Fiat, and A. Shamir, Zero knowledge proofs of identity, STOC ’87: Proceedings of the nineteenth annual ACM conference on Theory of computing (1987), pp. 210–217.

[43] D. Grigoriev and V. Shpilrain, Zero-knowledge authentication schemes from actions on graphs, groups, or rings, preprint. Available at http://arxiv.org/abs/0802.1661.

[44] M. R. Magyarik and N. R. Wagner, A Public Key Cryptosystem Based on the Word Problem. Advances in Cryptology – CRYPTO 1984, Lecture Notes in Computer Science 196, pp. 19–36. Springer, Berlin, 1985.

[45] G. Baumslag, A. G. Myasnikov, and V. Shpilrain, Open problems in combinatorial group theory. Second Edition. Combinatorial and geometric group theory, Contemporary Mathematics 296, pp. 1–38. American Mathematical Society, 2002.

[46] D. Osin and V. Shpilrain, Public key encryption and encryption emulation attacks. Computer Science in Russia 2008, Lecture Notes in Computer Science 5010, pp. 252–260. Springer, 2008.

[47] Wikipedia (https://www.wikipedia.org)

Αθήνα, 2016