μ Π λ ∀

Μη Μεταθετική Κρυπτογραφία
Διπλωματική Εργασία
Κελεσίδου Μαρία

Εθνικό και Καποδιστριακό
Πανεπιστήμιο Αθηνών

Μεταπτυχιακό Πρόγραμμα Λογικής και Θεωρίας Αλγορίθμων και Υπολογισμού

μΠλ ∀

.

ΜΗ ΜΕΤΑΘΕΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

Κελεσίδου Μαρία
Επιβλέπων: Ράπτης Ευάγγελος

Ιούνιος 2010

.

Στους γονείς μου Όλγα και Γιώργο

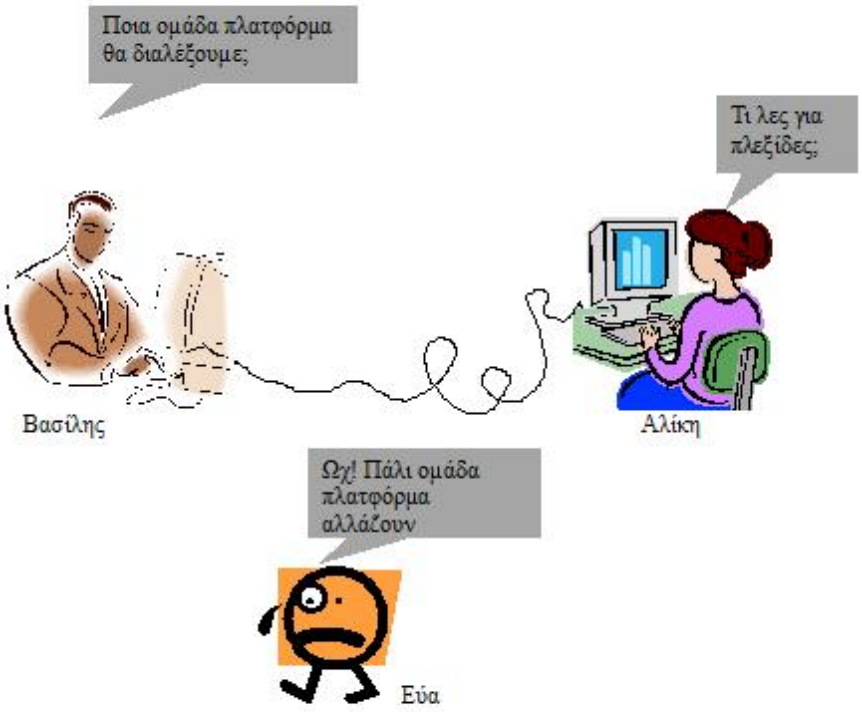
.

Πρόλογος

Η μελέτη που ακολουθεί αποτελεί τη διπλωματική μου εργασία όπως προβλέπει το πρόγραμμα σπουδών του Μ.Π.Λ.Α. Πρόκειται για μια προσπάθεια να παρουσιαστούν όσο το δυνατόν ολοκληρωμένα μη μεταθετικές ομάδες που χρησιμοποιούνται ως πλατφόρμες για πρωτόκολλα στην Κρυπτογραφία. Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου, κύριο Ευάγγελο Ράπτη για τη βοήθεια του και για την πρόταση του να ασχοληθώ με αυτό το ενδιαφέρον θέμα της ' Μη Μεταθετικής Κρυπτογραφίας '.

.

ΜΗ-ΜΕΤΑΘΕΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ



.

Σκοπός της μελέτης μας είναι να χρησιμοποιήσουμε τις μη-μεταθετικές ομάδες ως ομάδες πλατφόρμες στην Κρυπτογραφία του δημοσίου κλειδιού.

Πρώτοι ο *Neal R. Wagner* και η *Marianne R. Magyarik* το 1985 στο άρθρο τους '*A Public Key Cryptosystem Based on the Word Problem*' χρησιμοποίησαν τη πολυπλοκότητα άπειρων, μη-μεταθετικών ομάδων στην Κρυπτογραφία. Το δε πρωτόκολλο δημοσίου-κλειδιού που παρουσίασαν ήταν βασισμένο στη μη επιλυσιμότητα του προβλήματος λέξης για πεπερασμένα αναπαραστάσιμες ομάδες.

Σήμερα, η θεωρία των μη αβελιανών ομάδων στη Κρυπτογραφία τραβάει όλο και περισσότερο τη προσοχή με πρωτόκολλα που τα περισσότερα βασίζονται στα προβλήματα αναζήτησης. Αυτά όμως με τη σειρά τους ταιριάζουν με το γενικό παράδειγμα του πρωτοκόλλου του δημοσίου-κλειδιού το οποίο βασίζεται στη συνάρτηση μιας κατεύθυνσης. Αυτός ο κλάδος της Κρυπτογραφίας που λέγεται ***κανονική κρυπτογραφία*** θα συζητηθεί στο 1ο κεφάλαιο.

Επίσης θα μελετήσουμε ομάδες όπως οι ομάδες πλεξίδες, οι ομάδες πινάκων, οι ομάδες μικρών διαγραφών και άλλες που μπορούν να χρησιμοποιηθούν ως πλατφόρμες κρυπτογραφικών πρωτοκόλλων του κεφαλαίου 1.

Τέλος θα συζητήσουμε πρωτόκολλα βασισμένα σε προβλήματα απόφασης στο δημόσιο κλειδί της Κρυπτογραφίας και κατά πόσο παραμένουν ασφαλή σε διάφορες επιθέσεις του αντιπάλου (Εύα).

Περιεχόμενα

Μέρος Ι

ΕΙΣΑΓΩΓΗ

.

ΕΙΣΑΓΩΓΗ

Εδώ θα παρουσιάσουμε διάφορα πρωταρχικά κρυπτογραφικά πρωτόκολλα που χρησιμοποιούν ως πλατφόρμες μη μεταθετικές (ημι)ομάδες, χωρίς να παρεκλίνουμε από το κανονικό παράδειγμα του πρωτοκόλλου του δημοσίου κλειδιού, το οποίο βασίζεται σε συνάρτηση μιας κατεύθυνσης. Επίσης θα συζητήσουμε το πρωτόκολλο $ANSHEL-ANSHEL-GOLDFELD$, όπως επίσης και τα πρωτόκολλα που είναι κοντά στο πνεύμα των κλασικών πρωτοκόλλων και βασίζονται στις μεταθετικές (ημι)ομάδες.

Μέρος II

ΜΗ-ΜΕΤΑΘΕΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

Κεφάλαιο 1

ΚΑΝΟΝΙΚΗ ΜΗ-ΜΕΤΑΘΕΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

1.1 ΠΡΩΤΟΚΟΛΛΑ ΒΑΣΙΣΜΕΝΑ ΣΤΟ ΠΡΟΒΛΗΜΑ ΑΝΑΖΗΤΗΣΗΣ ΣΥΖΥΓΙΑΣ

.

Έστω G ομάδα με επιλύσιμο *το πρόβλημα λέξης*. Για $w, a \in G$ ο συμβολισμός w^a ισοδυναμεί με $a^{-1}wa$.

▶ **Ορισμός.** **Το Πρόβλημα απόφασης συζυγίας** (*conjugacy decision problem*) για τη G είναι: Δίνονται δύο στοιχεία $u, v \in G$. Βρείτε αν υπάρχει x της G τέτοιο ώστε $u^x = v$.

Απ΄ την άλλη πλευρά,**το πρόβλημα αναζήτησης συζυγίας** (*conjugacy search problem*), που μερικές φορές ονομάζεται και *πρόβλημα μάρτυρα συζυγίας* (*witness conjugacy problem*) είναι: Δίνονται δύο στοιχεία $u, v \in G$ και η πληροφορία ότι $u^x = v$ για κάποιο $x \in G$. Βρείτε ένα τουλάχιστον τέτοιο στοιχείο x.

.

Το *πρόβλημα απόφασης συζυγίας* είναι ένα από τα μεγαλύτερα και πιο ενδιαφέροντα προβλήματα της *θεωρίας ομάδων*. Αντιθέτως *το πρόβλημα αναζήτησης συζυγίας* είναι ενδιαφέρον για τη *θεωρία πολυπλοκότητας*, αλλά όχι για τη *θεωρία ομάδων*. Πράγματι αν ξέρουμε ότι το στοιχείο u είναι συζυγές με το v, μπορούμε να ανατρέξουμε σε

λέξεις της μορφής u^x και να τις συγκρίνουμε κάθε φορά με τη v, έως ότου να βρούμε ποια ταιριάζει. Αυτός ο αλγόριθμος είναι τουλάχιστον εκθετικού χρόνου ως προς το μήκος της v και επομένως θεωρείται ανέφικτος για πρακτικούς λόγους.

Έτσι αφού κανένας άλλος αλγόριθμος δεν είναι γνωστός για *το πρόβλημα αναζήτησης συζυγίας* σε μία ομάδα G, δε θα ήταν αδικαιολόγητο να ισχυριστούμε ότι
η $x \longrightarrow u^x$ είναι *συνάρτηση μιας κατεύθυνσης** και να χτίσουμε πάνω σ΄ αυτήν ένα κρυπτογραφικό πρωτόκολλο (δημοσίου κλειδιού) .

Ξεκινάμε με ένα απλό πρωτόκολλο, **το πρωτόκολλο** *Ko Lee et al* :

Περιγραφή **πρωτοκόλλου**.

1. Ενα στοιχείο $w \in G$ δημοσιεύεται.
2. Η Αλίκη επιλέγει ένα ιδιωτικό $a \in G$ και στέλνει w^a στον Βασίλη.
3.Ο Βασίλης επιλέγει ένα ιδιωτικό $b \in G$ και στέλνει w^b στην Αλίκη.
4. Η Αλίκη υπολογίζει $(w^b)^a = w^{ba}$ και ο Βασίλης $(w^a)^b = w^{ab}$.

Αν τα a, b έχουν επιλεχτεί από την *pool* των αντιμεταθετικών στοιχείων της ομάδας τότε $ab = ba$ και έτσι το κοινό μυστικό κλειδί του Βασίλη και της Αλίκης είναι $w^{ba} = w^{ab}$. Στην ουσία υπάρχουν δύο δημόσιες υποομάδες Α και Β της ομάδας G που προσφέρουν από τα δικά τους σύνολα γεννητόρων έτσι ώστε $ab = ba$ για οποιαδήποτε $a \in G, b \in G$.

Το να διαλέξει κανείς τη κατάλληλη ομάδα-πλατφόρμα για το παραπάνω πρωτόκολλο, είναι εύκολο· όμως υπάρχουν ορισμένες προϋποθέσεις:

(Π_0) Η ομάδα πρέπει να είναι πολύ καλά γνωστή. Το πρόβλημα αναζήτησης συζυγίας στην ομάδα ή θα πρέπει να μπορεί να μελετηθεί καλά ή να μπορεί να αναχθεί σε ένα πολύ καλά γνωστό πρόβλημα .

(Π_1) Το πρόβλημα λέξης στην ομάδα G, πρέπει να έχει μία γρήγορη (γραμμικού ή τετραγωνικού χρόνου) λύση από ένα ντετερμινιστικό αλγόριθμο.

(Π_2) Το πρόβλημα αναζήτησης συζυγίας δε πρέπει να έχει λύση υποεκθετικού χρόνου από ντετερμινιστικό αλγόριθμο.

**συνάρτηση μιας κατεύθυνσης* f : είναι η συνάρτηση, στην οποία είναι εύκολο κάποιος να υπολογίσει τη τιμή της $f(x)$, για κάθε x του πεδίου ορισμού της f, αλλά δύσκολο να υπολογίσει τη τιμή της $f^{-1}(y)$ για τα περισσότερα y του πεδίου τιμών της f.

(Π_3) Να υπάρχει τρόπος να παρουσιαστούν τα στοιχεία της G κατά τέτοιο τρόπο ώστε να είναι αδύνατο ν΄ ανακτηθεί το στοιχείο x απ΄ το στοιχείο $x^{-1}wx$.

Ένας τρόπος για να το πετύχουμε αυτό είναι να έχουμε *κανονική μορφή* για τα στοιχεία της G, το οποίο συνήθως σημαίνει ότι υπάρχει ένας αλγόριθμος που μετασχηματίζει οποιαδήποτε είσοδο u_{in}, η οποία είναι μία λέξη από τους γεννήτορες της G, σε μία έξοδο u_{out}, η οποία είναι μια άλλη λέξη από τους γεννήτορες της G, έτσι που $u_{in} = u_{out}$ της ομάδας G, χωρίς όμως αυτό να είναι εύκολο να ανιχνευθεί από μια επιθεώρηση.

Ελλείψει της κανονικής μορφής, δηλ. για παράδειγμα αν πούμε ότι η G δίνεται με γεννήτορες και σχέσεις χωρίς οποιεσδήποτε πρόσθετες πληροφορίες για τις ιδιότητες της G, τότε τουλάχιστον μερικές από αυτές τις σχέσεις πρέπει να είναι πολύ σύντομες.

(Π_4) Η ομάδα G θα πρέπει να είναι ομάδα *super*-πολυωνυμικής (δηλ. εκθετικής ή «ενδιάμεσης») αύξησης. Αυτό σημαίνει ότι ο αριθμός στοιχείων μήκους n της G, θα αυξηθεί γρηγορότερα απο οποιοδήποτε πολυώνυμο του n. Αυτό απαιτείται για να αποτρέψει τις επιθέσεις οι οποίες χρησιμοποιούνται για την πλήρη εξάντληση του χώρου των κλειδιών. Εδώ «το μήκος n» είναι ακριβώς το μήκος μιας λέξης που αναπαρίσταται ως στοιχείο μιας ομάδας.

Υπάρχουν ομάδες που έχουν τις (Π_1), (Π_4), πιθανότατα την (Π_2) και σε μια λογική έκταση την (Π_3). Αυτές οι ομάδες έχουν επιλύσιμο το πρόβλημα λέξης, αλλά μη επιλύσιμο το πρόβλημα συζυγίας.

1.2 ΠΡΩΤΟΚΟΛΛΑ ΒΑΣΙΣΜΕΝΑ ΣΤΟ ΠΡΟΒΛΗΜΑ ΑΠΟΣΥΝΘΕΣΗΣ

.

Μία από τις φυσικές διακλαδώσεις του προβλήματος αναζήτησης συζυγίας είναι το παρακάτω πρόβλημα αναζήτησης αποσύνθεσης.

►**Ορισμός.** **Πρόβλημα αναζήτησης αποσύνθεσης** (*decomposition search problem*): Δίνονται δύο στοιχεία w και $w^{'}$ μιας ομάδας G. Βρείτε δυο στοιχεία x, y που ανήκουν σε ένα δεδομένο σύνολο $A \subseteq G$ και ικανοποιούν τη σχέση $x \cdot w \cdot y = w^{'}$ υπό τον όρο ότι υπάρχει τουλάχιστον ένα τέτοιο ζευγάρι .

Αν το σύνολο A είναι υποομάδα τότε το πρόβλημα αυτό είναι γνωστό και ως **πρόβλημα διπλού σύμπλοκου** (*double coset problem*).

.

Παρατηρούμε ότι :
α) πάντα υπάρχουν κάποια x, y τέτοια που $x \cdot w \cdot y = w^{'}$ (π.χ. $x = 1, y = w^{-1}w^{'}$). Οπότε το μόνο που έχουμε να δείξουμε είναι ότι $x, y \in A$.
β) Η συνθήκη $x, y \in A$ ίσως δεν είναι εύκολο να ελεχτεί για μερικά υποσύνολα Α. Το αντίστοιχο πρόβλημα είναι γνωστό ως *membership decision problem*.
γ) το πρόβλημα αναζήτησης συζυγίας είναι ειδική περίπτωση του προβλήματος αποσύνθεσης όπου $w^{'}$ είναι συζυγές με το w και $x = y^{-1}$. .

Τώρα θα δώσουμε μία τυπική περιγραφή ενός χαρακτηριστικού πρωτοκόλλου που βασίζεται στο πρόβλημα αποσύνθεσης.

Περιγραφή **πρωτοκόλλου**.

Έχουμε μία δημόσια ομάδα G και δύο δημόσιες υποομάδες $A, B \subseteq G$ με την ιδιότητα $ab = ba, \forall a \in A$ και $\forall b \in B$.

1. Η Αλίκη επιλέγει τυχαία και ιδιωτικά δύο στοιχεία $a_1, a_2 \in A$. Μετά στέλνει στον Βασίλη $a_1 w a_2$.

2. Ο Βασίλης επιλέγει τυχαία και ιδιωτικά δύο στοιχεία $b_1, b_2 \in B$. Μετά στέλνει στην Αλίκη $b_1 w b_2$.

3. Η Αλίκη υπολογίζει $K_A = a_1 b_1 w b_2 a_2$. Ο Βασίλης υπολογίζει $K_B = b_2 a_1 w b_1 a_2$.

Όμως $a_i b_i = b_i a_i$ οπότε $K = K_A = K_B$ (ως ένα στοιχείο της G) το κοινό κλειδί της Αλίκης και του Βασίλη.

Ας δούμε μερικές τροποποιήσεις του ανωτέρω πρωτοκόλλου.

1.2.1 Συνεστραμμενο πρωτοκολλο (*"Twisted" protocol*) [*Shpilrain* και *Ushakov*]

.

Μία τροποποίηση του παραπάνω πρωτοκόλλου δίνει περισσότερη ασφάλεια ενάντια, στις λεγόμενες με βάση το μήκος επιθέσεις, σύμφωνα με πειράματα υπολογιστών.

Περιγραφή **πρωτοκόλλου**.

Πάλι έχουμε τη δημόσια ομάδα G και δύο δημόσιες υποομάδες $A, B \leq G$ με την ιδιότητα της μετάθεσης.

1. Η Αλίκη επιλέγει τυχαία και ιδιωτικά δύο στοιχεία $a_1 \in A,\ b_1 \in B$. Μετά στέλνει στον Βασίλη $a_1 w b_1$.

2. Ο Βασίλης επιλέγει τυχαία και ιδιωτικά δύο στοιχεία $a_2 \in A,\ b_2 \in B$. Μετά στέλνει στην Αλίκη $a_2 w b_2$.

3. Η Αλίκη υπολογίζει $K_A = a_1 b_2 w a_2 b_1 = b_2 a_1 w b_1 a_2$.

Ο Βασίλης υπολογίζει $K_B = b_2 a_1 w b_1 a_2$.

Αφού $a_ib_i = b_ia_i$ στο G έχουμε $K_A = K_B = K$ το οποίο τώρα είναι το κοινό μυστικό κλειδί της Αλίκης και του Βασίλη.

1.2.2 ΚΡΥΒΟΝΤΑΣ ΜΙΑ ΑΠ ΤΙΣ ΥΠΟΜΑΔΕΣ [*Shpilrain και Ushakov*]

.

►**Ορισμός.** Έστω G μία ομάδα και $g \in G$. Συμβολίζουμε με $C_G(g)$ τον **κεντροποιητή** (*centralizer*) **του** g **στην** G. Δηλαδή το σύνολο των στοιχείων h της G τέτοια που $hg = gh$. Για $S = \{g_1, ..., g_k\}$ και $S \subseteq G$ το $C_G(g_1, ..., g_k)$ συμβολίζει τον κεντροποιητή του S στην G που είναι η τομή των κεντροποιητών $C_G(g_i), i = 1, ..., k$.

Τώρα, λαμβάνοντας υπόψη ένα δημόσιο $w \in G$ η Αλίκη επιλέγει ιδιωτικά $a_1 \in G$ και δημοσιεύει μια υποομάδα $B \subseteq C_G(a_1)$. Ομοίως, ο Βασίλης επιλέγει ιδιωτικά $b_2 \in G$ και δημοσιεύει μια υποομάδα $A \subseteq C_G(b_2)$. Η Αλίκη τότε επιλέγει $a_2 \in A$ και στέλνει $w_1 = a_1wa_2$ στον Βασίλη, ενώ ο Βασίλης επιλέγει $b_1 \in B$ και στέλνει $w_2 = b_1wb_2$ στην Αλίκη.

Περιγραφή **πρωτοκόλλου**
Έστω G μια δημόσια ομάδα και w επίσης δημόσιο στοιχείο της G.

1. Η Αλίκη διαλέγει ένα στοιχείο $a_1 \in G$ και επιλέγει μια υποομάδα $C_G(a_1)$ και δημοσιεύει τους γεννήτορες της $A = \{\alpha_1, ..., \alpha_k\}$.
2. Ο Βασίλης διαλέγει ένα στοιχείο $b_2 \in G$ και επιλέγει μια υποομάδα $C_G(b_2)$ και δημοσιεύει τους γεννήτορες της $B = \{\beta_1, ..., \beta_m\}$.
3. Η Αλίκη επιλέγει τυχαία ένα στοιχείο a_2 από $\langle \beta_1, ..., \beta_m \rangle$ και στέλνει a_1wa_2 στον Βασίλη.
4. Η Βασίλης επιλέγει τυχαία ένα στοιχείο b_1 από $\langle \alpha_1, ..., \alpha_k \rangle$ και στέλνει b_1wb_2 στην Αλίκη.
5. Η Αλίκη υπολογίζει $K_A = a_1b_1wb_2a_2$
6. Ο Βασίλης υπολογίζει $K_B = b_1a_1wa_2b_2$

Εφόσον $a_1b_1 = b_1a_1$ και $a_2b_2 = b_2a_2$ έχουμε $K = K_A = K_B$ που είναι το κοινό μυστικό κλειδί.

1.2.3 Χρησιμοποιωντας το τριπλο προβλημα αποσυνθεσης (*triple decomposition problem*) [*Kurt*]

.

►**Ορισμός.** **Τριπλό πρόβλημα αποσύνθεσης**: γνωστό στοιχείο ως γινόμενο τριών αγνώστων παραγόντων.

.
Στο πρωτόκολλο της $Kurt$ το ιδιωτικό κλειδί έχει τρεις παράγοντες. Η ιδέα είναι να κρύψει κάθε ένα από αυτούς τους παράγοντες πολλαπλασιάζοντας τους με τυχαία στοιχεία μιας (δημόσιας) υποομάδας. Το σημαντικό μέρος είναι ότι ένας από τους παράγοντες πολλαπλασιάζεται με τυχαία στοιχεία και και από δεξιά και από αριστερά. Τώρα φτάνουμε στην περιγραφή πρωτοκόλλου.

Περιγραφή **πρωτοκόλλου**.

Υπάρχει μια δημόσια ομάδα πλατφόρμα, η G και δύο υποσύνολα της G που περιέχουν πέντε υποσύνολα της G το καθένα. Έστω το $A = \{A_1, A_2, A_3, X_1, X_2\}$ και $B = \{B_1, B_2, B_3, Y_1, Y_2\}$ ενώ ικανοποιούν τις εξής συνθήκες:
α) Σχέσεις αντιστροφής: Τα στοιχεία των X_1, X_2, Y_1, Y_2 είναι αντιστρέψιμα.
β) Σχέσεις μετάθεσης: $[A_2, Y_1] = 1, [A_3, Y_2] = 1, [B_1, X_1] = 1, [B_2, X_2] = 1$.

Η Αλίκη και ο Βασίλης συμφωνούν ποιο σύνολο θα χρησιμοποιήσουν. Ας πούμε η Αλίκη το Α και ο Βασίλης το Β. Τότε:

1. Η Αλίκη επιλέγει: $a_1 \in A_1,\ a_2 \in A_2,\ a_3 \in A_3,\ x_1 \in X_1,\ x_2 \in X_2$ και υπολογίζει: $u = a_1 x_1,\ v = x_1^{-1} a_2 x_2,\ w = x_2^{-1} a_3$. Το ιδιωτικό της κλειδί είναι: (a_1, a_2, a_3).

2. Ο Βασίλης επιλέγει $b_1 \in B_1,\ b_2 \in B_2,\ b_3 \in B_3,\ y_1 \in Y_1,\ y_2 \in Y_2$ και υπολογίζει: $p = b_1 y_1,\ q = y_1^{-1} b_2 y_2,\ r = y_2^{-1} b_3$. Το ιδιωτικό του κλειδί είναι: (b_1, b_2, b_3).

3. Η Αλίκη στέλνει (u, v, w) στο Βασίλη.

4. Ο Βασίλης στέλνει (p, q, r) στην Αλίκη.

5. Η Αλίκη υπολογίζει:

$$a_1 p a_2 q a_3 r = a_1(b_1 y_1) a_2 (y_1^{-1} b_2 y_2) a_3 (y_2^{-1} b_3) = a_1 b_1 a_2 b_2 a_3 b_3 = K_A$$

6. Ο Βασίλης υπολογίζει:

$$u b_1 v b_2 w b_3 = (a_1 x_1) b_1 (x_1^{-1} a_2 x_2) b_2 (y_2^{-1} b_3) b_3 = a_1 b_1 a_2 b_2 a_3 b_3 = K_B$$

Έτσι $K_A = K_B = K$ το κοινό μυστικό κλειδί του Βασίλη και της Αλίκης.

.

1.3 ΠΡΩΤΟΚΟΛΛΟ ΒΑΣΙΣΜΕΝΟ ΣΤΟ ΠΡΟΒΛΗΜΑ ΑΝΑΖΗΤΗΣΗΣ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗΣ

.

►**Ορισμός.** **Πρόβλημα αναζήτησης παραγοντοποίησης** (*factorization search problem*): Δίνεται ένα στοιχείο w μίας ομάδας G και δύο υποομάδες $A, B \leq G$. Ζητάμε να βρούμε δύο στοιχεία $a \in A$ και $b \in B$ τέτοια που $ab = w$.

Περιγραφή **πρωτοκόλλου**.

Έχουμε μια δημόσια ομάδα G και δύο δημόσιες υποομάδες $A, B \leq G$ με την ιδιότητα αντιμετάθεσης δηλ. $ab = ba$ για κάθε $a \in A$ και $b \in B$.

1. Η Αλίκη επιλέγει τυχαία, ιδιωτικά τα στοιχεία $a_1 \in A, b_1 \in B$. Μετά στέλνει a_1b_1 στον Βασίλη.

2. Ο Βασίλης επιλέγει τυχαία, ιδιωτικά τα στοιχεία $a_2 \in A, b_2 \in B$. Μετά στέλνει a_2b_2 στην Αλίκη.

3. Η Αλίκη υπολογίζει:

$$K_A = b_1(a_2b_2)a_1 = a_2b_1a_1b_2 = a_2a_1b_1b_2$$

και ο Βασίλης υπολογίζει:

$$K_B = a_2(a_1b_1)b_2 = a_2a_1b_1b_2.$$

Έτσι $K_A = K_B = K$ είναι το κοινό μυστικό κλειδί του Βασίλη και της Αλίκης.

Παρατηρούμε ότι αν η αντίπαλος (Εύα) ξέρει τα στοιχεία a_1b_1 και a_2b_2, θα μπορεί να υπολογίσει

$$(a_1b_1)(a_2b_2) = a_1b_1a_2b_2 = a_1a_2b_1b_2$$

και

$$(a_2b_2)(a_1b_1) = a_2b_2a_1b_1 = a_2a_1b_2b_1$$

αλλά κανένα από αυτά δεν είναι το K αφού $a_1a_2 \neq a_2a_1$ και $b_1b_2 \neq b_2b_1$.

.

1.4 ΠΡΩΤΟΚΟΛΛΟ ΑΝΤΑΛΛΑΓΗΣ *STICKEL*

.

Η επιλογή της ομάδας πλατφόρμας του $Stickel$ είναι η ομάδα των αντιστρέψιμων πινάκων επί πεπερασμένου σώματος, που όμως όπως θα δούμε είναι τρωτή, στις επιθέσεις της γραμμικής άλγεβρας. Επίσης θα δούμε ότι αυτό βελτιώνεται αν χρησιμοποιηθούν μη αντιστρέψιμοι πίνακες.

Περιγραφή **πρωτοκόλλου**

Εστω G μία δημόσια μη αβελιανή πεπερασμένη ομάδα, με $a, b \in G$ δημόσια στοιχεία τέτοια που $ab \neq ba$ και N, M οι τάξεις των a, b αντίστοιχα.

1. Η Αλίκη επιλέγει τυχαία δύο φυσικούς αριθμούς $n < N, m < M$ και στέλνει $u = a^n b^m$ στον Βασίλη.

2. Ο Βασίλης επιλέγει τυχαία δύο φυσικούς αριθμούς $r < N, s < M$ και στέλνει $v = a^r b^s$ στην Αλίκη.

3. Η Αλίκη υπολογίζει:

$K_A = a^n v b^m = a^{n+r} b^{m+s}$.

4. Ο Βασίλης υπολογίζει:

$K_B = a^r u b^s = a^{n+r} b^{m+s}$.

Έτσι, η Αλίκη και ο Βασίλης καταλήγουν στο ίδιο στοιχείο της ομάδας: $K = K_A = K_B$ που είναι και το κοινό μυστικό κλειδί τους.

Μία γενίκευση του παραπάνω πρωτοκόλλου ($Stickel$) είναι η εξής:

Έστω $w \in G$ δημόσιο στοιχείο.

1. Η Αλίκη επιλέγει τυχαία δύο φυσικούς αριθμούς $n < N, m < M$, ένα στοιχείο c_1 από το κέντρο της ομάδας G και στέλνει $u = c_1 a^n w b^m$ στον Βασίλη.

2. Ο Βασίλης επιλέγει τυχαία δύο φυσικούς αριθμούς $r < N, s < M$, ένα στοιχείο c_2 από το κέντρο της ομάδας G και στέλνει $v = c_2 a^r w b^s$ στην Αλίκη.

3. Η Αλίκη υπολογίζει:

$K_A = c_1 a^n v b^m = c_1 c_2 a^{n+r} w b^{m+s}$.

4. Ο Βασίλης υπολογίζει:

$K_B = c_2 a^r u b^s = c_1 c_2 a^{n+r} w b^{m+s}$.

Έτσι, η Αλίκη και ο Βασίλης καταλήγουν στο ίδιο στοιχείο της ομάδας:
$K = K_A = K_B$ που είναι και το κοινό μυστικό κλειδί τους.

Παρατηρούμε ότι για να δουλέψει αυτό το πρωτόκολλο η G δε χρειάζεται να είναι ομάδα. Και ως ημιομάδα δουλεύει το ίδιο καλά.

Ας θυμηθούμε τώρα τη μετάδοση της Αλίκης $u = c_1 a^n w b^m$ στον Βασίλη.

Ας υποθέσουμε ότι η αντίπαλος (Εύα) έχει τη μετάδοση του Βασίλη: $v = c_2 a^r w b^s$. Επίσης υποθέτουμε ότι της είναι εφικτό να βρει δύο στοιχεία $x, y \in G$ τέτοια που $xa = ax,\ yb = by,\ u = xwy$. Τότε η Εύα μπορεί να βρει το κοινό κλειδί της Αλίκης και του Βασίλη με τον εξής υπολογισμό:

$$xvy = xc_2 a^r w b^s y = c_2 a^r x w y b^s = c_2 a^r u b^s = K.$$

Παρατηρούμε ότι πολλαπλασιάζοντας με το c_i δεν ενισχύεται η ασφάλεια του πρωτοκόλλου. Επίσης δεν είναι απαραίτητο για την Εύα να βρει κάποιο από τα στοιχεία n, m, r, s. Αντιθέτως πρέπει να λύσει το σύστημα εξισώσεων $xa = ax,\ yb = by,\ u = xwy$, όπου a, b, u, w είναι γνωστά και x, y άγνωστα στοιχεία της βάσης (ημι)ομάδας G.

Στην ουσία το να λυθεί το παραπάνω σύστημα εξισώσεων στην G δεν είναι τίποτα άλλο από το:

►**Ορισμός.** **Πρόβλημα αναζήτησης αποσύνθεσης** (περιορισμένο στις υποημιομάδες): *Δοθέντος μιας αναδρομικής (ημι)ομάδας G, δύο αναδρομικών υπο(ημι)ομάδων $A, B < G$ και δύο στοιχείων $u, w \in G$, βρείτε δύο στοιχεία $x \in A$ και $y \in B$ που ικανοποιούν τη σχέση $xwy = u$ δίνοντας τουλάχιστον ένα τέτοιο ζευγάρι.*

Αναφερόμενοι στο σχήμα του *Stickel* οι υπο(ημι)ομάδες A, B είναι κεντροποιητές των στοιχείων a, b αντίστοιχα.

►**Ορισμός.** Ας θυμηθούμε **κεντροποιητής ενός στοιχείου** $g \in G$ *είναι το σύνολο όλων των στοιχείων $c \in G$ τέτοια που $cg = gc$.* Το σύνολο αυτό είναι μια υποημιομάδα της G. Γνωρίζουμε ότι αν G ομάδα, τότε το σύνολο αυτό είναι υπο-ομάδα.

.

1.4.1 Η ΕΠΙΘΕΣΗ ΤΗΣ ΓΡΑΜΜΙΚΗΣ ΑΛΓΕΒΡΑΣ ΣΤΟ ΠΡΩΤΟΚΟΛΛΟ ΤΟΥ *STICKEL*

.

Στο πρωτόκολλο *Stickel*, η G είναι η ομάδα των αντιστρέψιμων $k \times k$ πινάκων επί ενός πεπερασμένου σώματος F_{2^l} όπου $k = 31$ και $2 < l < k$. Η επιλογή των πινάκων a, b, w δεν είναι τόσο σπουδαία για τη επίθεση μας. Το σημαντικό είναι ότι a και b είναι αντιστρέψιμοι. Εδώ σημειώνουμε ότι η επιλογή των πινάκων a και b και πιο συγκεκριμμένα το γεγονός ότι οι είσοδοι αυτών των πινάκων είναι μηδέν ή ένα προσδίδει μια ακόμα αδυναμία στο σχήμα όπως θα δούμε παρακάτω.

Ας θυμηθούμε ότι η Εύα μπορεί να βρει τουλάχιστον μία λύση του συστήματος των εξισώσεων $xa = ax,\ yb = by,\ u = xwy$, όπου a, b, u, w είναι γνωστοί και x, y άγνωστοι $k \times k$ πίνακες πάνω στο σώμα F_{2^l}. Κάθε μία από τις δύο πρώτες εξισώσεις του συστήματος μεταφράζεται σε k^2 γραμμικές εξισώσεις για τις άγνωστες εισόδους των πινάκων x και y. Όμως η εξίσωση $u = xwy$ δε μεταφράζεται σ΄ ένα σύστημα γραμμικών εξισώσεων για τις εισόδους, γιατί περιέχει το γινόμενο δύο αγνώστων πινάκων. Ακολουθούμε την παρακάτω τεχνική:

Πολλαπλασιάζουμε και τα δύο μέρη της εξίσωσης $u = xwy$ με x^{-1} από τα αριστερά (εδώ χρησιμοποιούμε ότι το x είναι αντιστρέψιμο). Οπότε παίρνουμε:

$$x^{-1}u = wy.$$

Τώρα, αφού $xa = ax$ αν και μόνο αν $x^{-1}a = ax^{-1}$ συμβολίζουμε $x_1 = x^{-1}$. Οπότε:

$$x_1u = wy,\ x_1a = ax_1,\ yb = by.$$

Κάθε εξίσωση σ΄ αυτό το σύστημα μπορεί να δώσει k^2 γραμμικές εξισώσεις για τις άγνωστες εισόδους των πινάκων x_1 και y. Δηλαδή συνολικά έχουμε $3n^2$ γραμμικές εξισώσεις με $2k^2$ αγνώστους. Η λύση όμως που παράγει το σύστημα θα είναι το κοινό κλειδί K αν και μόνο αν το x_1 είναι αντιστρέψιμο αφού $K = xvy$, όπου $x = x_1^{-1}$.

Εφόσον ο u είναι γνωστός αντιστρέψιμος πίνακας μπορούμε να πολλαπλασιάσουμε και τα δύο μέρη της εξίσωσης $x_1u = wy$ με το u^{-1} από τα δεξιά και να πάρουμε $x_1 = wyu^{-1}$ και μετά να διώξουμε το x_1 από το σύστημα:

$$wyu^{-1}a = awyu^{-1},\ yb = by.$$

Τώρα έχουμε $2k^2$ γραμμικές εξισώσεις για k^2 εισόδους του y. Αυτό το υπερκαθορισμένο σύστημα γραμμικών εξισώσεων έχει τουλάχιστον μία μη τετριμμένη λύση.

Έτσι αν ανάγουμε το πίνακα του συστήματος σε *ανηγμένη κλιμακωτή μορφή* (*echelon*)* θα υπάρχει τουλάχιστον μία ελεύθερη μεταβλητή. Από την άλλη μεριά επειδή ακριβώς το σύστημα είναι υπερκαθορισμένο μπορούμε να αναμένουμε ότι ο αριθμός των ελεύθερων μεταβλητών δε θα είναι τόσο μεγάλος, ώστε να μας είναι εφικτό να ελέγχουμε τις τιμές των ελεύθερων μεταβλητών κάθε φορά, μέχρι να βρούμε κάποιες μεταβλητές που θα παράγουν τον αντιστρέψιμο πίνακα y.

Ας μη ξεχνάμε ότι οι είσοδοι του y είναι 0 ή 1 (αδυναμία που αναφέραμε πιο πριν). Σημειώνουμε ότι το να ελέγξουμε την αντιστρεψιμότητα δοθέντος πίνακα είναι εύκολο διότι είναι ισοδύναμο με το να ανάγουμε το πίνακα σε ανοιγμένη κλιμακωτή μορφή. Στη πραγματικότητα σε όλους τους πειραματισμούς μας υπήρχε ακριβώς μία ελεύθερη μεταβλητή, οπότε το τελευταίο βήμα (έλεγχος της αντιστρεψιμότητας) δε χρειάζεται εφόσον αν υπάρχει μία μοναδική μη μηδενική λύση του παραπάνω συστήματος τότε αυτή, δηλ.ο πίνακας y θα είναι αντιστρέψιμος.

Επομένως η πιο προφανής πρόταση για τη βελτίωση του σχήματος *Stickel* είναι να χρησιμοποιήσουμε μη αντιστρέψιμα στοιχεία a, b, w και ειδικότερα η ομάδα πλατφόρμα να είναι ημιομάδα με αρκετά μη αντιστρέψιμα στοιχεία. Κι αν κάποιος χρησιμοποιήσει πίνακες μπορεί να χρησιμοποιήσει την ημιομάδα με όλους τους $k \times k$ πίνακες επί ενός πεπερασμένου δακτυλίου (όχι απαραίτητα σώμα). Μια τέτοια ημιομάδα τυπικά έχει πολλά μη αντιστρέψιμα στοιχεία κι επομένως θα μας είναι εύκολο να διαλέξουμε a, b, w μη αντιστρέψιμα έτσι ώστε η επίθεση της γραμμικής άλγεβρας να μη δουλεύει.

Ένα ακόμα πλεονέκτημα στο να μη περιοριζόμαστε στην *pool* των αντιστρέψιμων πινάκων είναι ότι κάποιος μπορεί να χρησιμοποιήσει όχι μόνο δυνάμεις a^j του δοδομένου δημοσίου πίνακα στο πρωτόκολλο *Stickel*, αλλά αυθαίρετες εκφράσεις της μορφής: $\sum_{i=1}^{p} c_i a^i$ όπου c_i είναι σταθερές.

Βέβαια δεν υπάρχει επιτακτικός λόγος να χρησιμοποιήσουμε πίνακες στο σχήμα *Stickel*, αλλά όπως εξηγήσαμε παραπάνω με μία αφηρημένη (ημι)ομάδα πλατφόρμα G, το σχήμα *Stickel* σπάει αν λυθεί το σχετικό πρόβλημα αναζήτησης αποσύνθεσης

.

*ανηγμένη κλιμακωτή μορφή (echelon) ενός πίνακα είναι ένας πίνακας με τις εξής ιδιότητες:
1) όλες οι μη μηδενικές γραμμές (γραμμές με τουλάχιστον ένα μη μηδενικό στοιχείο) είναι πάνω από οποιαδήποτε σειρά με όλα τα στοιχεία της μηδέν
2) Το ηγηθέν στοιχείο (το πρώτο μη μηδενικό στοιχείο από τα αριστερά) είναι πάντα δεξιά του ηγηθέντος στοιχείου της πάνω γραμμής
3) το ηγηθέν στοιχείο κάθε μη μηδενικής σειράς είναι ένα.

και μέχρι τώρα καμμία αφηρημένη (ημι)ομάδα πλατφόρμα δεν έχει αναγνωριστεί ώστε να μπορεί ν΄ αντισταθεί στις γνωστές επιθέσεις για το πρόβλημα αναζήτησης αποσύνθεσης.

1.5 ΤΟ ΠΡΩΤΟΚΟΛΛΟ $ANSHEL-ANSHEL-GOLDFELD$

.

Εδώ θα περιγράψουμε ένα βασικό πρωτόκολλο που ξεχωρίζει πραγματικά διότι, σε αντίθεση με τα άλλα πρωτόκολλα αυτού του κεφαλαίου, δεν χρησιμοποιεί την μεταθετικότητα ούτε μεταθετικές ημιομάδες της ομάδας πλατφόρμας που μας δίνεται. Μπορεί να χρησιμοποιήσει οποιαδήποτε μη αβελιανή ομάδα με επιλύσιμο το πρόβλημα της λέξης όπως η πλατφόρμα. Αυτό πραγματικά κάνει τη διαφορά και δίνει ένα μεγάλο πλεονέκτημα στο πρωτόκολλο [1] έναντι των άλλων πρωτοκόλλων του κεφαλαίου. .

Περιγραφή **πρωτοκόλλου**

Μία ομάδα G και τα στοιχεία $a_1, ..., a_k, b_1, ..., b_m \in G$ είναι δημόσια.

(1). Η Αλίκη επιλέγει ένα ιδιωτικό $x \in G$ ως λέξη από τα $a_1, ..., a_k$ π.χ $x = x(a_1, ..., a_k)$ και στέλνει $b_1^x, ..., b_m^x$ στο Βασίλη.

(2). Ο Βασίλης επιλέγει ένα ιδιωτικό $y \in G$ ως λέξη από τα $b_1, ..., b_m$ π.χ $y = y(b_1, ..., b_m)$ και στέλνει $a_1^y, ..., a_k^y$ στην Αλίκη.

(3). Η Αλίκη υπολογίζει:

$$x(a_1^y, ..., a_k^y) = x^y = y^{-1}xy$$

και ο Βασίλης:

$$y(b_1^x, ..., b_m^x) = y^x = x^{-1}yx.$$

Τότε η Αλίκη και ο Βασίλης καταλήγουν στο κοινό ιδιωτικό κλειδί

$$K = x^{-1}y^{-1}xy$$

(που ονομάζεται *αντιμεταθέτης* των x και y) ως εξής: η Αλίκη πολλαπλασιάζει το $y^{-1}xy$ με x^{-1} από τ΄ αριστερά, ενώ ο Βασίλης πολλαπλασιάζει το $x^{-1}yx$ με y^{-1} από τ΄ αριστερά και μετά παίρνει το αντίστροφο της παράστασης $(y^{-1}x^{-1}yx)^{-1} = x^{-1}y^{-1}xy$.

Ίσως φαίνεται ότι λύνοντας το πρόβλημα αναζήτησης συζυγίας για τα $b_1^x, ..., b_m^x$, $a_1^y, ..., a_k^y$, της ομάδας G θα επέτρεπε στον αντίπαλο να βρει το μυστικό κλειδί K.

Όμως κοιτώντας πιο προσεκτικά το βήμα 3 του πρωτοκόλλου θα δούμε ότι ο αντίπαλος θα έπρεπε να ξέρει είτε το x είτε το y όχι απλά σα μια λέξη των γεννητόρων της ομάδας G, αλλά σα μια λέξη από τα $a_1, ..., a_k$ (ή σα μια λέξη από τα $b_1, ..., b_m$ αντίστοιχα). Διαφορετικά θα μπορούσε να συγκρίνει, ας πούμε το x^y από τα $a_1^y, ..., a_k^y$. Αυτό σημαίνει ότι ο αντίπαλος θα έπρεπε επίσης να λύσει το *membership search* πρόβλημα.

►**Ορισμός.** *Membership search* **πρόβλημα**: Δίνονται τα στοιχεία $x, a_1, ..., a_k$ της ομάδας G. Βρείτε μια έκφραση του x (αν υπάρχει) σα μια λέξη, από τα $a_1, ..., a_k$.

►**Ορισμός.** *Membership decision* **πρόβλημα**: Καθορίστε αν το δοθέν στοιχείο $x \in G$ ανήκει ή όχι στην υποομάδα της G η οποία έχει γεννήτορες τα δοθέντα $a_1, ..., a_k$.

► Επίσης βλέπουμε ότι αν ο αντίπαλος βρεί, έστω κάποιο $x^{'} \in G$ τέτοιο που $b_1^x = b_1^{x^{'}}, ..., b_m^x = b_m^{x^{'}}$ αυτό δε σημαίνει ότι $x^{'} = x$ στην G.
Πράγματι αν $x^{'} = c_b x$ όπου $c_b b_i = b_i c_b$ για όλα τα i (δηλ. το c_b κεντροποιεί το b_i), τότε $b_i^x = b_i^{x^{'}}$ για όλα τα i και έτσι $b^x = b^{x^{'}}$ για κάθε στοιχείο b από την υποομάδα με γεννήτορες $b_1, ..., b_m$. Ειδικότερα $y^x = y^{x^{'}}$. Τώρα το πρόβλημα είναι ότι αν το x' (παρόμοια και για το y') δεν ανήκει στην υποομάδα A με γεννήτορες $a_1, ..., a_k$ (αντίστοιχα στην υποομάδα B με γεννήτορες $b_1, ..., b_m$) τότε ο αντίπαλος δε μπορεί να βρει το μυστικό κλειδί K.

► Απ΄ την άλλη μεριά , αν το $x^{'}$ (και ομοίως, το $y^{'}$) δεν ανήκει στην υποομάδα A (αντιστοίχως, στην υποομάδα B) τότε ο αντίπαλος θα είναι σε θέση να πάρει το σωστό K ακόμα κι αν το $x^{'}$ του και το $y^{'}$ του είναι διαφορετικά από το x και y, αντίστοιχα.
Πράγματι, εάν $x^{'} = c_b x$, $y^{'} = c_a y$, όπου το c_b κεντροποιεί το B και το c_a κεντροποιεί το A, τότε:

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

αφού το c_b αντιμετατίθεται με το y και με το c_a και το c_a αντιμετατίθεται με το x.

Τονίζουμε ότι ο αντίπαλος καταλήγει στο σωστό κλειδί K (δηλ.

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

αν και μόνο αν το c_b αντιμετατίθεται με το c_a. Ο μόνος ορατός τρόπος για να εξασφαλιστεί αυτό είναι το $x^{'} \in A$ και το $y^{'} \in B$. Αν δεν επαληθευτεί τουλάχιστον ένας από αυτούς τους συνυπολογισμούς δεν φαίνεται να υπάρχει κανένας τρόπος για τον αντίπαλο για να σιγουρευτεί ότι πήρε το σωστό κλειδί.

Έτσι, φαίνεται ότι εάν ο αντίπαλος επιλέξει να λύσει το πρόβλημα αναζήτησης συζυγίας στην ομάδα G ώστε να ανακτήσει το x και το y, θα πρέπει να αντιμετωπίσει είτε το *Membership search* πρόβλημα είτε το *Membership decision* πρόβλημα· το τελευταίο μπορεί να είναι αλγοριθμικά μη επιλύσιμο στην ομάδα που μας δίνεται. Στην πραγματικότητα ο αντίπαλος πρέπει να λύσει μια δυσκολότερη έκδοση του προβλήματος αναζήτησης συζυγίας:

Δίνεται μία ομάδα G, μία υποομάδα $A \leq G$, και δύο στοιχεία $g, h \in G$. Βρείτε $x \in A$ τέτοιο που $h = x^{-1}gx$, δεδομένου ότι υπάρχει τουλάχιστον ένα τέτοιο x.

.

1.6 ΠΡΩΤΟΚΟΛΛΑ ΠΙΣΤΟΠΟΙΗΣΗΣ ΒΑΣΙΣΜΕΝΑ ΣΤΟ ΠΡΟΒΛΗΜΑ ΤΗΣ ΣΥΖΥΓΙΑΣ

.

Ο κύριος σκοπός ενός πρωτοκόλλου πιστοποίησης είναι να επιτραπεί σε έναν νόμιμο χρήστη (Αλίκη) να αποδείξει την ταυτότητά του, μέσα από ένα επισφαλές κανάλι, σε έναν κεντρικό υπολογιστή (Βασίλη), που χρησιμοποιεί το ιδιωτικό του κλειδί, χωρίς διαρροή οποιονδήποτε πληροφοριών που το αφορούν. Η Αλίκη συνήθως αναφέρεται ως *prover* και ο Βασίλης ως *verifier*.

1.6.1 ΣΧΗΜΑ *DIFFIE-HELLMAN*

.

Έστω G μία ομάδα και $A, B < G$ δύο μεταθετικές υποομάδες της G, δηλ. $ab = ba$ για κάθε $a \in A$ και $b \in B$.

Το ιδιωτικό κλειδί της Αλίκης είναι ένα στοιχείο $s \in A$. Το δημόσιο κλειδί της Αλίκης είναι ένα ζευγάρι (w, t), όπου w είναι ένα τυχαίο στοιχείο της G και $t = s^{-1}ws$.

Το πρωτόκολλο πιστοποίησης είναι:

(1). Ο Βασίλης επιλέγει $r \in B$ και στέλνει $w^{'} = r^{-1}wr$ στην Αλίκη.

(2). Η Αλίκη στέλνει την απάντηση $w^{''} = s^{-1}w^{'}s$ στον Βασίλη.

(3). Ο Βασίλης ελέγχει αν $w^{''} = r^{-1}tr$

Μια σωστή απάντηση του *prover* στο δεύτερο βήμα οδηγεί στην αποδοχή από τον *verifier* επειδή εκ κατασκευής τα στοιχεία r και s αντιμετατίθενται, και ως εκ τούτου η παρακάτω ισότητα ικανοποιείται:

$$w^{''} = s^{-1}w^{'}s = s^{-1}r^{-1}wrs = r^{-1}s^{-1}wsr = r^{-1}tr$$

.

1.6.2 ΣΧΗΜΑ *FIAT-SHAMIR*

.

Μία άλλη προτεινόμενη ομάδα που βασίζεται σε ένα σχήμα πιστοποίησης οφείλεται στον *Sibert et. al.* Μία από τις σημαντικές διαφορές του από το σχήμα $Diffie-Hellman$ είναι ότι δε χρειάζεται να διαλέξουμε μεταθετικές υποομάδες Α και Β.

Όπως παραπάνω το ιδιωτικό κλειδί της Αλίκης είναι ένα στοιχείο $s \in G$ και το δημόσιο κλειδί της ένα ζευγάρι (w, t), όπου w είναι ένα τυχαίο στοιχείο της G και $t = s^{-1}ws$.

Το πρωτόκολλο πιστοποίησης είναι:

1. Η Αλίκη επιλέγει ένα τυχαίο στοιχείο $r \in G$ και στέλνει το στοιχείο $x = r^{-1}tr$, που καλείται *δέσμευση*, στον Βασίλη.
2. Ο Βασίλης επιλέγει ένα τυχαίο *bit* c και το στέλνει στην Αλίκη.
   - Αν $c = 0$, τότε η Αλίκη στέλνει $y = r$ στον Βασίλη και ο Βασίλης ελέγχει αν η ισότητα $x = y^{-1}ty$ ικανοποιείται.
   - Αν $c = 1$, τότε η Αλίκη στέλνει $y = sr$ στον Βασίλη και ο Βασίλης ελέγχει αν η ισότητα $x = y^{-1}wy$ ικανοποιείται.

Είναι τετριμμένο να ελέγξουμε αν μια σωστή απάντηση του *prover* στο δεύτερο βήμα οδηγεί σε αποδοχή από τον *verifier*. Είναι όμως, κάπως λιγότερο εμφανές γιατί απαιτείται μια τέτοια ρύθμιση (το τυχαίο *bit*)· φαίνεται ότι η Αλίκη θα μπορούσε αν ήθελε να αποκαλύψει το $y = sr$: αυτό δεν αποκαλύπτει το μυστικό s, και ακόμα επιτρέπει στον Βασίλη να ελέγξει την ισότητα $x = y^{-1}wy$.

Εδώ σε αυτήν την περίπτωση, ο αντίπαλος, θα μπορούσε να πάρει ένα αυθαίρετο στοιχείο u και να στείλει $x = u^{-1}wu$ στον Βασίλη ως δέσμευση. Τότε αυτό το u θα μπορούσε να παίξει τον ίδιο ρόλο όπως το $y = sr$ για την επαλήθευση. Ομοίως, εάν ο αντίπαλος, ήξερε ότι η Αλίκη στα σίγουρα θα έστελνε $y = r$ για την επαλήθευση θα χρησιμοποιούσε ένα αυθαίρετο στοιχείο u στη θέση του r στο βήμα της δέσμευσης. Αυτές οι εκτιμήσεις, δείχνουν επίσης ότι το παραπάνω πρωτόκολλο πιστοποίησης θα πρέπει να τρέξει αρκετές φορές για καλύτερη αξιοπιστία διότι με ένα τρέξιμο, ο αντίπαλος θα μπορούσε επιτυχώς να πλαστοπροσωπήσει την Αλίκη με πιθανότητα $\frac{1}{2}$. Μετά από k τρεξίματα η πιθανότητα μειώνεται στο $\frac{1}{2^k}$.

Η ασφάλεια του σχήματος $Fiat-Shamir$ εξαρτάται από την υπολογιστική σκληρότητα του προβλήματος αναζήτησης συζυγίας στην ομάδα G. Είναι ενδιαφέρον να σημειωθεί ότι το πρόβλημα αναζήτησης αποσύνθεσης δεν μπορεί να χρησιμοποιηθεί για να επιτεθεί σε αυτό το ιδιαίτερο πρωτόκολλο επειδή ο Βασίλης δέχεται ακριβώς ένα στοιχείο, είτε r είτε sr, ανάλογα με τη τιμή του c, στο τελευταίο βήμα του πρωτοκόλλου.

.

1.6.3 ΣΧΗΜΑ ΠΙΣΤΟΠΟΙΗΣΗΣ ΒΑΣΙΣΜΕΝΟ ΣΤΟ ΣΥΝΕΣΤΡΑΜΜΕΝΟ ΠΡΟΒΛΗΜΑ ΣΥΖΥΓΙΑΣ

.
Το σχήμα πιστοποίησης *Fiat-Shamir* μπορεί να τροποποιηθεί ώστε να βασίζεται στο πρόβλημα αποσύνθεσης. Το σχήμα επιτρέπει επίσης μια πιό ενδιαφέρουσα τροποποίηση. Έστω φ ένας αυθαίρετος ενδομορφισμός (δηλ. ομομορφισμός στον εαυτό του) της ομάδας πλατφόρμαςG. Υποθέτουμε ότι η φ είναι δημοσίως γνωστή π.χ. μπορεί να είναι μέρος του δημόσιου κλειδιού της Αλίκης. Το ιδιωτικό κλειδί της Αλίκης είναι ένα στοιχείο $s \in G$ και το δημόσιο κλειδί της είναι ένα ζευγάρι (w, t), όπου w είναι ένα αυθαίρετο στοιχείο της G και $t = s^{-1}w\varphi(s)$.

Το πρωτόκολλο πιστοποίησης είναι:

- Αλίκη επιλέγει ένα τυχαίο στοιχείο $r \in G$ και στέλνει το στοιχείο $x = r^{-1}t\varphi(r)$, που καλείται *δέσμευση*, στον Βασίλη.

- Ο Βασίλης επιλέγει ένα τυχαίο *bit* c και το στέλνει στην Αλίκη.

  - Αν $c = 0$, τότε η Αλίκη στέλνει $y = r$ στον Βασίλη και ο Βασίλης ελέγχει αν η ισότητα $x = y^{-1}t\varphi(y)$ ικανοποιείται.

  - Αν $c = 1$, τότε η Αλίκη στέλνει $y = sr$ στον Βασίλη και ο Βασίλης ελέγχει αν η ισότητα $x = y^{-1}w\varphi(y)$ ικανοποιείται.

Πάλι, η σωστή απάντηση του *prover* στο δεύτερο βήμα οδηγεί σε αποδοχή από τον *verifier*.

Για να σπάσει το πρωτόκολλο αρκεί να βρούμε κάποιο στοιχείο $s^{'} \in G$ τέτοιο ώστε $t = (s^{'})^{-1}w\varphi(s^{'})$ το οποίο είναι ένα στιγμιότυπο ενός προβλήματος γνωστού ως πρόβλημα συνεστραμμένης (αναζήτησης) συζυγίας (*twisted conjugacy (search) problem*).

►Ορισμός. Πρόβλημα συνεστραμμένης (αναζήτησης) συζυγίας.
Έστω G μία ομάδα. Για κάθε $\varphi \in Aut(G)$ και ένα ζευγάρι στοιχείων $w, t \in G$, βρείτε ένα συνεστραμμένο συζυγές για τα w και t, δηλ. ένα στοιχείο $s \in G$ τέτοιο που $t = s^{-1}w\varphi(s)$ παρέχοντας ότι υπάρχει τουλάχιστον ένα τέτοιο s.

Η έκδοση απόφασης αυτού του προβλήματος είναι ένα σχετικά νέο αλγοριθμικό πρόβλημα στη θεωρία ομάδας· είναι αρκετά μη τετριμμένο, ακόμα και για ελεύθερες ομάδες.

.

Κεφάλαιο 2

ΟΜΑΔΕΣ ΠΛΑΤΦΟΡΜΕΣ

.

Παραπάνω περιγράψαμε μερικές από τις προϋποθέσεις που πρέπει να έχει η ομάδα πλατφόρμα σ΄ ένα πρωτόκολλο βασισμένο στο πρόβλημα αναζήτησης συζυγίας. Στην ουσία οι περισσότερες από αυτές τις απαιτήσεις ισχύουν για οποιοδήποτε «κανονικό» (δηλ. βασισμένο σε μια μονόδρομη λειτουργία) πρωτόκολλο κρυπτογραφίας, οπότε και συνοψίζουμε τις πιο γενικές:

($O\Pi_0$) Η ομάδα πρέπει να είναι πολύ καλά-γνωστή (ή καλά μελετημένη ή και τα δύο).

($O\Pi_1$) Το πρόβλημα της λέξης στην ομάδα G πρέπει να έχει μια γρήγορη (γραμμικού ή τετραγωνικού χρόνου) λύση από έναν ντετερμινιστικό αλγόριθμο. Ακόμα καλύτερα, να έχει μια υπολογίσιμη «κανονική μορφή» για τα στοιχεία της G.

($O\Pi_2$) Πρέπει να υπάρξει τρόπος ώστε να μπορούν να ¨μεταμφιεστούν' τα στοιχεία της ομάδας G έτσι που να είναι αδύνατο να ανακτηθούν. Πάλι εδώ είναι χρήσιμη, μια υπολογίσιμη κανονική μορφή. Ελλείψει κανονικής μορφής, ας πούμε ότι αν η G δίνεται ακριβώς υπο την έννοια γεννητόρων και σχέσεων χωρίς να δίδονται κάποιες πρόσθετες πληροφορίες για τις ιδιότητες της G, τότε τουλάχιστον μερικές από αυτές τις σχέσεις θα πρέπει να είναι πολύ σύντομες.

($O\Pi_3$) Η ομάδα G πρέπει να είναι μία ομάδα *super*-πολυωνυμικής (δηλ., εκθετικής ή «ενδιάμεσης») αύξησης. Αυτό σημαίνει ότι ο αριθμός στοιχείων μήκους n στη G θα πρέπει να αυξηθεί γρηγορότερα απ΄ ότι σ΄ ένα οποιοδήποτε πολυώνυμο τάξης n. Αυτό απαιτείται για να αποτρέψει τυχόν επιθέσεις για πλήρη εξαγωγή του βασικού κλειδιού. Εδώ «το μήκος n » είναι τυπικά το μήκος μιας λέξης που αντιπροσωπεύει ένα στοιχείο της ομάδας, αλλά σε μια πιο γενική κατάσταση, θα μπορούσε να είναι το μήκος κάποιας άλλης περιγραφής, ας πούμε της «πολυπλοκότητας πληροφοριών».

Σ΄ αυτό το κεφάλαιο, θα εξετάσουμε μερικές ομάδες (ή κλάσεις ομάδων) ως πιθανές πλατφόρμες των κρυπτογραφικών πρωτοκόλλων του δημόσιου κλειδιού.

2.1 ΟΜΑΔΕΣ ΠΛΕΞΙΔΕΣ

.

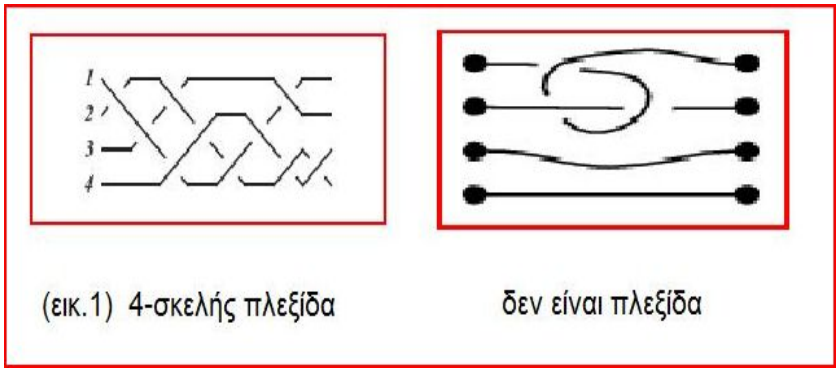
Οι ομάδες πλεξίδες εμφανίστηκαν ως πλατφόρμες μη μεταθετικών κρυπτογραφικών πρωτοκόλλων δημοσίου κλειδιού στο άρθρο [1]. Η παράδοση λέει ότι σφού οι συγγραφείς του άρθρου[1] είχαν βρει το πρωτόκολλό τους πλησίασαν την *Joan Birman* και της ζήτησαν να τους συστήσει «καλές» μη αβελιανές ομάδες που θα μπορούσαν να χρησιμοποιήσουν ως πλατφόρμες. Και η απάντηση ήταν «ομάδες πλεξίδων». Μετά από κάποιο αρχικό ενθουσιασμό που οδήγησε ακόμη και στην ονομασία ενός νέου τομέα «του συστήματος κρυπτογραφίας ομάδας πλεξίδας», τώρα φαίνεται ότι το πρόβλημα αναζήτησης συζυγίας σε μια ομάδα πλεξίδα δεν παρέχει ένα ικανοποιητικό επίπεδο ασφάλειας εκτός αν τα κλειδιά επιλεχθούν (ακόμα για να καθοριστούν) από μερικά μάλλον πολύ μικρά υποσύνολα της ομάδας. Παρακάτω θα συζητήσουμε εν συντομία τα πλεονεκτήματα και τα μειονεκτήματα των ομάδων πλεξίδων, και έπειτα θα δώσουμε ένα θεωρητικό υπόβαθρο για τον ενδιαφερόμενο αναγνώστη. Είναι γεγονός ότι οι αφηρημένες ομάδες δημιουργούν γενικά ένα πρόβλημα άμεσης αντίληψης τους, ενώ αντίθετα οι ομάδες πλεξίδες με ένα σύρσιμο απλών εικόνων μπορούν να εξηγήσουν τι ακριβώς είναι. Οι ομάδες πλεξίδες χρησιμοποιούν πολλούς διαφορετικούς τομείς μαθηματικών (και φυσικής) κι αυτό τους δίνει περισσότερη αξιοπιστία στη σκληρότητα του σχετικού προβλήματος (π.χ. πρόβλημα αναζήτησης συζυγίας).

Η εμπιστοσύνη στην ασφάλεια του κρυπτογραφικού συστήματος RSA βασίζεται κυριολεκτικά στην άμεση παραγοντοποίηση ακεραίων, πράγμα που προσπάθησαν για αιώνες χιλιάδες άνθρωποι, συμπεριλαμβανομένων και των *Euler* και *Gauss*. Η ιστορία των ομάδων πλεξίδων πηγαίνει πίσω προς το 1927, όπου εκατοντάδες άνθρωποι, συμπεριλαμβανομένων εξαίρετων μαθηματικών όπως *Artin*, *Birman*, *Thurston V.F.R. Jones*, και άλλων οι οποίοι δούλεψαν γύρω από διάφορες πτυχές αυτών των ομάδων, συμπεριλαμβανόμενης και της αλγοριθμικής. Απ΄ την άλλη μεριά όμως, από άποψη ασφάλειας, το γεγονός ότι οι ομάδες πλεξίδες εισχωρούν σε πολλές διαφορετικές περιοχές, αυτό μπορεί να αποτελέσει μειονέκτημα, επειδή μπορούν να παρέχουν διαφορετικά εργαλεία έτσι ώστε ένα πρόβλημα να γίνει προσιτό. Επιπλέον, οι ομάδες πλεξίδες αποδείχθηκαν γραμμικές, που τις καθιστά ενδεχομένως τρωτές στις γραμμικές αλγεβρικές επιθέσεις, το οποίο αυτό και μόνο είναι ένας σοβαρός κίνδυνος ασφάλειας.

Όπως αναφέραμε και πιο πριν, οι ομάδες πλεξίδες εμφανίζονται σε διάφορους τομείς των μαθηματικών, και έχουν πολλούς ισοδύναμους ορισμούς. Αρχίζουμε με μια αναπαράσταση τους με γεννήτορες και σχέσεις.

2.1.1 Η ΟΜΑΔΑ ΠΛΕΞΙΔΑ ΚΑΙ Η ΑΝΑΠΑΡΑΣΤΑΣΗ ΤΗΣ

► **Ορισμοί.** Μία πλεξίδα λαμβάνεται από τον καθορισμό παράλληλων ράβδων (σκέλη ή μέλη της πλεξίδας) και τον συνδιασμό τους προς την ίδια κατεύθυνση. Το επίπεδο που δημιουργούν οι παράλληλες ράβδοι είναι κάθετο με το έδαφος. Αριθμούμε τα σκέλη που είναι σε κάθε οριζόντια (ή κάθετη) θέση από πάνω προς τα κάτω (εικ.1).



Στα άκρα της κάθε ράβδου A_iC_i για $i = 1, ...n$ υπάρχουν γάντζοι-σημεία A_i, C_i που ικανοποιούν τη σχέση:

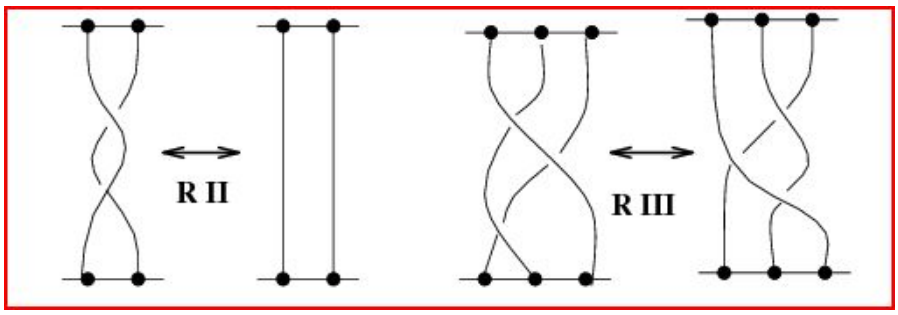
$$|A_{i+1} - A_i| = c = |C_{i+1} - C_i|$$

$\forall i : 0 \leq i \leq n-1$ και έτσι ώστε το A_i να βρίσκεται ακριβώς πάνω από το C_i. Υποθέτουμε ότι υπάρχουν n νήματα (ή καλώδια) με το ένα άκρο τους δεμένο σε κάποιον από τους γάντζους A_i και το άλλο τους άκρο σε κάποιον από τους γάντζους C_i. Δε πρέπει τα νήματα να μπλέκονται με τον εαυτό τους τους ούτε να δημιουργούν κόμπους, δηλ. γενικά να μη δημιουργούν U-στροφή. Πιο αυστηρά, κάθε ένας από τους γάντζους πρέπει να έχει δεμένο ακριβώς ένα νήμα και κάθε επίπεδο κάθετο στο επίπεδο των ράβδων, παράλληλο προς αυτές και διερχόμενο ανάμεσα τους να τέμνει κάθε νήμα σε ακριβώς ένα σημείο.

• Εαν τοποθετήσουμε δύο πλεξίδες u και v σε μία σειρά έτσι που το τέλος της u να ταιριάζει με την αρχή της v, παίρνουμε μια άλλη πλεξίδα την uv δηλ. η **παράθεση** n-μελών πλεξίδων είναι επίσης πλεξίδα.

.

• Δύο πλεξίδες είναι **ισοδύναμες** αν υπάρχει ένας ισότοπος μεταξύ τους, δηλ. αν είναι δυνατόν να μετακινηθούν τα σκέλη της μιας πλεξίδας στο χώρο (χωρίς να μετακινηθούν τα άκρα των σκελών και χωρίς να μετακινηθεί το ένα σκέλος μέσω του άλλου) ώστε να πάρουμε την άλλη πλεξίδα (εικ.2).



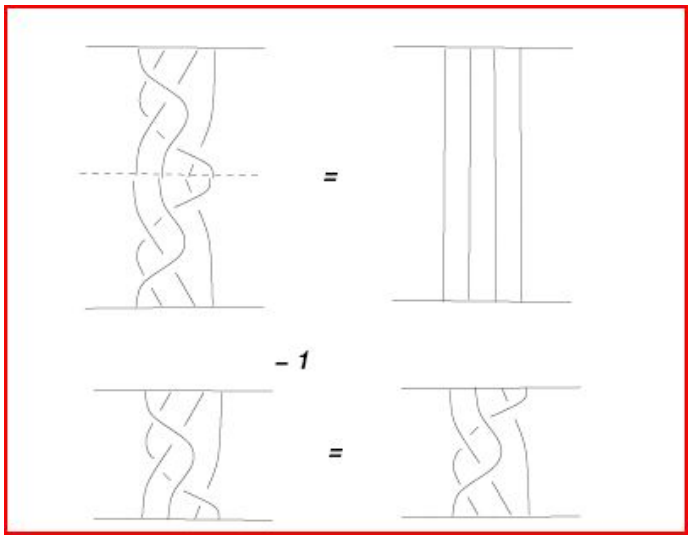
(**εικ.2**)

• Η n-μελής πλεξίδα που δεν περιέχει διασταυρώσεις ονομάζεται **τετριμμένη πλεξίδα**(εικ.2). Η τετριμμένη πλεξίδα συμπεριφέρεται όπως το μοναδιαίο στοιχείο από αριστερά κι από δεξιά στον πολλαπλασιασμό. Το σύνολο B_n των κλάσεων των ισοτόπων των n-μελών πλεξίδων, το οποίο καλούμε **n-πλεξίδα** έχει τη δομή ομάδας διότι αν παραθέσουμε μία πλεξίδα με το καθρέπτισμα της το αποτέλεσμα θα είναι ισότοπο με τη τετριμμένη πλεξίδα.
Στην ουσία πλεξίδα είναι μια ακολουθία διασταυρώσεων των σκελών της.
Οι ομάδες B_0 και B_1 είναι τετριμμένες.
Η B_2 είναι άπειρη κυκλική ομάδα.

• Μια διασταύρωση καλείται **θετική** αν το σκέλος που έρχεται από δεξιά περνά πάνω απ΄ αυτό που έρχεται από αριστερά. Στην αντίθετη περίπτωση καλείται **αρνητική**. Υπάρχουν ακριβώς $n-1$ τύποι διασταυρώσεων για μια n-μελή πλεξίδα που τις συμβολίζουμε $x_1, ..., x_{n-1}$, όπου x_i είναι η θετική διασταύρωση του i-οστού και του $i+1$-οστού σκέλους.

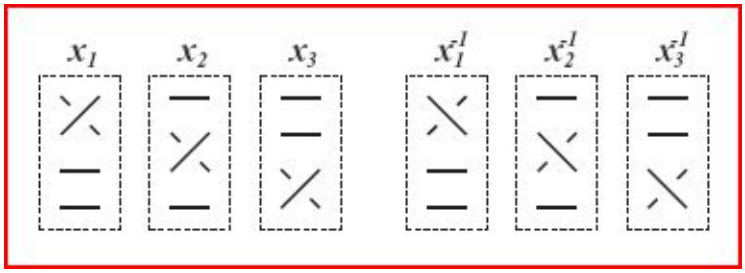
• **Το αντίστροφο μιας πλεξίδας** λαμβάνεται από την απεικόνιση της σε έναν οριζόντιο καθρέφτη που τοποθετείται στο επίπεδο του χαμηλότερου πλαισίου της πλεξίδας (εικ.3).

.



(**εικ.3**)

• Αφού κάθε πλεξίδα είναι μία ακολουθία διασταυρώσεων λέμε ότι το σύνολο $x_1, ..., x_{n-1}$ **παράγει** το B_n.



(**εικ.4**): Οι γεννήτορες του B_4 και οι αντίστροφοι τους

Είναι εύκολο να δει κανείς ότι οι διασταυρώσεις $x_1, ..., x_{n-1}$ ικανοποιούν τις σχέσεις:

$$[x_i, x_j] = 1$$

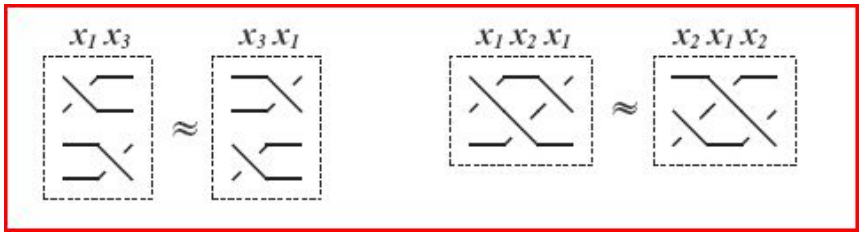
για κάθε i, j τέτοια που $|i - j| > 1$, και

$$x_i x_{i+1} x_i = x_{i+1} x_i x_i x_{i+1}$$

για κάθε i έτσι ώστε $1 \leq i \leq n - 2$.
Βέβαια είναι δύσκολο ν΄ αποδειχτεί ότι αυτές οι δύο σχέσεις περιγράφουν πραγματικά

την ισοδυναμία στις πλεξίδες, δηλ. η ομάδα πλεξίδων B_n έχει την $(Artin)$ αναπαράσταση (εικ.5):

$$B_n = \Big\langle x_1, ..., x_{n-1} \quad \Big| \quad x_i x_{i+1} x_i = x_{i+1} x_i x_{i+1} \quad \alpha\nu \quad |i-j| = 1$$
$$x_i x_j = x_j x_i \quad \alpha\nu \quad |i-j| > 1 \Big\rangle$$



(εικ.5)

Προκειμένου να περιγραφούν τα διαγράμματα πλεξίδων, μπορούμε να τα κωδικοποιήσουμε χρησιμοποιώντας τη **λέξη πλεξίδας**, δηλ. μια πεπερασμένη ακολουθία γραμμάτων. Εξετάζουμε από πάνω προς τα κάτω, τη πεπερασμένη διαδοχή των διασταυρώσεων, δηλ. ποια σκέλη διασχίζουν οι διαδοχικές διασταυρώσεις και με ποιο προσανατολισμό. Πιο αναλυτικά, έστω οι αριθμοί-θέσεις από το 1 έως το n σε ένα διάγραμμα πλεξίδων n σκελών και κάποιος καλεί το x_1· αυτό δηλώνει το πέρασμα όπου το σκέλος στη θέση 2 διασχίζει το σκέλος στη θέση 1, κατόπιν το x_2 που είναι το πέρασμα όπου το σκέλος στη θέση 3 διασχίζει το σκέλος στη θέση 2 κ.λπ. Συμμετρικά, θα χρησιμοποιούμε το x_1^{-1} για το πέρασμα όπου το σκέλος στη θέση 1 διασχίζει το σκέλος στη θέση 2, κατόπιν x_2^{-1} το πέρασμα όπου το σκέλος στη θέση 2 διασχίζει το σκέλος στη θέση 3 κ.λ.π.

2.1.2 *DEHORNOY HANDLE*

.

Μέχρι να φτάσουμε στη *Dehornoy handle* θα απαντήσουμε κατ' αρχήν σε ορισμένες εισαγωγικές ερωτήσεις.

• Ποιο είναι το πρόβλημα της τετριμμένης πλεξίδας;

Το πρόβλημα της τετριμμένης πλεξίδας είναι το εξής αλγοριθμικό πρόβλημα:
○ Δίνεται το διάγραμμα μιας πλεξίδας. Αποφασίστε εάν είναι η τετριμμένη.
Το διάγραμμα χωρίς πέρασμα κωδικοποιείται με την κενή λέξη (η λέξη με κανένα

γράμμα). Οπότε το πρόβλημα της τετριμμένης πλεξίδας μπορεί να διαμορφωθεί ως εξής:

◦ Δίνεται μια λέξη πλεξίδων. Αποφασίστε εάν είναι ισοδύναμη με την κενή λέξη.

• Το πρόβλημα των ισοτόπων πλεξίδων και το πρόβλημα της τετριμμένης πλεξίδας σχετίζονται;

Ναι, είναι πράγματι ισοδύναμα προβλήματα. Αρχικά, το πρόβλημα της τετριμμένης πλεξίδας είναι μια ειδική περίπτωση του προβλήματος των ισοτόπων πλεξίδων, έτσι που κάθε λύση στο τελευταίο δίνει αυτόματα μια λύση στα πρώτο. Αυτό εύκολα μπορεί κάποιος να το ελέγξει διότι, αν Δ και Ε είναι διαγράμματα n-σκελών πλεξίδων, τότε Δ και Ε ισοτοπικά εάν και μόνο εάν το διάγραμμα Ζ της πλεξίδας που λαμβάνεται από την ανάκλαση της εικόνας του Δ σε έναν οριζόντιο καθρέφτη επί του Δ, είναι η τετριμμένη πλεξίδα. Κατά συνέπεια, οποιαδήποτε λύση στο πρόβλημα της τετριμμένης πλεξίδας οδηγεί σε μια λύση στο πρόβλημα των ισοτόπων πλεξίδων.

• Τι είναι η *Handle* αναγωγή (*handle reduction*) ;

Η *Handle* αναγωγή είναι ένας από τους πολλούς τρόπους να λυθεί το πρόβλημα της τετριμμένης πλεξίδας δηλ. να αποφασιστεί αν το διάγραμμα πλεξίδας που κωδικοποιείται από μια δεδομένη λέξη πλεξίδας μπορεί να διαμορφωθεί σε ένα διάγραμμα χωρίς πέρασμα. Εξ αιτίας της παραπάνω παρατήρησης, η *Handle* αναγωγή παρέχει επίσης μια λύση στο πρόβλημα ισοτόπων πλεξίδων. Η *Handle* αναγωγή αποδεικνύεται εξαιρετικά αποδοτική στην πράξη: όταν εφαρμόζεται κατάλληλα, συγκρίνει διαγράμματα που περιλαμβάνουν χιλιάδες διασταυρώσεις σε λιγότερο από ένα λεπτό.

• Τι είναι *Handle* ;

Handle είναι μια λέξη πλεξίδας ειδικού τύπου. Έστω s ένα οποιοδήποτε γράμμα (από το a, b,...) που είναι το κατώτερο, τότε ορίζουμε ως s-*Handle* τη λέξη πλεξίδας τύπου $s...S$, όπου S είναι το ανώτερο γράμμα που συνδέεται με το s ενώ όλα τα ενδιάμεσα γράμματα μεταξύ του s και του S είναι γράμματα πριν το s κατά αλφαβητική σειρά.
Συμμετρικά, αν S ένα οποιοδήποτε γράμμα (από το a, b,...) που είναι το ανώτερο, τότε ορίζουμε ως S-*Handle* τη λέξη πλεξίδας τύπου $S...s$, όπου s είναι το κατώτερο γράμμα που συνδέεται με το S ενώ όλα τα ενδιάμεσα γράμματα μεταξύ του S και του s είναι γράμματα πριν το s κατά αλφαβητική σειρά.

Και τώρα είμαστε έτοιμοι να συζητήσουμε τη *Dehornoy handle*.

• Έστω w μία λέξη από τους γεννήτορες του B_n. Μία x_i-*handle* είναι μια υπολέξη της w της μορφής:

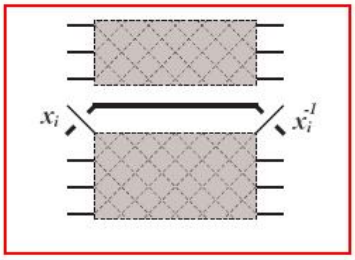
$$x_i^{-\varepsilon} w(x_1, ..., x_{i-2}, x_{i+1}, ..., x_n) x_i^{\varepsilon}$$

όπου $\varepsilon = \pm 1$ (εικ.6).

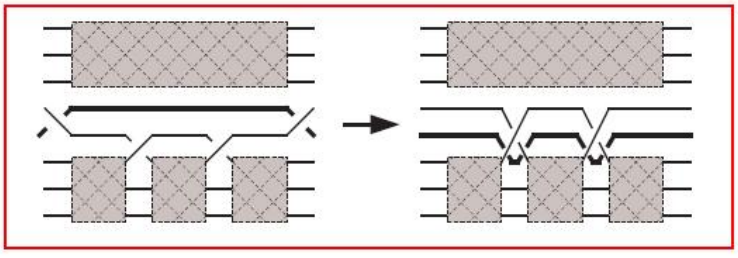
• Μία x_i-*handle* $x_i^{-\varepsilon} w x_i^{\varepsilon}$ όπου $w = w(x_1, ..., x_{i-2}, x_{i+1}, ..., x_n)$ καλείται **επιτρεπόμενη** (*permitted*) αν η w δεν περιέχει x_{i+1}-*handles*.

• Λέμε ότι η λέξη πλεξίδα v' λαμβάνεται από τη λέξη πλεξίδα v με **ενός βήματος** *handle*-**αναγωγή** (*one step handle reduction*) (εικ.7) αν κάποια υπολέξη του v είναι μία επιτρεπόμενη x_i-*handle* $x_i^{-\varepsilon} w x_i^{\varepsilon}$ και η v' λαμβάνεται από τη v με την εφαρμογή των ακόλουθων αντικαταστάσεων όλων των γραμμάτων στη *handle* $x_i^{-\varepsilon} w x_i^{\varepsilon}$:

$$x_j^{\pm 1} \longrightarrow \begin{cases} 1 & \text{αν } j = i \\ x_{i+1}^{\varepsilon} x_i^{\pm 1} x_{i+1}^{\varepsilon} & \text{αν } j = i+1 \\ x_j^{\pm 1} & \text{αν } j < i \text{ και } j > i+1 \end{cases}$$



εικ.6 : Handle



εικ.7 : Ενός βήματος handle αναγωγή μίας επιτρεπόμενης x_i-handle

.

• Λέμε ότι η λέξη πλεξίδα $v^{'}$ λαμβάνεται από τη λέξη πλεξίδα v μετά από m **βήματα** $handle$**-αναγωγής** αν υπάρχει ακολουθία $m+1$ λέξεων $v = v_0, v_1, ..., v_m = v^{'}$ κάθε μία εκ των οποίων λαμβάνεται από τη προηγούμενη με ενός βήματος $handle$ αναγωγή.

• Μια λέξη πλεξίδας καλείται $handle$ **ελεύθερη** εάν δεν περιέχει καμία $handle$. Η $handle$ αναγωγή μπορεί να διατυπωθεί με το ακόλουθο θεώρημα:

Θεώρημα: Έστω v μια λέξη πλεξίδα. Τότε:
• Κάθε ακολουθία $handle$-αναγωγών που εφαρμόζονται για τη v τελικά σταματούν και παράγουν μία $handle$ ελεύθερη λέξη πλεξίδα $v^{'}$ (που γενικά εξαρτάται από την ιδιαίτερη ακολουθία αναγωγών) η οποία αντιπροσωπεύει το στοιχείο της ομάδας πλεξίδων που είναι ίδιο με το v.
• Η λέξη v αντιπροσωπεύει το μοναδιαίο στοιχείο της ομάδας πλεξίδων αν και μόνο αν οποιαδήποτε ακολουθία $handle$-αναγωγών που εφαρμόζονται στο v παράγει την τετριμμένη λέξη.

2.1.3 Η κανονικη μορφη του *Garside*

.

• Έστω μια ομάδα μεταθέσεων S_n με n σύμβολα. Για κάθε μετάθεση $s \in S_n$ θεωρούμε την κοντύτερη θετική πλεξίδα ξ_s έτσι ώστε $\pi(\xi_s) = s$. Τα στοιχεία:

$$S = \{\xi_s \mid s \in S_n\} \subset B_n$$

καλούνται **απλά στοιχεία**.

• Για τις μεταθέσεις s και t λέμε ότι ένα απλό στοιχείο ξ_s είναι είναι **μικρότερο** από το ξ_t (ή, ότι το ξ_s είναι ένας αριστερός διαιρέτης του ξ_t) και το συμβολίζουμε με $\xi_s < \xi_t$ αν υπάρχει $r \in S_n$ τέτοιο ώστε $\xi_t = \xi_s\xi_r$.

Υπάρχουν δύο ειδικές απλές πλεξίδες του B_n: η τετριμμένη πλεξίδα που είναι το μικρότερο στοιχείο του S και η ημι-ανεστραμμένη πλεξίδα $\Delta = \xi_{(n,n-1,...,2,1)}$ η οποία είναι το μεγαλύτερο στοιχείο του S. Το σύνολο των απλών πλεξίδων της τάξης $<$ όπως ορίστηκε παραπάνω έχει τη δομή πλέγματος με gcd και lcm που ορίζονται ως εξής:

$$gcd(\xi_s, \xi_t) = max\{\xi_r \mid \xi_r < \xi_s \text{ και } \xi_r < \xi_t\}$$

και

$$lcm(\xi_s, \xi_t) = min\{\xi_r \mid \xi_s < \xi_r \text{ και } \xi_t < \xi_r\}$$

Παρατηρούμε ότι αφού το S περιέχει και το ελαχιστικό στοιχείο και μεγιστικό οι gcd και lcm είναι καλά ορισμένες.

• **Η αριστερή κανονική μορφή μιας πλεξίδας** $\alpha \in B_n$ **του** $Garside$ είναι ένα ζευγάρι $(p,(s_1,...,s_l))$, όπου $p \in \mathbb{Z}$ και $s_1,...,s_l$ μία ακολουθία μεταθέσεων στο $S_n - \{1,\Delta\}$ που ικανοποιεί την παρακάτω ιδιότητα: για κάθε $i = 1,...,l-1$,

$$\xi_1 = gcd(\xi_{s_i^{-1}\Delta}, \xi_{s_{i+1}})$$

Η κανονική μορφή $(p,(s_1,...,s_l))$, αναπαριστά το παρακάτω στοιχείο του B_n:

$$\xi_\Delta^p \cdot \xi_{s_1} \cdot ... \cdot \xi_{s_n}$$

Θεώρημα (εκτίμηση πολυπλοκότητας). Υπάρχει ένας αλγόριθμος που για οποιαδήποτε λέξη πλεξίδας $w = w(x_1,...,x_{n-1})$ υπολογίζει την κανονική μορφή της αντίστοιχης πλεξίδας.
Επιπλέον, η χρονική πολυπλοκότητα του αλγορίθμου είναι $O(n^2|w|^2)$.

2.2 ΟΜΑΔΑ *THOMPSON*

.

Η ομάδα $Thompson\ F$, όπως και οι ομάδες πλεξίδων B_n είναι πολύ καλά γνωστές σε πολλούς κλάδους μαθηματικών όπως της άλγεβρας, της γεωμετρίας,της ανάλυσης κι οπότε ικανοποιεί την ιδιότητα (OB_0) στην εισαγωγή του κεφαλαίου. Επίσης, αυτή η ομάδα είναι άπειρη μη αβελιανή.

Τώρα όσον αφορά τις ιδιότητες $(OB_1)-(OB_3)$ σημειώνουμε ότι η ομάδα $Thompson$ έχει την ακόλουθη αναπαράσταση:

$$F = \langle x_0, x_1, x_2, ... \mid x_i^{-1} x_k x_i = x_{k+1}\ (k > i) \rangle \qquad (5.1)$$

Αυτή η αναπαράσταση είναι άπειρη. Επίσης υπάρχουν πεπερασμένες αναπαραστάσεις αυτής της ομάδας. Για παράδειγμα:

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

όμως η άπειρη αναπαράσταση πιο πάνω επιτρέπει μια κατάλληλη κανονική μορφή, οπότε εδώ θα χρησιμοποιήσουμε εκείνη την αναπαράσταση. Η κλασσική κανονική μορφή για ένα στοιχείο της ομάδας $Thompson$ είναι μια λέξη της μορφής:

$$x_{i_1}...x_{i_s}x_{j_t}^{-1}...x_{j_l}^{-1} \qquad (5.2)$$

η οποία ικανοποεί τις επόμενες δύο συνθήκες:

$(NF1)$ $i_1 \leq ... \leq i_s$ και $j_1 \leq ... \leq j_t$

$(NF2)$ αν συμβαίνουν και το x_i και το x_i^{-1} τότε συμβαίνει επίσης είτε το x_{i+1} είτε το x_{i+1}^{-1}.

• Λέμε ότι η λέξη w είναι σε **ημικανονική μορφή** αν είναι της μορφής (5.2) και ικανοποιεί την $(NF1)$.

Έχει δειχτεί ότι η κανονική μορφή μιας δεδομένης λέξης w στην ομάδα $Thompson\ F$ μπορεί να υπολογιστεί σε χρόνο $O(|w|log|w|)$.

2.3 ΟΜΑΔΕΣ ΠΙΝΑΚΩΝ

.

Εδώ προτείνουμε τις ομάδες πινάκων επί πεπερασμένων μεταθετικών δακτυλίων από τις καλύτερες πλατφόρμες για κανονικά κρυπτογραφικά πρωτόκολλα διότι αυτές οι ομάδες έχουν «το καλύτερο και των δύο κόσμων» υπό την έννοια ότι ναι μεν ο πολλαπλασιασμός πινάκων είναι μη μεταθετικός όμως οι καταχωρήσεις πινάκων προέρχονται από μεταθετικό δακτύλιο παρέχοντας έτσι έναν καλό μηχανισμό απόκρυψης. Επίσης οι ομάδες πινάκων έχουν το πλενέκτημα να παρουσιάζουν τα στοιχεία τους σε μία «φυσική» κανονική μορφή.

Ο λόγος που θέλουμε ο βασικός δακτύλιος να είναι πεπερασμένος, είναι ότι οι πεπερασμένοι δακτύλιοι R είναι περιοδικοί και περιοδικός δακτύλιος σημαίνει ότι για κάθε $u \in R$ υπάρχουν θετικοί ακέραιοι m ,k τέτοιοι που $u^m = u^k$.

Τονίζουμε ιδιαίτερα ότι

ΜΕΤΑΘΕΤΙΚΟΤΗΤΑ ΚΑΙ ΠΕΡΙΟΔΙΚΟΤΗΤΑ

.
είναι δύο εργαλεία υψίστης σημασίας στο να κρύβουμε τους παράγοντες ενός γινομένου· παρά ταύτα η σημαντικότητα τους για την ασφάλεια της κρυπτογραφίας δεν μπορεί γενικά να υπερεκτιμηθεί.
Για την καλύτερη ασφάλεια η μεταθετικότητα μπορεί να ενισχυθεί από τη μή μεταθετικότητα. Οπότε η

ΜΕΤΑΘΕΤΙΚΟΤΗΤΑ υπό την ενίσχυση της ΜΗ-ΜΕΤΑΘΕΤΙΚΟΤΗΤΑΣ

είναι ένα άλλο σημαντικό συστατικό για την ασφάλεια της κρυπτογραφίας. Αποτρέπει τον επιτιθέμενο με χρησιμοποίηση προφανών σχέσεων, όπως $ab = ba$, να εξαγάγει

τους παράγοντες του γινομένου.
Τέλος ϑ′ αναφερθούμε σε παραδείγματα πεπερασμένων δακτυλίων που ϑα μπορούσαν να χρησιμοποιηθούν ως βασικοί δακτύλιοι στις ομάδες πινάκων στην κρυπτογραφία:
∘ Ο απλούστερος είναι ο δακτύλιος $\mathbb{Z}_n$.
∘ Ένας άλλος είναι ο $R = F_p[x]/(f(x))$, όπου το F_p είναι σώμα με p στοιχεία, το $F_p[x]$ δακτύλιος πολυωνύμων επί του F_p και $(f(x))$ το ιδεώδες του $F_p[x]$ που παράγεται από το ανάγωγο πολυώνυμο $f(x)$ βαθμού n. Αυτός ο δακτύλιος είναι ισόμορφος με το σώμα F_{p^n}, που όμως η αναπαράσταση του R ως σώμα πηλίκο μας επιτρέπει ένα μεγάλο κλειδί κρατώντας όλες τις βασικές παραμέτρους μάλλον μικρές.

2.4 ΟΜΑΔΕΣ ΜΙΚΡΩΝ ΔΙΑΓΡΑΦΩΝ

.

Οι ομάδες μικρών διαγραφών προτείνονται ως πλατφόρμες.

► **Ορισμός.** Οι **ομάδες μικρών διαγραφών** έχουν σχέσεις ($relators$) που ικανοποιούν μία μετρική συνθήκη. Πιο συγκεκριμμένα έστω $F(X)$ μια ελεύθερη ομάδα με βάση $X = \{x_i \mid i \in I\}$, όπου I ένα σύνολο ευρετήριο. Έστω $\epsilon_k \in \{\pm 1\}$ όπου $1 \leq k \leq n$. Μία λέξη

$$w(x_1, ..., x_n) = x_{i_1}^{\epsilon 1} x_{i_2}^{\epsilon_2} ... x_{i_n}^{\epsilon_n}$$

στο $F(X)$ με όλα τα x_{i_k} όχι απαραιτήτως διακριτά, είναι μια **μειωμένη X-λέξη** ($reduced\ X-word$), αν $x_{i_k}^{\epsilon_k} \neq x_{i_{(k+1)}}^{-\epsilon_{(k+1)}}$, για $1 \leq k-1 \leq n$. Επί προσθέτως, η λέξη $w(x_1, ..., x_n)$ είναι **κυκλικά μειωμένη** ($cyclically\ reduced$) αν είναι μία μειωμένη X-λέξη και $x_{i_1}^{\epsilon_1} \neq x_{i_n}^{-\epsilon_n}$. Ένα σύνολο R που περιέχει κυκλικά μειωμένες λέξεις από το $F(X)$ είναι **συμμετρικό** ($symmetrized$) αν είναι κλειστό ως προς τις κυκλικές μεταθέσεις και στο να παίρνει αντιστρόφους.

► **Ορισμός.** Έστω G μια ομάδα με αναπαράσταση $\langle X; R\rangle$. Μία μη κενή λέξη $u \in F(X)$ καλείται *piece* αν υπάρχουν δύο διαφορετικές σχέσεις ($relators$) $r_1, r_2 \in R$ της G, τέτοιοι ώστε $r_1 = uv_1$ και $r_2 = uv_2$ για κάποια $v_1, v_2 \in F(X)$ και με καμμία απαλοιφή μεταξύ των u και v_1 ή μεταξύ των u και v_2.

Μία ομάδα G ανήκει στη τάξη $C(p)$ αν κανένα στοιχείο του R δεν είναι γινόμενο λιγότερο από p *pieces*.

Επίσης η ομάδα G ανήκει στη τάξη $C'(\lambda)$ αν για κάθε $r \in R$ τέτοιο ώστε $r = uv$ και u είναι ένα *piece* ισχύει: $|u| < \lambda|r|$.

2.4.1 ΑΛΓΟΡΙΘΜΟΣ *DEHN*

.

Αν η G ανήκει στη κλάση $C^{'}(\frac{1}{6})$ τότε ο αλγόριθμος $DEHN$ λύνει το πρόβλημα λέξης αποτελεσματικά. Ο αγόριθμος αυτός είναι πολύ απλός:

1. Σε μία (μη κενή) λέξη εισόδου w, κοιτάζουμε για ένα μεγάλο *piece* της σχέσης $(relator)$ της R (δηλ. ένα *piece* του οποίου το μήκος είναι περισσότερο από το μισό του μήκους ολόκληρης της σχέσης $(relator)$). Αν δεν υπάρχει τέτοιο *piece* τότε παίρνουμε στην έξοδο '$w \neq 1$ στην G'.

2. Εάν ένα τέτοιο *piece*, ας το πούμε u, δεν υπάρχει τότε $r = uv$ για κάποιο $r \in R$, όπου το μήκος της v είναι μικρότερο της u. Τότε αντικαθιστούμε τη u με τη v^{-1} στην w. Το μήκος της λέξης $w^{'}$ του αποτελέσματος είναι μικρότερο από εκείνο της w. Αν $w^{'} = 1$, τότε παίρνουμε στην έξοδο '$w = 1$ στην G'.

3. Εάν το $w^{'} \neq 1$, τότε επαναλαμβάνουμε από ΒΗΜΑ 1. με $w := w^{'}$

Αφού το μήκος της w μειώνεται μετά από κάθε *loop*, αυτός ο αλγόριθμος θα τερματίσει μετά από έναν πεπερασμένο αριθμό βημάτων. Έχει πολυπλοκότητα τετραγωνικού χρόνου ως προς το μήκος της λέξης εισόδου w.

Τέλος, σημειώνουμε ότι μια γενικά πεπερασμένα αναπαραστάσιμη ομάδα είναι μία ομάδα μικρών διαγραφών (δείτε [4]).

2.5 ΕΠΙΛΥΣΙΜΕΣ ΟΜΑΔΕΣ

.

• Ας θυμηθούμε ότι μία ομάδα G καλείται **αβελιανή** (ή μεταθετική) αν $[a, b] = 1$ για κάθε a, b όπου με $[a, b]$ συμβολίζουμε $a^{-1}b^{-1}ab$.
Αυτό μπορεί να γενικευτεί κατά διάφορους τρόπους.
• Μία ομάδα G καλείται **μεταβελιανή** αν $[[x, y], [z, t]] = 1$ για κάθε $x, y, z, t \in G$.
• Μία ομάδα G καλείται **μηδενοδύναμη της τάξης** $c \geq 1$ αν $[y_1, y_2, ..., y_{c+1}] = 1$ για κάθε $y_1, y_2, ..., y_{c+1} \in G$, όπου $[y_1, y_2, y_3] = [[y_1, y_2], y_3]$ κλπ.

• Η **αντιμεταθετική υποομάδα της** G είναι η ομάδα $G^{'} = [G, G]$ που παράγεται από όλους τους αντιμεταθέτες δηλ., από εκφράσεις της μορφής $[u, v] = u^{-1}v^{-1}uv$, όπου $u, v \in G$.

Επιπλέον, μπορούμε να καθορίσουμε, τον k-οστό όρο της *κατώτερης κεντρικής σειράς* της G: $\gamma_1(G) = G$, $\gamma_2(G) = [G, G]$, $\gamma_k(G) = [\gamma_{k-1}(G), G]$. Σημειώστε ότι κάποιο έχει $\alpha([u, v]) = [\alpha(u), \alpha(v)]$ για κάθε ενδομορφισμό α στην G. Επομένως, η $\gamma_k(G)$ είναι μία πλήρως αμετάβλητη υποομάδα της G, για κάθε $k \geq 1$, και έτσι

$$G^{''} = [G^{'}, G^{'}].$$

Θα εστιάσουμε στις ελεύθερες μεταβελιανές ομάδες καθότι αυτές οι ομάδες χρησιμοποιούνται ως πλατφόρμες στα κρυπτογραφικά πρωτόκολλα.

• Έστω F_n μία ελεύθερη ομάδα τάξης n. Η σχετικά ελεύθερη ομάδα $F_n/F_n^{''}$ καλείται **ελεύθερη μεταβελιανή ομάδα** τάξης n, την οποία συμβολίζουμε με M_n.

2.5.1 ΚΑΝΟΝΙΚΕΣ ΜΟΡΦΕΣ ΣΤΙΣ ΕΛΕΥΘΕΡΕΣ ΜΕΤΑΒΕΛΙΑΝΕΣ ΟΜΑΔΕΣ

.

Σε αυτήν την ενότητα θα περιγράψουμε την κανονική και την ημικανονική μορφή των στοιχείων μιας ελεύθερης μεταβελιανής ομάδας M_n. Η ημικανονική μορφή είναι καλή για τις μεταδόσεις, γιατί είναι εύκολα μετατρέψιμη πίσω στη λέξη που αντιπροσωπεύει το μεταδιδόμενο στοιχείο. Εντούτοις, αυτή η μορφή δεν είναι μοναδική εάν $n > 2$ (κι αυτός είναι ο λόγος που τη καλούμε ημικανονική) κι έτσι δε μπορεί να χρησιμοποιηθεί ως κοινό μυστικό από την Αλίκη και το Βασίλη σε ένα κρυπτογραφικό πρωτόκολλο. Για το λόγο αυτό , μπορεί να χρησιμοποιηθεί η κανονική μορφή (πίνακας 2×2).

Έστω $u \in M_n$. Με $\boxed{u_{ab}}$ συμβολίζουμε τον αβελιανισμό του u δηλ. την εικόνα του u ως προς τον επιμορφισμό $\alpha : M_n \longrightarrow M_n/[M_n, M_n]$. Σημειώνουμε ότι μπορούμε να προσδιορίσουμε το $M_n/[M_n, M_n]$ με το $F_n/[F_n, F_n]$. Στην ουσία το u_{ab} είναι ένα στοιχείο από την ομάδα παραγόντων της F_n, αλλά ωστόσο χρησιμοποιούμε επίσης τον ίδιο συμβολισμό u_{ab} για κάθε λέξη με γεννήτορες x_i (δηλ. ένα στοιχείο από το περιβάλλον της ελεύθερης ομάδας F_n) που αναπαριστά το u_{ab} όταν δεν είναι διφορούμενη.

Για $u, v \in M_n$, με $\boxed{u^v}$ συμβολίζουμε την έκφραση $v^{-1}uv$. Ή αλλοιώς λέμε ότι τα u και v είναι συζυγή. Αν $u \in [M_n, M_n]$ τότε μπορεί να επεκταθεί στο δακτύλιο $\mathbb{Z}(M_n/[M_n, M_n])$ τον οποίο θα συμβολίζουμε με $\mathbb{Z}A_n$. (Εδώ $A_n = M_n/[M_n, M_n]$ είναι ελεύθερη αβελιανή ομάδα τάξης n.)

Έστω $W \in \mathbb{Z}A_n$ της μορφής $\sum = a_i v_i$, όπου $a_i \in \mathbb{Z}$ και $v_i \in A_n$. Τότε με u^W συμβολίζουμε το γινόμενο $\prod (u^{a_i})^{v_i}$. Αυτό το γινόμενο είναι καλά ορισμένο αφού κάθε δύο στοιχεία του $[M_n, M_n]$ αντιμετατίθενται στο M_n.

Τώρα έστω $u \in M_n$. Τότε το u μπορεί να γραφεί στη παρακάτω ημικανονική μορφή:

$$u = u_{ab} \prod_{i<j} [x_i, x_j]^{W_{ij}} \qquad (5.3)$$

όπου $W_{ij} \in \mathbb{Z}A_n$. Για να φτάσουμε σε αυτήν την μορφή χρησιμοποιούμε 'τη διαδικασία συλλογής ' που βασίζεται στις παρακάτω ταυτότητες (θυμόμαστε ότι $[x, y] = x^{-1}y^{-1}xy$):

$$[y, x] = [x, y]^{-1},$$

$$xy = yx[x, y],$$

$$xy^{-1} = y^{-1}[y,x]^{y^{-1}x^{-1}}x,$$
$$x^{-1}y = y[y,x]^{y^{-1}x^{-1}}x^{-1},$$
$$[x,y]z = z[x,y]^z$$

Η διαδικασία συλλογής είναι απλή:

1. Χρησιμοποιώντας τις παραπάνω ιδιότητες, πηγαίνουμε από τα αριστερά προς τα δεξιά κατά μήκος της λέξης u συλλέγοντας όλες τις 'μη-μεταθετικές ' εμφανίσεις του x_1 στα αριστερά (που σημαίνει ότι δε νοιαζόμαστε για τις εμφανίσεις $[x_1, x_j]$ ή $[x_j, x_1]$ που δημιουργούνται κατά την πρόοδο της διαδικασίας). Επαναλαμβάνουμε με $x_2,\ x_3, ..$ Στο τέλος της διαδικασίας, η u θα έχει τη μορφή $u = u_{ab} \cdot c$, όπου $c \in [M_n, M_n]$ είναι το γινόμενο εκφράσεων της μορφής $[x_i, x_j]^g$, $g \in M_n$.

2. Αφού δύο οποιαδήποτε στοιχεία του $[M_n, M_n]$ μετατίθενται στο $[M_n]$ μπορεί κάποιος εύκολα να ανασυγκροτήσει τις εκφράσεις $[x_i, x_j]^g$ έτσι που η u να πάρει τη μορφή

$$u = u_{ab} \cdot \prod_{i<j} [x_i, x_j]^{W_{ij}},\ \text{όπου } W_{ij} \in \mathbb{Z}A_n.$$

Αυτή η διαδικασία παίρνει τετραγωνικό χρόνο όσον αφορά το μήκος του u.

Το να μετατρέψουμε την ημικανονική μορφή (5.3) σε λέξη είναι τετριμμένο καθότι η (5.3) είναι ήδη λέξη. Το μόνο πρόβλημα με τη (5.3) είναι ότι δεν είναι μοναδική αν $n > 2$ κι επομένως δε μπορεί να χρησιμοποιηθεί ως κοινό μυστικό κλειδί της Αλίκης και του Βασίλη.
(Για $n > 2$ χρησιμοποιούμε τη κανονική μορφή που είναι μοναδική, αποτελεσματικά υπολογίσιμη (σε τετραγωνικό χρόνο όσον αφορά το μήκος της u), αλλά όχι και τόσο εύκολα μετατρέψιμη πίσω στη λέξη).

2.6 ΟΜΑΔΕΣ *ARTIN*

.

Οι ομάδες $ARTIN$ μπορούν να χρησιμοποιηθούν ως πλατφόρμες στα κρυπτογραφικά πρωτόκολλα.

Εστω $G(\Gamma)$ μία ομάδα με αναπαράσταση

$$G(\Gamma) = \langle g_1, ..., g_n\ ,\ r(g_i, g_j) = 1\ (\text{για } 1 \le i, j \le n \text{ και } i \ne j)\rangle$$

όπου $n \ge 2$ και $r(g_i, g_j) = 1$ είναι μία σχέση ($relator$) με δύο γεννήτορες. Αν δίνεται η ομάδα $G(\Gamma)$ τότε υπάρχει ένα σχετικό γράφημα με ετικέτες και αντιστρόφως. Οι κόμβοι του γραφήματος Γ_G έχουν ως ετικέτες τους γεννήτορες της $G(\Gamma)$. Κάθε δύο κόμβοι $g_i, g_j \in \Gamma_G$ συνδέονται με ακμή αν υπάρχει μία σχέση $r(g_i, g_j) \in G(\Gamma)$ μεταξύ των αντίστοιχων γεννητόρων. Με άλλα λόγια, οι ακμές έχουν ως ετικέτες σχέσεις.

ΠΑΡΑΔΕΙΓΜΑ 1. Ομάδα $ARTIN$ $A(\Gamma)$ είναι μία ομάδα με αναπαράσταση

$$A(\Gamma) = \langle a_1, ..., a_n \ , \ \mu_{ij} = \mu_{ji} \text{ για } 1 \leq i < j \leq n \rangle,$$

όπου $\mu_{ij} = \underbrace{a_i a_j a_i ...}_{m_{ij}}$ και $m_{ij} = m_{ji}$.

Οι ομάδες $ARTIN$ είναι μία γενίκευση των ομάδων πλεξίδων ([3]). Για μία ομάδα $ARTIN$ $A(\Gamma)$, το σχετικό γράφημα Γ_A με ετικέτες δεν έχει πολλαπλές ακμές ή βρόχους. Οι κόμβοι a_i του Γ_A είναι οι γεννήτορες της ομάδας $ARTIN$. Κάθε δύο κόμβοι $a_i a_j \in \Gamma_A$ συνδέονται με ακμή, η οποία έχει ως ετικέτα τον ακέραιο m_{ij}, που αντιστοιχεί στη σχέση $\mu_{ij} = \mu_{ji}$ (μεταξύ των αντίστοιχων γεννητόρων $a_i a_j \in A(\Gamma)$. Γενικά, οι αυτομορφισμοί (ή ενδομορφισμοί) του γραφήματος Γ_G εισάγουν αυτομορφισμούς (ή ενδομορφισμούς) της ομάδας $G(\Gamma)$. Έτσι το γράφημα που σχετίζεται με την $G(\Gamma)$ μας δίνει έναν τρόπο να κατασκευάσουμε μία ημιομάδα ενδομορφισμών της $G(\Gamma)$ η οποία μπορεί να περιέχει μία μεγάλη *pool* αντιμεταθετικών στοιχείων.

ΠΑΡΑΔΕΙΓΜΑ 2. Οι σχέσεις της ομάδας πλεξίδων B_n χρησιμοποιούν δύο γεννήτορες. Το αντίστοιχο γράφημα της B_n είναι ένα απλό μονοπάτι και έχει μόνο έναν αυτομορφισμό, εκείνον της B_n : $\sigma_i \longmapsto \sigma_{n-i}$ και ο οποίος συμβαίνει να είναι ένας εσωτερικός αυτομορφισμός της B_n. Για τις άλλες ομάδες $G(\Gamma)$ τα αντίστοιχα γραφήματα είναι πιο περίπλοκα και είναι εύκολο να φτιάξουμε μία μεγάλη ημιομάδα (ή ημιομάδα) $T \subseteq End G(\Gamma)$ ενδομορφισμών (ή αυτομορφισμών).

Οι ομάδες $ARTIN$ $A(\Gamma)$ με την ιδιότητα $m_{ij} \geq 4$ καλούνται **ομάδες** $ARTIN$ **εξαιρετικά μεγάλου τύπου**. Ένα δέντρο Γ_A που αντιστοιχεί σε μία ομάδα $ARTIN$ εξαιρετικά μεγάλου τύπου, παρέχει μία άμεση διαδικασία κατασκευής ημιομάδας ενδομορφισμών της $A(\Gamma)$. Πιο αναλυτικά, οι ομάδες $ARTIN$ εξαιρετικά μεγάλου τύπου δουλεύουν αυτόματα, οπότε το πρόβλημα λέξης για ομάδες αυτής της κλάσης μπορούν να λυθεί σε τετραγωνικό χρόνο.

Κεφάλαιο 3

ΠΡΟΒΛΗΜΑΤΑ ΑΠΟΦΑΣΗΣ ΣΤΟ ΔΗΜΟΣΙΟ ΚΛΕΙΔΙ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

ΕΙΣΑΓΩΓΗ

Σε αυτό το κεφάλαιο, προτείνουμε τη χρήση προβλημάτων απόφασης από τη συνδυαστική θεωρία ομάδων ως πυρήνα πρωτοκόλλων δημοσίου κλειδιού ή ενός κρυπτοσυστήματος δημοσίου κλειδιού. Τα προβλήματα απόφασης είναι προβλήματα της ακόλουθης λογικής: Δίνεται μία ιδιότητα $\mathcal{P}$ και ένα αντικείμενο $\mathcal{O}$. Εξετάστε αν ναι ή όχι το αντικείμενο $\mathcal{O}$ έχει την ιδιότητα $\mathcal{P}$. Τα προβλήματα απόφασης μας επιτρέπουν να ανταποκριθούμε στην εξής πρόκληση του δημοσίου κλειδιού κρυπτογραφίας: σχεδιάστε ένα κρυπτογραφικό σύστημα που να είναι ασφαλές σε επιθέσεις «ωμής βίας» ($brute\ force$) αντιπάλων με αποτελεσματικά απεριόριστες υπολογιστικές ικανότητες. (Εάν κάποιος χρησιμοποιεί επίθεση «ωμής βίας» ($brute\ force$) απλά ελέγχει ένα προς ένα στοιχεία για να δει αν οι σχέσεις που έχει ικανοποιούνται αυτόματα).

.

3.1 ΤΟ ΣΧΗΜΑ $SHPILRAIN - ZAPATA$

.

►**Ορισμός.** **Πρόβλημα λέξης:**

Ένα ενδιαφέρον πρόβλημα απόφασης είναι το **πρόβλημα λέξης** το οποίο είναι: Δίνεται μία αναδρομική αναπαράσταση της ομάδας G και ένα στοιχείο $g \in G$. Εξετάστε αν ναι ή όχι $g = 1$ στη G.
Από την ίδια την περιγραφή του προβλήματος λέξης βλέπουμε ότι αποτελείται από δύο μέρη: τα «ναι» και «όχι», τα οποία καλούμε το «ναι» και «όχι» μέρος του προβλήματος λέξης, αντίστοιχα. Εάν μια ομάδα δίνεται από μια αναδρομική αναπαράσταση με γεννήτορες και σχέσεις ($relators$) τότε το «ναι» μέρος του προβλήματος λέξης έχει μια αναδρομική λύση διότι μπορεί κάποιος να απαριθμήσει αναδρομικά όλα τα αποτελέσματα καθορισμένων σχέσεων ($relators$), αντιστρόφων και συζυγών. Όμως, ο αριθμός παραγόντων που απαιτούνται για να αναπαραστήσουν μία λέξη μήκους n η οποία είναι ίση με 1 στο G, μπορεί να είναι πολύ μεγάλος σε σύγκριση με το n. Ιδιαιτέρως υπάρχουν ομάδες G με αποτελεσματικά επιλύσιμο το πρόβλημα της λέξης και λέξεις w μήκους n ίσες με 1 στο G, έτσι ώστε ο αριθμός των παραγόντων οποιασδήποτε παραγοντοποίησης της w σ′ ένα αποτέλεσμα των καθορισμένων σχέσεων ($relators$), αντιστρόφων και συζυγών τους, να μη φράσσεται από καμμία εκθετική δύναμη του n. Επιπλέον, εάν σε μια ομάδα G το πρόβλημα λέξης είναι αναδρομικά μη επιλύσιμο τότε το μήκος μιας απόδειξης που ελέγχει αν $w = 1$ στην G, δε φράσσεται από καμμία αναδρομική συνάρτηση του μήκους του w.

Επίσης σημειώνουμε ότι το «όχι» μέρος του προβλήματος λέξης σε πολλές ομάδες δεν είναι αναδρομικά επιλύσιμο και επομένως η επίθεση «ωμής βίας», εναντίον αυτού του μέρους δεν είναι αποτελεσματική. Πρέπει να επισημάνουμε ότι δεν υπάρχει αναδρομικά αναπαραστάσιμη ομάδα (ή ημιομάδα) που να έχει και τα δυο μέρη «ναι» και «όχι» του προβλήματος λέξης αναδρομικά μη επιλύσιμα.

Εδώ, θα περιγράψουμε ένα κρυπτογραφικό πρωτόκολλο που υιοθετεί την υπολογιστική δυσκολία του προβλήματος λέξης στις ομάδες. Σε αυτό το πρωτόκολλο, ο Βασίλης διαβιβάζει στην Αλίκη μια κρυπτογραφημένη δυαδική ακολουθία που η Αλίκη αποκρυπτογραφεί σωστά με πιθανότητα πάρα πολύ κοντά στο 1.

Σημειώνουμε ότι πολύ καιρό πριν, υπήρξε μια προσπάθεια να χρησιμοποιηθεί το πρόβλημα λέξης στο δημόσιο κλειδί κρυπτογραφίας αλλά δεν απέδωσε για πολλούς λόγους. Ένας από αυτούς τους λόγους, είναι το πρόβλημα επιλογής λέξης:

►**Ορισμός.** **Πρόβλημα επιλογής λέξης:**

Δίνονται $g,\ w_1,\ w_2 \in G$. Βρείτε αν $g = w_1$ ή $g = w_2$ στην G υπό τον όρο ότι μια από τις δύο ισότητες ισχύει.

Σε αυτό το πρόβλημα, και τα δύο μέρη είναι αναδρομικά επιλύσιμα για κάθε αναδρομικά αναπαραστάσιμη ομάδα βάση G αφού και τα δύο είναι στο «ναι» μέρος του προβλήματος λέξης και γι αυτό το πρόβλημα επιλογής λέξης δε μπορεί να χρησιμοποιηθεί στους σκοπούς μας.

3.1.1 ΤΟ ΠΡΩΤΟΚΟΛΛΟ

.

Παρουσιάζουμε το πρωτόκολλο.

Πρωτόκολλο (Ω)

1. Μία *pool* αναπαραστάσεων ομάδων με επιλύσιμο το πρόβλημα λέξης θεωρείται δημόσια (π.χ.μέρος του λογισμικού της Αλίκης).

2. Η Αλίκη επιλέγει τυχαία μία ειδική αναπαράσταση Γ από τη *pool*, τη διασκορπίζει με απεικόνιση που διατηρεί τους ισομορφισμούς για να πάρει μία διασκορπισμένη αναπαράσταση $\Gamma^{'}$, απορρίπτει μερικές από τις σχέσεις (*relators*) και δημοσιεύει τη σύντομη διασκορπισμένη αναπαράσταση $\hat{\Gamma}$.

3. Ο Βασίλης μεταδίδει την ιδιωτική του δυαδική ακολουθία στην Αλίκη, μεταδίδοντας ένα στοιχείο ίσο με 1 στη $\hat{\Gamma}$ (και έτσι επίσης στη $\Gamma^{'}$), στη θέση του '1' και ένα στοιχείο που δεν είναι ίσο με 1 στην $\Gamma^{'}$ στη θέση του '0'.

4. Η Αλίκη ανακτά τη δυαδική ακολουθία του Βασίλη πρώτα μετατρέποντας στοιχεία της $\Gamma^{'}$ στα αντίστοιχα στοιχεία της Γ και μετά λύνοντας το πρόβλημα λέξης στη Γ.

Το να βρει ο Βασίλης ένα στοιχείο που να μην είναι ίσο με το 1 στη $\Gamma^{'}$ φαίνεται να είναι δύσκολο αφού ο Βασίλης δεν γνωρίζει εξ ολοκλήρου την αναπαράσταση $\Gamma^{'}$. Το πρόβλημα αυτό λύνεται «πηγαίνοντας με το ρεύμα», τρόπος του λέγειν. Πιό συγκεκριμένα, αφήνουμε το Βασίλη να διαλέξει τυχαία μια λέξη αρκετά μεγάλου μήκους και δείχνουμε ότι, με συντριπτική πιθανότητα, ένα τέτοιο στοιχείο δεν είναι ίσο με 1 στην $\Gamma^{'}$.

Υπογραμμίζουμε ότι η κύρια καινοτομία αυτού του πρωτοκόλλου έναντι των υπαρχόντων είναι η αποθάρρυνση της αντιπάλου (Εύας) στο να επιτεθεί στο πρωτόκολλο κάνοντας μια εξαντλητική αναζήτηση του ιδιωτικού κλειδιού του αποστολέα, όπου ο προφανής (αν και συχνά «υπολογιστικά ανέφικτος») τρόπος είναι να επιτεθεί σε όλο το υπάρχον πρωτόκολλο του δημόσιου κλειδιού. Αν ο Βασίλης μεταδώσει ένα στοιχείο g που δεν είναι ίσο με το 1 στο $\hat{\Gamma}$ τότε η ανίχνευση του είναι πολύ δύσκολη για την Εύα. Στην πραγματικότητα, είναι γενικά αδύνατο.

►**Ορισμός.** **Επίθεση πηλίκου:** Η καλύτερη εκδοχή, αν η Εύα είναι

αρκετά τυχερή, είναι να βρει μία ομάδα παραγόντων της $\hat{\Gamma}$ όπου το πρόβλημα λέξης είναι επιλύσιμο και $g \neq 1$ σε αυτήν την ομάδα παραγόντων. Είναι αυτό που καλούμε **επίθεση πηλίκου**.

Τώρα ας ρίξουμε μία ματιά στην *επίθεση εξομοίωσης της κρυπτογράφησης (encryption emulation)* η οποία είναι:

Η Εύα παράγει κλειδιά ξανά και ξανά με διαφορετική κάθε φορά τυχαιότητα ώσπου να το πετύχει. Αυτό μπορεί να συμβεί τελικά με συντριπτική πιθανότητα. Η ακρίβεια του σχεδίου εγγυάται ότι το αντίστοιχο μυστικό κλειδί, όπως λαμβάνεται από την Εύα της επιτρέπει τη παράνομη αποκρυπτογράφηση.

.

3.1.2 *POOL* ΑΝΑΠΑΡΑΣΤΑΣΕΩΝ ΟΜΑΔΑΣ

.

Εδώ θα βασιστούμε στο γεγονός ότι αν η G ανήκει στη κλάση $C^{'}(\frac{1}{6})$ τότε ο αλγόριθμος *Dehn* λύνει το πρόβλημα της λέξης για την G. Αυτός ο αλγόριθμος έχει πολυπλοκότητα τετραγωνικού χρόνου ως προς το μήκος και της λέξης εισόδου w.

Σημειώνουμε ότι μία γενικά πεπερασμένα αναπαραστάσιμη ομάδα είναι μία ομάδα μικρών διαγραφών (*small cancellation group*). Η Αλίκη το μόνο που μπορεί να κάνει, είναι να επιλέξει μερικές τυχαίες λέξεις και να ελέγξει αν το αντίστοιχο συμμετρικό σύνολο ικανοποιεί τη συνθήκη για το $C^{'}(\frac{1}{6})$. Αν όχι, τότε επαναλαμβάνει.

Τώρα ξαναγράφουμε το πρωτόκολλο (Ω) με δείγματα παραμέτρων ώστε να φτιάξει η Αλίκη μία αναπαράσταση Γ.

1. Η Αλίκη σταθεροποιεί τον αριθμό k, $10 \leq k \leq 20$ των γεννητόρων στην αναπαράσταση της Γ. Έτσι η αναπαράσταση Γ της Αλίκης θα έχει $x_1, ..., x_k$ γεννήτορες.

2. Η Αλίκη επιλέγει m τυχαίες λέξεις $r_1, ..., r_m$ με γεννήτορες $x_1, ..., x_k$. Εδώ το $10 \leq m \leq 30$ και τα μήκη l_i των r_i είναι τυχαίοι ακέραιοι από το διάστημα $L_1 \leq l_i \leq L_2$. Έστω $L_1 = 12$ και $L_2 = 20$.

3. Αφού η Αλίκη πάρει τη σύντομη αναπαράσταση $\hat{\Gamma}$, προσθέτει τη σχέση

$$x_i^{'} = \prod_{j=1}^{M} [x_i^{'}, w_j]$$

σε αυτήν , όπου $x_i^{'}$ είναι ένας (τυχαία επιλεγμένος) γεννήτορας από το $\hat{\Gamma}$, w_j είναι τυχαία στοιχεία μήκους 1 ή 2 με γεννήτορες $x_1^{'}, x_2^{'}, ...,$ και M=10. (Η μεταθετική μας σχέση είναι $[a, b] = a^{-1}b^{-1}ab$). Αυτή η σχέση

χρειάζεται για να αποτρέψει τις επιθέσεις πηλίκου. Μετά η Αλίκη βρίσκει την προεικόνα αυτής της σχέσης ως προς τον ισομορφισμό μεταξύ των Γ και $\hat{\Gamma}$ και προσθέτει αυτήν την προεικόνα στις καθορισμένες σχέσεις ($relators$) του Γ. Έτσι, η Γ τελικά έχει k γεννήτορες και $m+1$ καθορισμένες σχέσεις ($relators$).

4. Τέλος, η Αλίκη ελέγχει αν η ιδιωτική της αναπαράσταση Γ ικανοποιεί την συνθήκη μικρών διαγραφών $C^{'}(\frac{1}{6})$. Αν όχι τότε ξαναρχίζει.

.

3.1.3 ΙΣΟΜΟΡΦΙΚΗ ΕΠΙΘΕΣΗ

.

Εδώ θα συζητήσουμε για την πιθανή επίθεση «ωμής βίας» στο πρωτόκολλο (Ω).

Ξέροντας την *pool* των ομάδων αναπαραστάσεων από την οποία η Αλίκη επιλέγει την δική της αναπαράσταση Γ, η Εύα θα προσπαθήσει να αυξήσει τη δημόσια αναπαράσταση $\hat{\Gamma}$ σε μία αναπαράσταση που θα είναι ισομορφική με μια από την *pool*. Θεωρητικά, αυτό είναι δυνατό και διότι η *pool* είναι αναδρομική και διότι το σύνολο των πεπερασμένων αναπαραστάσεων που είναι ισομορφικό με ένα δεδομένο είναι επίσης αναδρομικό. Εντούτοις, αυτή η διαδικασία απαιτεί τεράστιους πόρους. Ας ρίξουμε μια προσεκτικότερη ματιά σ΄ αυτό.

Η Εύα μπορεί να προσθέσει ένα στοιχείο κάθε φορά και να ελέγχει αν η αναπαράσταση που προκύπτει, ας την καλέσουμε $\hat{\Gamma}_+$, είναι ισόμορφη με μία από τις αναπαραστάσεις από την *pool* της Αλίκης. Πιο αναλυτικά. Η Εύα θέλει να ελέγξει αν η $\hat{\Gamma}_+$ είναι ισόμορφη με κάποια Γ_i. Ψάχνει όλες τις απεικονίσεις από το Γ_i στο $\hat{\Gamma}_+$, μία κάθε φορά, ορίζοντας τους γεννήτορες της Γ_i. Ταυτοχρόνως ψάχνει όλες τις απεικονίσεις από το $\hat{\Gamma}_+$ στο Γ_i μία κάθε φορά, ορίζοντας τους γεννήτορες της $\hat{\Gamma}_+$. Συνθέτει διάφορα ζευγάρια αυτών των απεικονίσεων και ελέγχει:
(1) αν παίρνει ίδια απεικόνιση με την Γ_i.
(2) αν και οι δύο απεικονίσεις του ζευγαριού είναι ομομορφικές, δηλ. αν στέλνουν τις σχέσεις ($relators$) κάθε αναπαράστασης σε στοιχεία ίσα με 1 της άλλης αναπαράστασης. Έχοντας επιλύσιμο το πρόβλημα λέξης στην Γ_i κάνει τον έλεγχο πιο αποδοτικό αλλά στην πραγματικότητα δεν είναι απαραίτητο διότι εδώ συμβαίνει το 'ναι' μέρος του προβλήματος λέξης το οποίο είναι πάντα αναδρομικό.

Τώρα ας εστιάσουμε στο μέρος της διαδικασίας, όπου η Εύα δουλεύει μια ιδιαίτερη αναπαράσταση Γ_i από την *pool* της Αλίκης. Υποθετουμε ότι η Γ_i δεν είναι ισομορφική με την $\hat{\Gamma}_+$. Αφού το 'όχι' μέρος του ισομορφικού προβλήματος μεταξύ των $\hat{\Gamma}_+$ και Γ_i δεν είναι αναδρομικό, η Εύα θα προσπαθήσει να δοκιμάσει διάφορα ζευγάρια απεικονίσεων μεταξύ των $\hat{\Gamma}_+$ και Γ_i επ΄ αορίστου. Έτσι, θα πρέπει να διαθέσει (κατά αόριστο τρόπο) μερικούς πόρους μνήμης στον έλεγχο αυτής της ιδιαίτερης Γ_i. Αφού ο αριθμός Γ_i αυξάνεται εκθετικά ως προς το μέγεθος της αναπαράστασης (το οποίο είναι το συνολικό μήκος των σχέσεων ($relators$)), η Εύα θα απαιτήσει απεριόριστο χώρο αποθήκευσης και, στην πραγματικότητα, θα φθάσει στα φυσικά όρια (π.χ. στον αριθμό ηλεκτρονίων στον κόσμο) του αποθηκευτικού χώρου πολύ γρήγορα επειδή,

για παράδειγμα, ο αριθμός αναπαραστάσεων έξι γεννητόρων με το συνολικό μήκος των σχέσεων ($relators$) να φράσσεται από το 100 είναι ήδη παραπάνω από 10^{100}.

Ίσως υπάρχουν εξυπνότεροι τρόποι να βρούμε μία αναπαράσταση μικρών διαγραφών ισόμορφη με την $\hat{\Gamma}_+$, αλλά αυτός ο έλεγχος (τουλάχιστον, στη χειρότερη περίπτωση) θα απαιτούσε εξαιρετικά απεριόριστους υπολογιστικούς πόρους.

3.1.4 ΕΠΙΘΕΣΗ ΠΗΛΙΚΟΥ

.

Εδώ θα συζητήσουμε μία επίθεση η οποία, γενικά, είναι πιο αποτελεσματική (ιδιαίτερα στην παραγματική ζωή) από την επίθεση «ωμής βίας» που αναφέραμε πιο πάνω.

Σημειώνουμε ότι στον καθορισμό μιας αβελιανής ομάδας, είναι αρκετό να απαιτήσουμε ότι $[x_i, x_j] = 1$ για όλους τους γεννήτορες x_i, x_j της ομάδας G. Έτσι κάθε πεπερασμένα παραγόμενη αβελιανή ομάδα είναι πεπερασμένα αναπαραστάσιμη. Το ίδιο ισχύει για όλες τις πεπερασμένα παραγόμενες μηδενοδυνάμειες ομάδες οποιασδήποτε τάξης $c \geq 1$, αλλά όχι για όλες τις μεταβελιανές ομάδες. Πιο συγκεκριμμένα, είναι γνωστό ότι οι πεπερασμένα παραγόμενες ελεύθερες μεταβελιανές ομάδες είναι απείρως αναπαραστάσιμες.

Τώρα θα αναφερθούμε στις επιθέσεις πηλίκου. Ένας τρόπος για την Εύα είναι να προσπαθήσει να προσδιορίσει, εκείνες τις θέσεις στη δυαδική ακολουθία του Βασίλη όπου σκόπευε να μεταδώσει 0, με τη δοκιμή του πηλίκου. Αυτό σημαίνει τα εξής: Η Εύα προσπαθεί να προσθέσει πεπερασμένα ή άπειρα πολλές σχέσεις ($relators$) στη δεδομένη αναπαράσταση $\hat{\Gamma}$, ώστε να λάβει μία αναπαράσταση που ορίζει μία ομάδα H με επιλύσιμο το πρόβλημα λέξης.

Έχει σημασία για την Εύα να δοκιμάσει μόνο αναγνωρίσιμα πηλίκα, όπως των αβελιανών, ή πιο γενικά, των μηδενοδυνάμεων ομάδων. Αυτό ισοδυναμεί με το να προσθέσει συγκεκριμένες σχέσεις ($relators$) στην $\hat{\Gamma}$. Για παράδειγμα, για ένα αβελιανό πηλίκο, η Εύα μπορεί να προσθέσει τις σχέσεις ($relators$) $[x_i^{'}, x_j^{'}]$ για όλα τα ζευγάρια γεννητόρων $x_i^{'}, x_j^{'}$ της $\hat{\Gamma}$. Για τα μηδενοδύναμα πηλίκα η Εύα πρέπει να προσθέσει στους γεννήτορες μεταθέτες μεγαλύτερου βάρους. Για ένα μεταβελιανό πηλίκο, η Εύα πρέπει να προσθέσει απείρως πολλές σχέσεις ($relators$) (διότι όπως έχουμε ήδη αναφέρει, οι ελεύθερες μεταβελιανές ομάδες είναι απείρως αναπαραστάσιμες), αλλά αυτό δεν αποτελεί πρόβλημα αφού δεν ειναι απαραίτητο «να προσθέσει πραγματικά» αυτές τις σχέσεις ($relators$)· μπορεί απλά να θεωρήσει τη $\hat{\Gamma}$ σαν μία αναπαράσταση στην ποικιλία των μεταβελιανών ομάδων και να εφαρμόσει το σχετικό αλγόριθμο για το πρόβλημα λέξης το οποίο είναι καθολικό για όλες τις πεπερασμένα αναπαραστάσιμες ομάδες στην ποικιλία των μεταβελιανών ομάδων.

Τελικά φαίνεται ότι μια επίθεση πηλίκου μπορεί ουσιαστικά να υιοθετήσει είτε ένα μηδενοδύναμο είτε ένα μεταβελιανό πηλίκο στην $\hat{\Gamma}$. Κι αυτός είναι ο λόγος που για να αποτρέψει τέτοιες επιθέσεις, η Αλίκη προσθέτει τη σχέση:

$$x_i^{'} = \prod_{j=1}^{M} [x_i^{'}, w_j]$$

στη $\hat{\Gamma}$.

Μέρος III

ΕΠΙΛΟΓΟΣ

.

Η Κρυπτογραφία έχει συμβάλλει στην εξέλιξη πολλών κλάδων της επιστήμης όπως των Μαθηματικών, Πληροφορικής, Αστροφυσικής.

Σήμερα βρισκόμαστε στην εποχή της ρομποτικής. Η μεταβίβαση μηνυμάτων πλανητικά και εξωπλανητικά επιβάλλει την άμεση και ασφαλή μεταφορά μηνυμάτων και πληροφοριών.

Η Εύα δουλεύει συνεχώς πυρετωδώς στο σπάσιμο κωδικών και διαρροή πληροφοριών. Είναι κοινό μυστικό ότι πολλά κράτη εκπαιδεύουν τέτοιες '' ισχυρές '', Εύες.

Τα υπολογιστικά συστήματα συνεχώς αυξάνουν τις δυνατότητες τους. Η ασφαλής μεταβίβαση μηνυμάτων συνεχώς κινδυνεύει. Τα πρωτόκολλα πρέπει συνεχώς να βρίσκονται ένα βήμα πιο μπροστά από κάθε προοδευτικό στόχο του αντιπάλου.

Η μη μεταθετική-Κρυπτογραφία έχει προσφέρει πολλά μέχρι στιγμής αλλά ο τομέας είναι ακόμα ανοιχτός, αφού έχει να δώσει πολλά ακόμα στον σύγχρονο άνθρωπο, του οποίου οι απαιτήσεις αυξάνουν όλο και πιο πολύ, αφού ο γρήγορος ρυθμός που του έχει επιβάλλει η εξέλιξη της τεχνολογίας πολλές φορές τον αφήνει ακάλυπτο σε πολλές πτυχές της καθημερινότητας του.

Βιβλιογραφία

[1] *I. Anshel, M.Anshel, and D. Goldfeld,*
An algebraic method for public − key cryptography, Math. Res. Lett. 6 (1999), *pp.* 287 − 291.

[2] *I. Anshel, M.Anshel, D. Goldfeld, and S. Lemieux,*
Key Agreement, The Algebraic EraserTM, and Lightweight Cryptography. Algebraic Methods in Cryptography, Contemporary Mathematics 418, *pp.* 1 − 34.*American Mathematical Society,* 2006.

[3] *K. Appel and P. Schupp, Artin groups and infinite Coxeter groups,*
Invent.Math. 72 (1983), *pp.* 201 − 220.

[4] *G. Arzhantseva and A. Olshanskii, Genericity of the class of groups in whichsubgroups with a lesser number of generators are free, (Russian) Mat. Zametki* 59 (1996), *pp.* 489 − 496.