Εθνικο Καποδιστριακο Πανεπιστημιο Αθηνων

τμημα μαθηματικων

Διπλωματικη εργασια ειδικευσης
στα θεωρητικα μαθηματικα

Κρυπτογραφία επί μη Αβελιανών Ομάδων

χρυσοστομος ζαμπετακης

Επιβλέπων:

δημητριος βαρσος

2013

στη μνήμη του
Αλέξανδρου Φερρίδη

In mathematics you don't understand things.
You just get used to them.

—*Johann Von Neumann*

Περιεχόμενα

Πρόλογος

Η ανάπτυξη της επιστήμης των μαθηματικών αποτελεί μία από τις σημαντικότερες πνευματικές δραστηριότητες του ανθρώπου, για περισσότερα από 2.500 χρόνια. Η ανάγκη για την επινόηση μεθόδων που θα έβρισκαν άμεση εφαρμογή σε καθημερινές πρακτικές, αποτέλεσε ουσιαστικό κίνητρο για την έρευνα και τη θεμελίωση της μαθηματικής γνώσης. Μεταξύ άλλων, παρουσιάστηκε η ανάγκη για ασφαλείς επικοινωνίες μέσω ανοικτών διαύλων, που οδήγησε σε προσπάθειες για τη διασφάλιση του περιεχομένου των διακινούμενων μηνυμάτων. Η μελέτη και η ανάπτυξη των σχετικών μεθόδων αποτελούν σκοπούς του κλάδου που σήμερα καλείται Κρυπτογραφία.

Η Κρυπτογραφία, εν γένει, αφορά την κατασκευή και ανάλυση πρωτοκόλλων που σχετίζονται με θέματα ασφάλειας των πληροφοριών, όπως η εμπιστευτικότητα, η ακεραιότητα των δεδομένων, η πιστοποίηση οντοτήτων και η επικύρωση προέλευσης των δεδομένων. Στις πρώιμες μεθόδους κρυπτογράφησης, καθώς και στις τρέχουσες, εξέχοντα ρόλο διαδραματίζουν πρωτόκολλα που στηρίζονται σε στοιχειώδη αποτελέσματα της Θεωρίας Αριθμών. Η ανάπτυξη της επιστήμης των υπολογιστών προσέφερε νέα προοπτική και είχε καταλυτικές συνέπειες στην εξέλιξη της Κρυπτογραφίας.

Οι εφαρμογές της Κρυπτογραφίας περιλαμβάνουν πλέον σημαντικούς τομείς της ανθρώπινης δραστηριότητας, όπως οι συναλλαγές με ATM, οι κωδικοί ηλεκτρονικών λογαριασμών (passwords), το ηλεκτρονικό εμπόριο κ.α. Γίνεται σαφές ότι μία παραβίαση των πρωτοκόλλων που χρησιμοποιούνται στις μέρες μας θα είχε ανυπολόγιστες συνέπειες ως προς την ασφάλεια των πληροφοριών. Η ανάπτυξη των κβαντικών υπολογιστών καθιστά επιτακτική την επανεξέταση των ισχυόντων κρυπτογραφικών πρωτοκόλλων, με το ενδιαφέρον να στρέφεται προς τη χρήση μη-Αβελιανών ομάδων, οι οποίες παρέχουν τα απαραίτητα εχέγγυα για την υλοποίηση ασφαλέστερων πρωτοκόλλων.

Στην παρούσα εργασία παρουσιάζονται εφαρμογές της Κρυπτογραφίας που σχετίζονται με τη Θεωρία Ομάδων και ειδικότερα με την υλοποίηση σε μοντέλα μη-Αβελιανών ομάδων. Η έμφαση δίδεται στις μαθηματικές έννοιες και τη θεωρία που υπεισέρχεται στις αντίστοιχες κρυπτογραφικές μεθόδους. Ως εκ τούτου, η αναφορά σε έννοιες που άπτονται της επιστήμης των υπολογιστών έχει απλώς το χαρακτήρα μνείας.

Ευχαριστώ θερμά τον επιβλέποντα Καθηγητή κ.Δημήτριο Βάρσο για τα κίνητρα και τη διαρκή υποστήριξη που μου παρείχε, κατά τη συγγραφή της παρούσας εργασίας.

Κεφάλαιο 1

Βασικές έννοιες

1.1 Σύνολο γεννητόρων ομάδας

Ορισμός 1.1.1. Έστω G ομάδα και $S \subseteq G$. Ορίζουμε ως $\langle S \rangle$ την υποομάδα της G που παράγεται από το σύνολο S. Η υποομάδα $\langle S \rangle$, ως τομή των υποομάδων της G που περιέχουν το σύνολο S, είναι η μικρότερη υποομάδα της G που περιέχει κάθε στοιχείο του S.

$$\langle S \rangle = \bigcap \{H : H \leqslant G \text{ και } S \subseteq H\}$$

Αποδεικνύεται ότι η $\langle S \rangle$ είναι η υποομάδα των στοιχείων της G τα οποία εκφράζονται ως πεπερασμένα γινόμενα στοιχείων και αντιστρόφων στοιχείων του συνόλου S.

$$\langle S \rangle = \{s_{i_1}^{\varepsilon_1} \dots s_{i_n}^{\varepsilon_n} : \ s_{i_j} \in S, \ \varepsilon_j \in \{-1, 1\}, \ j = 1, \dots, n, \ n \in \mathbb{N}\}$$

Αν $G = \langle S \rangle$ τότε λέμε ότι η ομάδα G *παράγεται* από το σύνολο S και τα στοιχεία του S λέγονται *γεννήτορες* της G.

Παράδειγμα 1.1.2. *Αν $S = \{x\}$ τότε $\langle S \rangle = \langle x \rangle$, δηλαδή η υποομάδα που παράγεται από το μονοσύνολο S είναι η κυκλική ομάδα με γεννήτορα το στοιχείο $x \in S$.*

Ορισμός 1.1.3. Έστω G ομάδα και S πεπερασμένο υποσύνολο της G τέτοιο ώστε $G = \langle S \rangle$. Τότε η ομάδα G λέγεται *πεπερασμένα παραγόμενη*.

1.2 Ελεύθερες Ομάδες

Έστω G ομάδα παραγόμενη από ένα σύνολο S. Τότε κάθε στοιχείο της G εκφράζεται ως γινόμενο στοιχείων και αντιστρόφων στοιχείων του S. Η γραφή αυτή δεν είναι μοναδική.

Παράδειγμα 1.2.1. $1 = ss^{-1} = s^{-1}s$ *για κάθε* $s \in S$.

Παράδειγμα 1.2.2. *Σε μία Αβελιανή ομάδα έχουμε ότι* $g = ab = ba$.

Κατ' επέκταση, πάντοτε υπάρχουν σχέσεις μεταξύ των στοιχείων του S στην ομάδα G. Οι σχέσεις αυτές μπορούν να θεωρηθούν ως ισότητες μεταξύ γινομένων στοιχείων και αντιστρόφων στοιχείων του S.

Τα γινόμενα στοιχείων και αντιστρόφων στοιχείων του S μπορούν να αναχθούν, διαγράφοντας όσα γινόμενα της μορφής ss^{-1} ή $s^{-1}s$ εμφανίζονται στην παράσταση του γινομένου.

Αναγωγή: Έστω S σύνολο. Θέτουμε S^{-1} ένα σύνολο ισοπληθικό και ξένο με το S και μία $1-1$ απεικόνιση $s \mapsto s^{-1}$ του συνόλου S επί του συνόλου S^{-1}. Ορίζεται τότε και η αντίστροφη απεικόνιση από το σύνολο S^{-1} στο S έτσι ώστε $(s^{-1})^{-1} = s$ για κάθε $s \in S$ και επομένως $(t^{-1})^{-1} = t$ για κάθε $t \in T = S \cup S^{-1}$.

Σημειώνουμε ότι η έκφραση s^{-1} είναι απλώς ένας *συμβολισμός* για το αντίστροφο του στοιχείου $s \in S$.

Ορισμός 1.2.3. Μία *λέξη* w στο αλφάβητο T είναι μία πεπερασμένη, πιθανώς κενή, ακολουθία στοιχείων του T.

$$w = (s_1, \ldots, s_n),\ s_i \in T,\ 1 \leq i \leq n$$

Ο αριθμός n καλείται *μήκος* της λέξης w και συμβολίζεται με $|w|$. Η κενή λέξη συμβολίζεται με ϵ και θέτουμε $|\epsilon| = 0$.

Ορισμός 1.2.4. Μία λέξη $a = (a_1, \ldots, a_n), a_i \in T, 1 \leq i \leq n$ λέγεται *ανηγμένη* αν $a_{i+1} \neq a_i^{-1}$ για κάθε i με $1 \leq i < n$. Το μήκος της ανηγμένης λέξης a καλείται *ανηγμένο μήκος*.

Παράδειγμα 1.2.5. *Η κενή λέξη καθώς και οι μονογράμματες λέξεις είναι ανηγμένες, ελλείψει διαδοχικών γραμμάτων στην παράστασή τους.*

Παράδειγμα 1.2.6. *Αν $S = \{x, y, z, \dots\}$ τότε οι λέξεις (x, y, z) και (x, x, x) είναι ανηγμένες ενώ η λέξη (x, y, y^{-1}, z) δεν είναι ανηγμένη.*

Το σύνολο W των λέξεων, εφοδιασμένο με την πράξη της συνένωσης των λέξεων, αποτελεί το ελεύθερο μονοειδές επί του S. Παρατηρούμε ότι, αν δεν υπεισέλθει η έννοια της αναγωγής, το W με την πράξη της συνένωσης των λέξεων δεν αποτελεί ομάδα, καθώς είναι αδύνατο να προκύψει η κενή λέξη ως αποτέλεσμα συνένωσης δύο λέξεων και επομένως μία μη κενή λέξη στο W δεν έχει αντίστροφο.

Η διαδικασία της αναγωγής έγκειται στη διαγραφή υπακολουθιών της μορφής (a_i, a_i^{-1}) έως την επίτευξη ανηγμένης μορφής της λέξης.

Ορισμός 1.2.7. Στο W συμβολίζουμε με $a \xrightarrow{1} b$ την αναγωγή μίας λέξης $a = (a_1, \dots, a_n)$ με $a_{i+1} = a_i^{-1}$ σε μία λέξη $b = (a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n)$ για κάποιο i με $1 \leq i < n$. Επίσης συμβολίζουμε με $a \xrightarrow{k} b$ για $k \geq 0$ αν $a \xrightarrow{1} a' \xrightarrow{1} a'' \to \dots \xrightarrow{1} a^{(k)} = b$ για λέξεις $a', a'', \dots, a^{(k)} \in W$. Τέλος, συμβολίζουμε με $a \to b$ την αναγωγή της λέξης a στη λέξη b αν υπάρχει $k \geq 0$ τέτοιο ώστε $a \xrightarrow{k} b$.

Προφανώς, αν η λέξη a είναι ανηγμένη τότε $a \xrightarrow{k} b \Rightarrow k = 0$ αφού δεν υπάρχει λέξη c τέτοια ώστε $a \xrightarrow{1} c$ και $a \to b \Rightarrow a = b$.

Λήμμα 1.2.8. Έστω $a \in W$ μία λέξη. Τότε υπάρχει αναγωγή $a \to b$ της λέξης a σε μία ανηγμένη λέξη b.

Απόδειξη. Με επαγωγή στο μήκος της λέξης a. Αν η a είναι ανηγμένη τότε θέτουμε $b = a$. Διαφορετικά, υπάρχει λέξη $c \in W$ τέτοια ώστε $a \xrightarrow{1} c$ και $c \to b$ όπου b ανηγμένη λέξη στο W, αφού η c έχει μικρότερο μήκος από την a και άρα $a \to b$. □

Θα δείξουμε ότι η λέξη b του Λήμματος 1.2.8 είναι μοναδική.

Λήμμα 1.2.9. Αν $a \xrightarrow{1} b$ και $a \xrightarrow{1} c \neq b$ τότε υπάρχει λέξη $d \in W$ τέτοια ώστε $b \xrightarrow{1} d$ και $c \xrightarrow{1} d$.

Απόδειξη. Έστω $a = (a_1, \ldots, a_n)$. Τότε υπάρχει i με $1 \leq i < n$ τέτοιο ώστε $a_{i+1} = a_i^{-1}$ και $b = (a_1, \ldots, a_{i-1}, a_{i+2}, \ldots, a_n)$. Επίσης υπάρχει j με $1 \leq j < n$ τέτοιο ώστε $a_{j+1} = a_j^{-1}$ και $c = (a_1, \ldots, a_{j-1}, a_{j+2}, \ldots, a_n)$. Εφόσον $b \neq c$ έπεται ότι $i \neq j$ και μπορούμε να υποθέσουμε ότι $i < j$. Αν $j = i + 1$ τότε $a_i = a_{i+1}^{-1} = a_{j+1} = a_{i+2}$ και $(a_{i-1}, a_{i+2}, a_{i+3}) = (a_{j-2}, a_{j-1}, a_{j+2})$ και άρα $b = c$, άτοπο. Επομένως $j \geq i + 2$. Τότε τα a_i, a_{i+1} είναι διαδοχικά γράμματα της λέξης c ενώ τα a_j, a_{j+1} είναι διαδοχικά γράμματα της λέξης b και μπορούμε να θέσουμε $d = (a_1, \ldots, a_{i-1}, a_{i+2}, \ldots, a_{j-1}, a_{j+2}, \ldots, a_n)$ (ή $d = (a_1, \ldots, a_{i-1}, a_{j+2}, \ldots, a_n)$ αν $j = i + 2$) και έχουμε τη ζητούμενη λέξη. □

Λήμμα 1.2.10. Έστω $a \to b$ και $a \to c$. Τότε υπάρχει λέξη d τέτοια ώστε $b \to d$ και $c \to d$.

Απόδειξη. Υποθέτουμε ότι $a \xrightarrow{k} b$ και $a \xrightarrow{l} c$. Το ζητούμενο είναι τετριμμένο αν $k = 0$ ή $l = 0$. Έστω $l = 1$. Θα δείξουμε το ζητούμενο με επαγωγή στο k. Έχουμε ότι $a \xrightarrow{1} c$. Αν $k \leq 1$ τότε από το Λήμμα 1.2.9 το ζητούμενο ισχύει. Υποθέτουμε ότι $k > 1$ δηλαδή υπάρχει λέξη u τέτοια ώστε $a \xrightarrow{1} u \xrightarrow{k-1} b$. Αν $u = c$ τότε θέτουμε $d = b$ και έχουμε τη ζητούμενη λέξη. Διαφορετικά, υπάρχει λέξη v τέτοια ώστε $u \xrightarrow{1} v$ και $c \xrightarrow{1} v$. Από το Λήμμα 1.2.9 έχουμε:

$$\begin{array}{ccccc} a & \xrightarrow{1} & u & \longrightarrow & b \\ \downarrow & & \downarrow & & \downarrow \\ c & \xrightarrow{1} & v & \longrightarrow & d \end{array}$$

Από την επαγωγική υπόθεση και τις αναγωγές $u \xrightarrow{k-1} b$ και $u \xrightarrow{1} v$ συνεπάγεται ότι υπάρχει λέξη d τέτοια ώστε $b \to d$ και $c \xrightarrow{1} v \to d$. Επομένως το Λήμμα ισχύει για $l \leq 1$. Η γενική περίπτωση αποδεικνύεται με επαγωγή στο l.

$$\begin{array}{ccccc} a & \xrightarrow{1} & u & \longrightarrow & c \\ \downarrow & & \downarrow & & \downarrow \\ b & \longrightarrow & v & \longrightarrow & d \end{array}$$

Αν $l > 1$ τότε $a \to b$ και υπάρχει λέξη u τέτοια ώστε $a \xrightarrow{1} u \xrightarrow{l-1} c$. Από την περίπτωση $l = 1$ έχουμε ότι υπάρχει λέξη v τέτοια ώστε $b \to v$ και $u \to v$. Από την επαγωγική υπόθεση και τις αναγωγές $u \to v$ και $u \xrightarrow{l-1} c$ έχουμε τελικά ότι υπάρχει λέξη d τέτοια ώστε $b \to v \to d$ και $c \to d$. □

Λήμμα 1.2.11. Έστω $a \in W$ μία λέξη. Τότε υπάρχει μοναδική ανηγμένη λέξη b τέτοια ώστε $a \to b$.

Απόδειξη. Αν $a \to b$ και $a \to c$ όπου b, c ανηγμένες λέξεις τότε από το Λήμμα 1.2.10 έπεται ότι υπάρχει λέξη d τέτοια ώστε $b \to d$ και $c \to d$ και επομένως $b = d = c$. □

Ορισμός 1.2.12. Η αναγωγή red$a$ της λέξης $a \in W$ είναι η μοναδικά ορισμένη ανηγμένη λέξη b τέτοια ώστε $a \to b$.

Πρόταση 1.2.13. Το σύνολο F_S των ανηγμένων λέξεων επί του S είναι ομάδα με πράξη την $\cdot : a \cdot b = \mathrm{red}(ab)$

Απόδειξη. Έστω $a \xrightarrow{1} b$. Τότε $ac \xrightarrow{1} bc$ και $ca \xrightarrow{1} cb$ για κάθε λέξη $c \in W$. Επομένως αν $a \to b$ έπεται ότι $ac \to bc$ και $ca \to cb$ για κάθε λέξη $c \in W$. Αν οι λέξεις $a, b, c \in W$ είναι ανηγμένες τότε έχουμε ότι $ab \to a \cdot b$ και $bc \to b \cdot c$ και επομένως $abc \to (a \cdot b)c \to (a \cdot b) \cdot c$ και $abc \to a(b \cdot c) \to a \cdot (b \cdot c)$. Άρα έχουμε ότι $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, δηλαδή η πράξη $\cdot$ είναι προσεταιριστική. Η κενή λέξη $\epsilon = (\ )$ είναι ανηγμένη και αποτελεί το μοναδιαίο στοιχείο της F_S αφού αν $a \in W$ ανηγμένη λέξη τότε $\epsilon \cdot a = \mathrm{red}\ (\epsilon a) = \mathrm{red}a = a$ και $a \cdot \epsilon = \mathrm{red}(a\epsilon) = \mathrm{red}a = a$. Η αντίστροφη της ανηγμένης λέξης $a = (a_1, \ldots, a_n)$ είναι η $a^{-1} = (a_n^{-1}, \ldots, a_1^{-1})$. Πράγματι, η a^{-1} είναι ανηγμένη διότι $a_i^{-1} \neq (a_{i-1}^{-1})^{-1}$ για κάθε $i > 1$ και $aa^{-1} \to \epsilon$, $a^{-1}a \to \epsilon$. Επομένως η F_S είναι ομάδα με πράξη την $\cdot$. □

Ειδικότερα, η αντίστροφη της μονογράμματης λέξης (y) είναι η (y^{-1}).

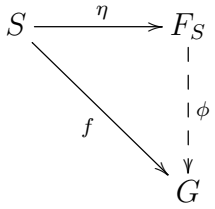
Ορισμός 1.2.14. Η ομάδα F_S, που αποτελείται από τις ανηγμένες λέξεις επί του S, καλείται η *ελεύθερη ομάδα* επί του S.

Ιδιότητες: Η ελεύθερη ομάδα επί του S παράγεται από το σύνολο S. Το σύνολο S, κατά τρόπο αυστηρό, δεν είναι υποσύνολο της F_S. Όμως υπάρχει κανονική εμφύτευση $\eta : S \to F_S, s \mapsto (s)$ που επεκτείνεται στο $T = S \cup S^{-1}$ έτσι ώστε $\eta : s^{-1} \mapsto (s^{-1})$. Τότε η ομάδα F_S παράγεται από την εικόνα $\eta(S)$.

Πρόταση 1.2.15. Έστω $a = (a_1, \ldots, a_n)$ ανηγμένη λέξη στο S. Τότε $a = \eta(a_1) \ldots \eta(a_n)$. Ειδικότερα, η F_S παράγεται από την εικόνα $\eta(S)$.

Απόδειξη. Εφόσον η λέξη $a = (a_1, \ldots, a_n)$ είναι ανηγμένη τότε από τη συνένωση των μονογράμματων λέξεων $(a_1), \ldots, (a_n)$ προκύπτει ανηγμένη λέξη. Άρα $a = (a_1) \ldots (a_n) = \eta(a_1) \ldots \eta(a_n)$. Αφού $\eta(s^{-1}) = \eta(s)^{-1}$ για κάθε $s \in S$ έχουμε ότι κάθε λέξη $a \in F_S$ είναι γινόμενο στοιχείων και αντιστρόφων στοιχείων της εικόνας $\eta(S)$. □

Θεώρημα 1.2.16. Έστω $\eta : S \to F_S$ η κανονική εμφύτευση. Τότε για κάθε απεικόνιση f του συνόλου S σε μία ομάδα G υπάρχει μοναδικός ομομορφισμός $\phi : F_S \to G$ τέτοιος ώστε $f = \phi \circ \eta$. Με άλλα λόγια, το παρακάτω διάγραμμα είναι μεταθετικό:



Απόδειξη. Πρώτα δείχνουμε τη μοναδικότητα. Έστω $\phi : F_S \to G$ ομομορφισμός τέτοιος ώστε $f = \phi \circ \eta$. Επεκτείνουμε την f στο S^{-1} έτσι ώστε $f(s^{-1}) = f(s)^{-1}$ για κάθε $s \in S$ και έχουμε ότι $\phi(\eta(s)) = f(s)$ και $\phi(\eta(s^{-1})) = \phi(\eta(s)^{-1}) = f(s)^{-1} = f(s^{-1})$. Αν $a = (a_1, \ldots, a_n)$ ανηγμένη λέξη τότε $\phi(a) = \phi(\eta(a_1) \ldots \eta(a_n)) = f(a_1) \ldots f(a_n)$ αφού η ϕ ομομορφισμός. Άρα η ϕ είναι μοναδική. Μένει να δείξουμε ότι η απεικόνιση $\phi : F_S \to G$ με $\phi(a) = f(a_1) \ldots f(a_n)$, όπου $a = (a_1, \ldots, a_n)$ ανηγμένη λέξη, είναι ομομορφισμός ομάδων. Επεκτείνουμε τη ϕ σε ολόκληρο το W, χρησιμοποιώντας τον παραπάνω τύπο για κάθε λέξη, ανηγμένη ή μη. Τότε $\phi(ab) = \phi(a)\phi(b)$ για κάθε $a, b \in W$. Επίσης αν $a \xrightarrow{1} b$ έπεται ότι $\phi(a) = \phi(b)$. Πράγματι,

αν $a = (a_1, \ldots, a_n)$ με $a_{i+1} = a_i^{-1}$ και $b = (a_1, \ldots, a_{i-1}, a_{i+2}, \ldots, a_n)$, για $1 \leq i < n$, τότε $f(a_{i+1}) = f(a_i)^{-1}$ και

$$\begin{aligned} \phi(a) &= f(a_1) \ldots f(a_{i-1}) f(a_i) f(a_{i+1}) f(a_{i+2}) \ldots f(a_n) \\ &= f(a_1) \ldots f(a_{i-1}) f(a_{i+2}) \ldots f(a_n) \\ &= \phi(b) \end{aligned}$$

Επομένως, $a \to b$ συνεπάγεται ότι $\phi(a) = \phi(b)$. Αν οι λέξεις a, b είναι ανηγμένες τότε $\phi(a \cdot b) = \phi(ab) = \phi(a)\phi(b)$ και άρα η ϕ είναι ομομορφισμός ομάδων. □

Πόρισμα 1.2.17. Έστω G ομάδα παραγόμενη από ένα υποσύνολο S. Τότε υπάρχει επιμορφισμός ομάδων της F_S στη G.

Απόδειξη. Από Θεώρημα 1.2.16 υπάρχει ομομορφισμός $\phi : F_S \to G$ τέτοιος ώστε $\phi \circ \eta$ είναι η εμφύτευση $S \hookrightarrow G$. Τότε $Im\phi = G$ αφού η εικόνα $Im\phi$ περιέχει κάθε γεννήτορα $s = \phi(\eta(s))$ της G. □

Συμβολισμοί: Μετά την κατασκευή της F_S συνηθίζεται η ταύτιση των στοιχείων $s \in S$ και $\eta(s) = (s) \in F_S$ καθώς και των στοιχείων $s^{-1} \in S^{-1}$ και $\eta(s^{-1}) = (s)^{-1} \in F_S$. Επίσης συνηθίζεται η γραφή των στοιχείων της F_S ως λέξεων αντί ακολουθιών (π.χ. $abb^{-1}c$ αντί για (a, b, b^{-1}, c)). Τότε έχουμε ότι $S \subseteq F_S$, $\eta : S \to F_S$ είναι η εμφύτευση και η F_S παράγεται από το σύνολο S.

Με αυτές τις ταυτοποιήσεις η **καθολική ιδιότητα** [1] του Θεωρήματος 1.2.16 υποδηλώνει ότι κάθε απεικόνιση f του S σε μία ομάδα G επεκτείνεται κατά μοναδικό τρόπο σε έναν ομομορφισμό $\phi : F_S \to G$. Αν $S \subseteq G$ τότε η ϕ απεικονίζει ένα στοιχείο της F_S, που είναι γινόμενο στοιχείων και αντιστρόφων στοιχείων του S, στο ίδιο γινόμενο υπολογισμένο στην ομάδα G. Ο πυρήνας $Ker\phi$ του ομομορφισμού ϕ ενδέχεται να είναι μη τετριμμένος. Σε αυτήν την περίπτωση υπάρχει ανηγμένη λέξη $w \in F_S$ τέτοια ώστε $\phi(w) = 1$. Τότε, από το Πρώτο Θεώρημα Ισομορφισμών έχουμε ότι $F_S \Big/ Ker\phi \simeq Im\phi$. Αν $G = \langle S \rangle$ τότε η ϕ είναι επιμορφισμός και επομένως $G \simeq F_S \Big/ Ker\phi$, δηλαδή η G είναι πηλίκο της ελεύθερης ομάδας F_S.

[1] Η έννοια της Καθολικής Ιδιότητας αποτελεί αντικείμενο της Θεωρίας Κατηγοριών.

1.3 Παραστάσεις Ομάδων

Έστω S σύνολο και G ομάδα με $G = \langle S \rangle$. Τότε η G είναι ισόμορφη με το πηλίκο $F_S \Big/ Ker\phi$, όπου F_S η ελεύθερη ομάδα επί του S και ϕ ο μοναδικός ομομορφισμός της F_S στην G. Εφόσον $Ker\phi \lhd F_S$ υπάρχει $R \subseteq F_S$ τέτοιο ώστε:

$$Ker\phi = \langle R \rangle^{F_S} = \bigcap \{H : H \lhd F_S \text{ και } R \subseteq H\}$$

Επομένως, η G καθορίζεται πλήρως από το σύνολο γεννητόρων S και το σύνολο R.

Ορισμός 1.3.1. Το σύνολο R με την ιδιότητα $Ker\phi = \langle R \rangle^{F_S}$ καλείται *σύνολο οριζουσών σχέσεων* της G και ένα στοιχείο του R καλείται *ορίζουσα σχέση* για την G.

Έτσι μπορούμε να συμβολίσουμε την ομάδα G ως το ζεύγος $\langle S \mid R \rangle$ το οποίο καλείται *παράσταση* της G.

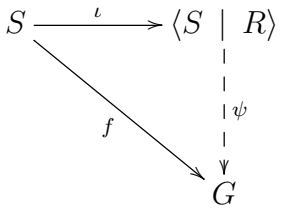
Αντιστρόφως, έστω S σύνολο και $R \subseteq F_S$. Τότε το ζεύγος (S, R) ορίζει *μοναδικά* μία παράσταση ομάδας $\langle S \mid R \rangle$. Η ομάδα $\langle S \mid R \rangle$ προκύπτει μέσω μίας απεικόνισης $\iota : S \to \langle S \mid R \rangle$ που είναι σύνθεση της εμφύτευσης $\eta : S \to F_S$ και της προβολής $\pi : F_S \to F_S \Big/ \langle R \rangle^{F_S} : \iota = \pi \circ \eta$.

Παρατήρηση 1.3.2. Η ομάδα G με παράσταση $\langle S \mid R \rangle$ είναι η "μεγαλύτερη" ομάδα που παράγεται από το S και υπόκειται σε κάθε σχέση $r \in R$, υπό την έννοια της επόμενης ιδιότητας.

Καθολική Ιδιότητα

Θεώρημα 1.3.3 (Dyck, 1882)**.** Έστω S σύνολο και R σύνολο σχέσεων μεταξύ στοιχείων του S. Θεωρούμε ακόμη μία ομάδα G και μία απεικόνιση $f : S \to G$ τέτοια ώστε κάθε σχέση $r \in R$ να ισχύει στην G μέσω της f. Τότε υπάρχει μοναδικός ομομορφισμός $\psi : \langle S \mid R \rangle \to G$ τέτοιος ώστε $f = \psi \circ \iota$, όπου $\iota : S \to \langle S \mid R \rangle$ η απεικόνιση-κανόνας. Αν η G παράγεται από την εικόνα $f(S)$ τότε η ψ είναι επιμορφισμός.

Με άλλα λόγια, το παρακάτω διάγραμμα είναι μεταθετικό:



Ειδικότερα, αν μία ομάδα G παράγεται από ένα σύνολο S και κάθε σχέση $r \in R$ ισχύει στην G τότε υπάρχει επιμορφισμός ομάδων $\langle S \mid R\rangle \to G$ και η G είναι ισόμορφη με μία ομάδα πηλίκο της $\langle S \mid R\rangle$.

Απόδειξη. Έστω $N = \bigcap\{H : H \lhd F_S \text{ και } R \subseteq H\}$. Από Θεώρημα 1.2.16 (καθολική ιδιότητα ελεύθερων ομάδων) υπάρχει μοναδικός ομομορφισμός $\phi : F_S \to G$ που επεκτείνει την f. Αφού κάθε σχέση $r \in R$ ισχύει στην G μέσω της f έχουμε ότι $\phi(r) = \phi(1)$ και άρα $r \in Ker\phi$ για κάθε $r \in R$. Επομένως $N \leqslant Ker\phi$. Έστω $\pi : F_S \to F_S\big/N = \langle S \mid R\rangle$ η κανονική προβολή. Τότε υπάρχει μοναδικός ομομορφισμός $\psi : \langle S \mid R\rangle \to G$ τέτοιος ώστε $\phi = \psi \circ \pi$. Επομένως $f = \psi\circ\iota$. Επιπλέον η ψ είναι ο μοναδικός ομομορφισμός της $\langle S \mid R\rangle$ στην G έτσι ώστε $\psi \circ \iota = f$. Πράγματι, αν υπάρχει $\chi : \langle S \mid R\rangle \to G$ με $\chi \circ \iota = f$ τότε $\psi(\iota(s)) = \chi(\iota(s))$ για κάθε $s \in S$ και άρα $\chi = \psi$. Αν $G = \langle f(S)\rangle$ τότε για κάθε γεννήτορα $f(s)$ της G έχουμε ότι $f(s) = \psi(\iota(s))$ και επομένως $G = \langle Im\psi\rangle$. □

Πόρισμα 1.3.4. Έστω S σύνολο και $R_1, R_2 \subseteq F_S$ με $R_1 \subseteq R_2$. Τότε η ομάδα με παράσταση $\langle S \mid R_2\rangle$ είναι πηλίκο της ομάδας με παράσταση $\langle S \mid R_1\rangle$.

Παρατήρηση 1.3.5. Μία ομάδα G ορίζεται μοναδικά από ένα ζεύγος (S, R). Όμως το ζεύγος (S, R) που ορίζει τη δεδομένη ομάδα G δεν είναι κατ' ανάγκη μοναδικό.

Παράδειγμα 1.3.6. *Έστω* $G = \langle \alpha \mid a^6 = 1\rangle$. *Επίσης έχουμε ότι*

$$G = \langle\ x, y \mid x^3, y^2, [x, y]\ \rangle.$$

Ορισμός 1.3.7. Έστω G ομάδα με παράσταση $\langle S \mid R\rangle$. Η G λέγεται *πεπερασμένα παριστώμενη* αν τα σύνολα S, R είναι πεπερασμένα.

Παρατήρηση 1.3.8. Έστω G πεπερασμένη ομάδα. Τότε ο πολλαπλασιαστικός πίνακας της G παρέχει μία πεπερασμένη παράσταση της G. Θεωρούμε ως γεννήτορες όλα τα στοιχεία $g_i \in G$ και ως ορίζουσες σχέσεις όλες τις ισότητες $g_i g_j = g_k$ που ισχύουν στην G. Επομένως μπορούμε να θεωρήσουμε την παράσταση της ομάδας ως μία συντομευμένη γενίκευση του πολλαπλασιαστικού πίνακα της ομάδας.

Παράδειγμα 1.3.9. *Υπάρχουν πολλά παραδείγματα άπειρων ομάδων που έχουν πεπερασμένη παράσταση. Ενδεικτικά αναφέρουμε:*

- *Η άπειρη διεδρική ομάδα* $D_\infty \cong \langle r, f \mid f^2, (rf)^2 \rangle$
- $\mathbb{Z} \times \mathbb{Z} \cong \langle x, y \mid xy = yx \rangle$

Από την άλλη μεριά, ο B.H.Neumann απέδειξε, το 1937, ότι υπάρχει υπεραριθμήσιμο πλήθος μη-ισόμορφων ομάδων που παράγονται από δύο στοιχεία. Αυτό εξηγεί την ύπαρξη πεπερασμένα παραγόμενων ομάδων που δεν επιδέχονται πεπερασμένη παράσταση.

1.4 Αλγοριθμικά προβλήματα

Πρίν αναφερθούμε στα αλγοριθμικά προβλήματα της Θεωρίας Ομάδων, είναι χρήσιμο να διατυπώσουμε μερικούς ορισμούς.

Ορισμός 1.4.1. Έστω $T \subseteq \mathbb{N}$. Το T καλείται *αναδρομικό* αν υπάρχει ολικά υπολογίσιμη συνάρτηση[2] f τέτοια ώστε

$$f(x) = \begin{cases} 1 & \text{αν } x \in T \\ 0 & \text{αν } x \notin T \end{cases}$$

Ορισμός 1.4.2. Έστω $T \subseteq \mathbb{N}$. Το T καλείται *αναδρομικά αριθμήσιμο* αν υπάρχει μερική αναδρομική συνάρτηση[3] f με πεδίο ορισμού το T.

[2]Μία συνάρτηση $f : \mathbb{N}^n \to \mathbb{N}$ για την οποία υπάρχει επαρκής αλγόριθμος για τον υπολογισμό των τιμών της καλείται *ολικά υπολογίσιμη συνάρτηση*.

[3]Μία συνάρτηση $f : \mathbb{N}^n \to \mathbb{N}$ η οποία είναι υπολογίσιμη για μερικές τιμές του πεδίου ορισμού της καλείται *μερική αναδρομική συνάρτηση*.

Έστω S σύνολο το οποίο επιδέχεται αρίθμηση από ένα σύνολο δεικτών I, ίσο με το $\mathbb{N}$ ή με πεπερασμένο υποσύνολο του $\mathbb{N}$. Μπορούμε τότε να ορίσουμε μία $1-1$ κωδικοποίηση (ή αρίθμηση Gödel) $f : F_S \to \mathbb{N}$, όπου F_S η ελεύθερη ομάδα επί του S. Με χρήση της κωδικοποίησης f μπορούμε να εντοπίσουμε αλγόριθμους που να υπολογίζουν ένα στοιχείο w δεδομένου του $f(w)$, και αντιστρόφως. Θα λέμε ότι ένα υποσύνολο U της F_S είναι *αναδρομικό* (αντίστοιχα *αναδρομικά αριθμήσιμο*) αν το $f(U)$ είναι αναδρομικό (αντίστοιχα αναδρομικά αριθμήσιμο). Αν το S επιδέχεται αρίθμηση όπως παραπάνω και το R είναι αναδρομικά αριθμήσιμο θα λέμε ότι η παράσταση είναι μία *αναδρομική παράσταση* και η αντίστοιχη ομάδα θα λέγεται *αναδρομικά παριστώμενη*.

Ο G.Higman απέδειξε, το 1961, ότι μία πεπερασμένα παραγόμενη ομάδα G έχει αναδρομική παράσταση αν και μόνο αν η G εμφυτεύεται σε μία πεπερασμένα παριστώμενη ομάδα. Επομένως, από το αποτέλεσμα του Neumann, προκύπτει ότι υπάρχουν πεπερασμένα παραγόμενες ομάδες που δεν επιδέχονται αναδρομική παράσταση.

Τα αλγοριθμικά προβλήματα της Θεωρίας Ομάδων διαχωρίζονται σε δύο κατηγορίες:

- Στα *προβλήματα απόφασης* τα οποία είναι της μορφής: Έστω $\mathcal{A}$ ένα αντικείμενο και $\mathcal{I}$ μία ιδιότητα. Να εξεταστεί αν το αντικείμενο $\mathcal{A}$ διαθέτει την ιδιότητα $\mathcal{I}$.

- Στα *προβλήματα αναζήτησης* τα οποία είναι της μορφής: Έστω $\mathcal{I}$ μία ιδιότητα που γνωρίζουμε ότι χαρακτηρίζει κάποια αντικείμενα. Να βρεθεί ένα τουλάχιστον αντικείμενο που διαθέτει την ιδιότητα $\mathcal{I}$.

Στη μελέτη θεμάτων σχετικών με την Κρυπτογραφία, θα μας απασχολήσουν τα παρακάτω αλγοριθμικά προβλήματα της Θεωρίας Ομάδων:

1.4.1 Το πρόβλημα της λέξης

Έστω G μία ομάδα με σύνολο γεννητόρων $S = \{s_1, \ldots, s_n\}$ και σύνολο οριζουσών σχέσεων $R = \{r_1, \ldots, r_k\}$. Θεωρούμε τις σχέσεις ως ρητά δηλωμένες λέξεις με γράμματα τα στοιχεία $s_i^{\pm 1}$. Το πρόβλημα της λέξης αποκαλείται

επιλύσιμο για την παράσταση της ομάδας αν υπάρχει αλγόριθμος που, δεδομένης μίας λέξης w με γράμματα από το S, μπορεί να αποφανθεί αν $w = 1 \in G$ (με άλλα λόγια αν η λέξη w ανήκει στην κανονική υποομάδα που παράγεται από το σύνολο R, μέσα στην ελεύθερη ομάδα F_S). Δηλαδή, αν θεωρήσουμε την ομάδα G ως το πηλίκο $F_S \Big/ N$, ο αλγόριθμος να μπορεί να αποφανθεί αν το στοιχείο w, θεωρούμενο ως λέξη της ελεύθερης ομάδας F_S, ανήκει στη N.

Είναι σχεδόν άμεσο το συμπέρασμα ότι το πρόβλημα της λέξης είναι ανεξάρτητο της εκάστοτε παράστασης. Θα λέμε ότι η ομάδα G έχει επιλύσιμο το πρόβλημα της λέξης αν το πρόβλημα είναι επιλύσιμο για κάποια -και επομένως για οποιαδήποτε- παράσταση της G.

Πρόταση 1.4.3. Έστω G ομάδα με αναδρομική παράσταση $\langle S \mid R \rangle$. Τότε το σύνολο των λέξεων $g \in G$ έτσι ώστε $g = 1$ είναι αναδρομικά αριθμήσιμο.

Απόδειξη. Ορίζουμε το σύνολο

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

Τότε υπάρχει μερική αναδρομική συνάρτηση f_P τέτοια ώστε:

$$f_P(\langle u, v \rangle) = \begin{cases} 0 & \text{αν } \langle u, v \rangle \in W \\ \text{μη ορισμένη} & \text{αν } \langle u, v \rangle \notin W \end{cases}$$

Επομένως μπορούμε να κατασκευάσουμε αναδρομική συνάρτηση g τέτοια ώστε:

$$g(\langle u, v \rangle) = \begin{cases} 0 & \text{αν } \langle u, v \rangle \notin W \\ \text{μη ορισμένη} & \text{αν } \langle u, v \rangle \in W \end{cases}$$

Αφού στην G $u = v \Leftrightarrow uv^{-1} = 1 \in G$ έπεται ότι μπορούμε να κατασκευάσουμε αναδρομική συνάρτηση h τέτοια ώστε:

$$h(x) = \begin{cases} 0 & \text{αν } x \neq 1 \in G \\ \text{μη ορισμένη} & \text{αν } x = 1 \in G \end{cases}$$

□

Παρατήρηση 1.4.4. Είναι πλέον γνωστό ότι υπάρχουν αναδρομικά αριθμήσιμα σύνολα των οποίων τα συμπληρώματα δεν είναι αναδρομικά αριθμήσιμα, π.χ. ένα αναδρομικά αριθμήσιμο σύνολο που δεν είναι αναδρομικό. Βάσει αυτού εξηγείται και η ύπαρξη πεπερασμένα παριστώμενων ομάδων για τις οποίες δε μπορούμε να αποφανθούμε αν το πρόβλημα της λέξης είναι επιλύσιμο (Θεώρημα Boone-Novikov). Παρά ταύτα υπάρχουν σημαντικές κλάσεις πεπερασμένα παριστώμενων ομάδων για τις οποίες το πρόβλημα της λέξης είναι επιλύσιμο.

Ορισμός 1.4.5. Έστω G ομάδα. Η G λέγεται προσεγγιστικά πεπερασμένη (residually finite) αν για κάθε $g \in G$ με $g \neq 1 \in G$ υπάρχει ομομορφισμός $h : G \to H$, όπου H πεπερασμένη ομάδα, τέτοιος ώστε $h(g) \neq 1$.

Ισοδύναμα, η G λέγεται προσεγγιστικά πεπερασμένη αν για $g \in G$ με $g \neq 1$ υπάρχει $N \lhd G$ τέτοια ώστε $g \notin N$ και η N είναι πεπερασμένου δείκτη (δηλαδή η G/N είναι πεπερασμένη).

Θεώρημα 1.4.6. Έστω G ομάδα πεπερασμένα παριστώμενη και προσεγγιστικά πεπερασμένη. Τότε το πρόβλημα της λέξης είναι επιλύσιμο για την G.

Απόδειξη. Έστω $G \cong \langle X \mid R \rangle$ πεπερασμένα παριστώμενη και προσεγγιστικά πεπερασμένη ομάδα. Θεωρούμε επίσης την ομάδα:

$$S = \{\sigma : \mathbb{N} \to \mathbb{N} : \sigma(i) = i \text{ για κάθε } i \in \mathbb{N} \setminus A, A \text{ πεπερασμένο } \}$$

Τότε:

1. Η S είναι τοπικά πεπερασμένη, δηλαδή κάθε πεπερασμένα παραγόμενη υποομάδα της S είναι πεπερασμένη, και περιέχει αντίγραφο κάθε πεπερασμένης ομάδας (Θεώρημα Cayley).

2. Το πρόβλημα της λέξης είναι επιλύσιμο στην S, υπολογίζοντας τα γινόμενα μεταθέσεων, διότι ένα στοιχείο της S γράφεται ως πεπερασμένο γινόμενο από γεννήτορες, οι οποίοι παράγουν πεπερασμένη ομάδα στην οποία το πρόβλημα της λέξης είναι επιλύσιμο.

3. Υπάρχει αναδρομική αρίθμηση όλων των απεικονίσεων του πεπερασμένου συνόλου X στην S.

4. Εφόσον η G είναι προσεγγιστικά πεπερασμένη, αν w είναι λέξη με γράμματα από το σύνολο γεννητόρων X με $w \neq 1$ τότε μπορούμε να βρούμε ένα μη τετριμμένο πεπερασμένο πηλίκο, του οποίου ένα αντίγραφο περιέχεται στην S, επομένως $w \neq 1$ αν και μόνο αν υπάρχει απεικόνιση του X στο S που επάγει ομομορφισμό τέτοιο ώστε $w \neq 1 \in S$.

Επομένως ορίζεται αναδρομική συνάρτηση h τέτοια ώστε:

$$h(x) = \begin{cases} 0 & \text{αν } x \neq 1 \in G \\ \text{μη ορισμένη} & \text{αν } x = 1 \in G \end{cases}$$

που σημαίνει ότι το πρόβλημα της λέξης είναι επιλύσιμο στην G. □

1.4.2 Το πρόβλημα της συζυγίας

Το δεύτερο αλγοριθμικό πρόβλημα της Θεωρίας Ομάδων που θα μας απασχολήσει σε θέματα Κρυπτογραφίας είναι το *πρόβλημα της συζυγίας* (ή πρόβλημα μετασχηματισμού):

Έστω G ομάδα με μία δεδομένη παράσταση και δύο στοιχεία $g, h \in G$. Το πρόβλημα της συζυγίας αποκαλείται επιλύσιμο για την G αν υπάρχει αλγόριθμος που προσδιορίζει την ύπαρξη ή μη ενός στοιχείου z τέτοιου ώστε $g = zhz^{-1}$.

Το πρόβλημα της συζυγίας, όπως και το πρόβλημα της λέξης, διατυπώθηκαν από τον Max Dehn το 1911, ως θεμελιώδη προβλήματα αποφάσεων της Θεωρίας Ομάδων.

Παρατήρηση 1.4.7. Το πρόβλημα της λέξης εμπεριέχεται, ως ειδική περίπτωση, στο πρόβλημα της συζυγίας: αν x και y είναι λέξεις με γράμματα από ένα σύνολο γεννητόρων, η απόφαση στο ερώτημα αν ταυτίζονται ισοδυναμεί με την απόφαση στο ερώτημα αν η λέξη xy^{-1} ισούται με το μοναδιαίο στοιχείο, με άλλα λόγια αν η λέξη xy^{-1} είναι συζυγής με το μοναδιαίο στοιχείο.

Για πολλές κλάσεις ομάδων είναι πλέον γνωστό πως δε μπορούμε να αποφανθούμε αν το πρόβλημα της συζυγίας είναι επιλύσιμο σε αυτές. Υπάρχουν όμως κλάσεις παραστάσεων ομάδων για τις οποίες το πρόβλημα της συζυγίας είναι επιλύσιμο.

Παράδειγμα 1.4.8. *Οι ελεύθερες ομάδες και οι πεπερασμένα παραγόμενες αβελιανές ομάδες έχουν επιλύσιμο το πρόβλημα της συζυγίας.*

Μία σημαντική κλάση ομάδων για την οποία είναι γνωστό ότι τα προβλήματα της λέξης και της συζυγίας είναι επιλύσιμα, είναι οι *ομάδες πλεξιδίων (braid groups)* στις οποίες αναφερόμαστε στο επόμενο κεφάλαιο.

1.4.3 Το πρόβλημα της διάσπασης

Μία γενικευμένη εκδοχή του προβλήματος της συζυγίας αποτελεί το *πρόβλημα της διάσπασης*:

Έστω G ομάδα αναδρομικά παριστώμενη, $A, B \leq G$ αναδρομικά παραγόμενες υποομάδες της G και δύο στοιχεία $g, h \in G$. Να βρεθούν στοιχεία $x \in A$ και $y \in B$ τέτοια ώστε $x \cdot g \cdot y = h$, δεδομένου ότι υπάρχει τουλάχιστον ένα τέτοιο ζεύγος στοιχείων.

Παρατήρηση 1.4.9. Η διατύπωση αυτή αποτελεί την εκδοχή του προβλήματος αναζήτησης. Η εκδοχή του αντίστοιχου προβλήματος απόφασης δε συναντάται σε θέματα σχετικά με την Κρυπτογραφία.

Παρατήρηση 1.4.10. Παρατηρούμε ότι πάντοτε υπάρχει ένα ζεύγος στοιχείων x, y έτσι ώστε $x \cdot g \cdot y = h$ (π.χ. θέτουμε $x = 1, y = g^{-1}h$). Επομένως, το ζητούμενο για τα στοιχεία x, y είναι να πληρούν τις προϋποθέσεις $x \in A$ και $y \in B$.

Στην ειδική περίπτωση όπου ισχύει ότι $A = B$, το πρόβλημα καλείται επίσης *προβλήμα διπλού συμπλόκου*.

Μία άλλη ειδική περίπτωση του προβλήματος της διάσπασης, όπου ισχύει ότι $g = 1$, αποτελεί το *πρόβλημα της παραγοντοποίησης*:

Έστω G ομάδα αναδρομικά παριστώμενη, $A, B \leq G$ υποομάδες της G και $w \in G$ ένα στοιχείο της G. Να βρεθούν στοιχεία $a \in A$ και $b \in B$ τέτοια ώστε $a \cdot b = w$.

Όπως αποδεικνύεται στο κεφάλαιο 4, ισχύει η εξής πρόταση η οποία συσχετίζει τα παραπάνω αλγοριθμικά προβλήματα.

Πρόταση 1.4.11. Έστω G ομάδα αναδρομικά παριστώμενη. Τότε:

1. Αν το πρόβλημα της συζυγίας είναι επιλύσιμο στη G, το πρόβλημα της διάσπασης είναι επίσης επιλύσιμο για δύο μετατιθέμενες υποομάδες $A, B \leq G$ (δηλαδή τέτοιες ώστε $ab = ba$ για κάθε $a \in A$ και $b \in B$).

2. Αν το πρόβλημα της συζυγίας είναι επιλύσιμο στη G, το πρόβλημα της παραγοντοποίησης είναι επίσης επιλύσιμο για δύο μετατιθέμενες υποομάδες $A, B \leq G$.

1.4.4 Το πρόβλημα του μέλους

Το *πρόβλημα του μέλους* διατυπώνεται ως εξής:

Έστω G ομάδα αναδρομικά παριστώμενη, $H \leq G$ υποομάδα της G με σύνολο γεννητόρων $h_1, \ldots, h_k$ και $g \in G$ ένα στοιχείο της G. Να εξεταστεί αν ισχύει ότι $g \in H$.

Παρατήρηση 1.4.12. Η παραπάνω διατύπωση αποτελεί την εκδοχή του προβλήματος απόφασης. Το σκέλος της θετικής απάντησης στο πρόβλημα έχει πάντοτε αναδρομική λύση, καθώς είναι εφικτή η αναδρομική απαρίθμηση όλων των στοιχείων μίας υποομάδας με πεπερασμένο σύνολο γεννητόρων.

1.5 Κανονικές Μορφές

Οι κανονικές μορφές των στοιχείων μίας ομάδας αποτελούν έναν κύριο μηχανισμό απόκρυψης για τα κρυπτογραφικά πρωτόκολλα. Για μία κανονική μορφή απαιτούμε να έχει τις εξής δύο βασικές ιδιότητες:

1. κάθε στοιχείο της ομάδας πρέπει να έχει ακριβώς μία κανονική μορφή

2. δύο στοιχεία που έχουν την ίδια κανονική μορφή πρέπει να είναι ισοδύναμα, ως προς κάποια σχέση ισοδυναμίας (βλ. Παράδειγμα 1.5.2)

Παράδειγμα 1.5.1. *Στην προσθετική ομάδα των ακεραίων μπορούμε να έχουμε διάφορες κανονικές μορφές : τη δεκαδική, τη δυαδική κλπ. Αυτές αποτελούν μία καλή μέθοδο για την απόκρυψη των παραγόντων ενός γινομένου. Μία σημαντική παρατήρηση από τη σκοπιά της Κρυπτογραφίας είναι ότι αν*

υπάρχουν διαφορετικές κανονικές μορφές για τα στοιχεία μίας δεδομένης ομάδας τότε μία κανονική μορφή μπορεί να αποκαλύπτει αυτό που μία άλλη προσπαθεί να αποκρύψει: π.χ. ο αριθμός 31 στη δεκαδική μορφή φαίνεται ' τυχαίος ', όμως ο ίδιος αριθμός στη δυαδική μορφή έχει ξεκάθαρο πρότυπο: 11111.

Παράδειγμα 1.5.2. *Αν έχουμε μία ελεύθερη ομάδα F_S επί του S, σύμφωνα με το Λήμμα 1.2.11 κάθε στοιχείο της έχει μοναδική κανονική μορφή (την ανηγμένη). Σε μία ομάδα με παράσταση $\langle S \mid R \rangle$ μπορούμε να κατασκευάσουμε συστήματα επαναγραφής, δηλαδή αλγόριθμους που λαμβάνουν μία λέξη από το δεδομένο αλφάβητο και τη μετατρέπουν σε μία άλλη λέξη του ίδιου αλφάβητου, χρησιμοποιώντας τις ορίζουσες σχέσεις. Ο αλγόριθμος τερματίζεται παράγοντας την κανονική μορφή του στοιχείου της ομάδας που αναπαριστά η λέξη που εισήχθη.*

Σε ομάδες που δίνονται με γεννήτορες και σχέσεις, οι κανονικές μορφές μπορεί να βασίζονται σε πιο ειδικές ιδιότητες (τοπολογικές, γεωμετρικές κλπ) μίας δεδομένης ομάδας κι όχι απλώς σε ένα σύστημα επαναγραφής. Παράδειγμα τέτοιας περίπτωσης αποτελούν οι κανονικές μορφές στις ομάδες πλεξιδίων, στις οποίες θα αναφερθούμε.

Κεφάλαιο 2

Ομάδες Πλεξιδίων

2.1 Εισαγωγή

Οι ομάδες πλεξιδίων παρουσιάστηκαν για πρώτη φορά από τον E.Artin, το 1925. Παρουσιάζουν σημαντικές ιδιότητες που τις καθιστούν ενδεδειγμένο μοντέλο για την ανάπτυξη Κρυπτογραφικών Πρωτοκόλλων[1]. Επί παραδείγματι, είναι μη Αβελιανές, που είναι θεμελιώδης απαίτηση για τη μη-μεταθετική Κρυπτογραφία. Επιπλέον, αποδείχθηκε πως είναι προσεγγιστικά πεπερασμένες, επομένως το πρόβλημα της λέξης είναι επιλύσιμο σε αυτές τις ομάδες. Σημαντικό πλεονέκτημα αποτελεί επίσης η δυνατότητα απτής απεικόνισης των στοιχείων μίας ομάδας πλεξιδίων.

Η εμφάνιση των ομάδων πλεξιδίων σε διάφορες περιοχές των Μαθηματικών (καθώς και της Φυσικής) - όπως για παράδειγμα η Θεωρία Κόμβων, η Τοπολογία, η Θεωρία Κβαντικών Πεδίων και η Στατιστική Μηχανική - προσδίδει αξιοπιστία ως προς τη δυσκολία επίλυσης σχετικών προβλημάτων. Από την άλλη μεριά, η εμφάνιση των πλεξιδίων σε διάφορες περιοχές των Μαθηματικών επιτρέπει τη χρήση διαφορετικών εργαλείων για την αντιμετώπιση ενός προβλήματος.

Όπως αποδείχθηκε, από τους D.Krammer και S.Bigelow, οι ομάδες πλεξιδίων είναι γραμμικές, και αυτή η ιδιότητα τις καθιστά δυνητικά ευπαθείς σε

[1]Η έννοια του Κρυπτογραφικού Πρωτοκόλλου παρουσιάζεται στο Κεφάλαιο 3.

γραμμικές αλγεβρικές επιθέσεις. Έτσι, ο αρχικός ενθουσιασμός σχετικά με τις εφαρμογές των ομάδων πλεξιδίων περιορίστηκε εξαιτίας αυτών των ενδείξεων ελλιπούς ασφάλειας στις αντίστοιχες Κρυπτογραφικές μεθόδους.

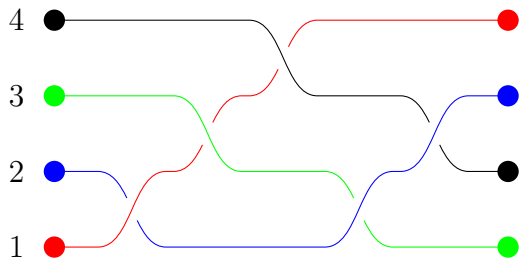
Παρ' όλα αυτά η μελέτη του αντικειμένου των ομάδων πλεξιδίων μπορεί να αποδειχθεί ιδιαίτερα χρήσιμη, καθώς αποτελεί κοινή παραδοχή ότι μία μη Αβελιανή ομάδα θα διαδραματίσει καθοριστικό ρόλο στην εξέλιξη της Κρυπτογραφίας δημοσίου κλειδιού.

2.2 Παράσταση μίας ομάδας πλεξιδίων

Μία εποπτική παρουσίαση

Για την πιο κατανοητή προσέγγιση της έννοιας του πλεξιδίου και των ιδιοτήτων που εμφανίζει, είναι χρήσιμο να προηγηθεί μία εποπτική παρουσίαση, χωρίς αυστηρότητα.

Ένα πλεξίδιο προκύπτει με τοποθέτηση παράλληλων νημάτων, πεπερασμένου πλήθους, τα οποία σχηματίζουν μία $1-1$ αντιστοιχία και κινούνται προς την ίδια κατεύθυνση, χωρίς να σχηματίζουν βρόγχους (θηλιές). Για την απεικόνιση των πλεξιδίων, εφαρμόζουμε οριζόντια τοποθέτηση των νημάτων με προσανατολισμό από αριστερά προς τα δεξιά και αρίθμηση που ξεκινάει από κάτω.

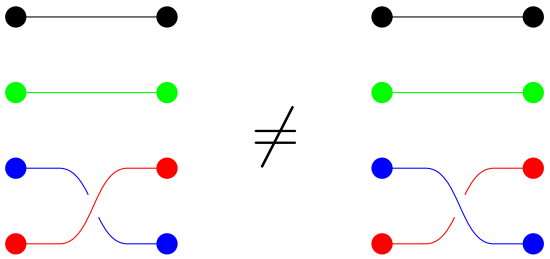


ένα πλεξίδιο

Παρατήρηση 2.2.1. Ένα πλεξίδιο αποτελεί μία απεικόνιση που είναι 1-1 και επί, επομένως μπορεί να θεωρηθεί ως μία μετάθεση.

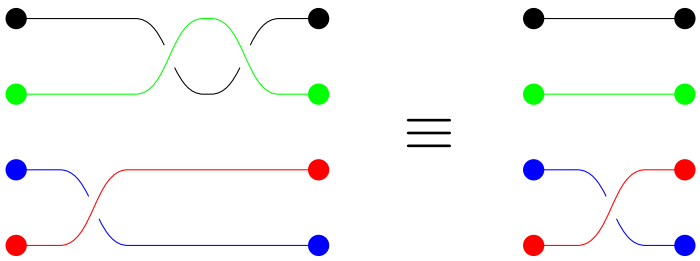
Δύο νήματα ενός πλεξιδίου μπορούν να διασταυρωθούν με δύο διαφορετικούς τρόπους -έμπροσθεν και όπισθεν- με αποτέλεσμα τη δημιουργία διαφορετικών πλεξιδίων.

Σύμφωνα με αυτήν τη διάκριση, έχουμε ότι:



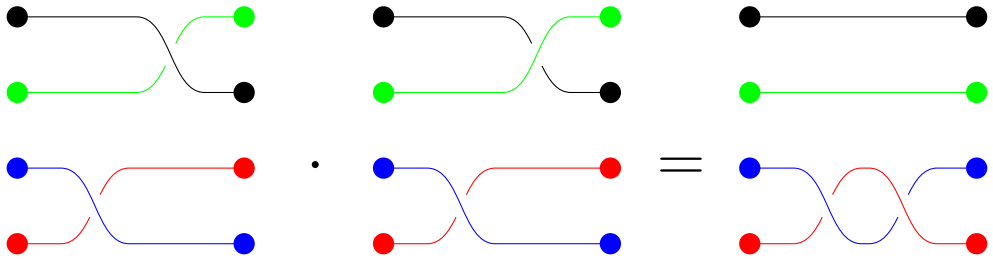
Παρατήρηση 2.2.2. Εδώ υπεισέρχεται η ουσιαστική διαφορά μεταξύ της έννοιας του πλεξιδίου και της μετάθεσης. Στα δύο πλεξίδια που απεικονίζονται στο παραπάνω σχήμα, αντιστοιχεί η ίδια μετάθεση $(1\ 2)$, όμως, ως πλεξίδια, θεωρούνται διαφορετικά.

Δύο πλεξίδια θα θεωρούνται ισοδύναμα αν το ένα προκύπτει από το άλλο με μετακίνηση των νημάτων στο χώρο, χωρίς ταυτόχρονη μετακίνηση των άκρων ή παρεμβολή της κίνησης σε άλλα νήματα. Έτσι, τα παρακάτω πλεξίδια είναι ισοδύναμα:



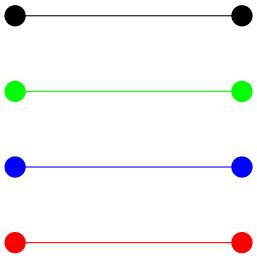
Η συνένωση δύο πλεξιδίων u, v, έτσι ώστε το τέλος του u να συμπίπτει με την αρχή του v, παράγει ένα νέο πλεξίδιο, το uv. Με άλλα λόγια, η πράξη της συνένωσης πλεξιδίων μπορεί να θεωρηθεί ως γινόμενο.

Για παράδειγμα:



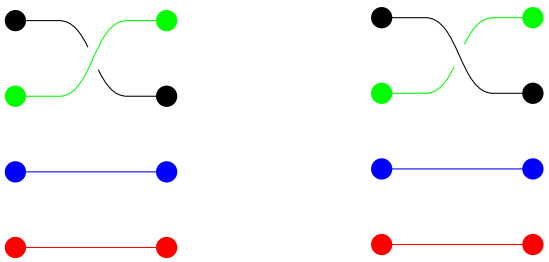
u v uv

Το σύνολο των πλεξιδίων με 4 νήματα συμβολίζεται με B_4. Στη γενική περίπτωση των πλεξιδίων με n το πλήθος νήματα, συμβολίζουμε το αντίστοιχο σύνολο με B_n. Η συνένωση πλεξιδίων, όπως ορίστηκε παραπάνω, αποτελεί πράξη με την οποία το σύνολο B_n αποκτά δομή ομάδας. Το ουδέτερο στοιχείο της ομάδας είναι το πλεξίδιο με τέσσερα παράλληλα νήματα:



το τετριμμένο πλεξίδιο

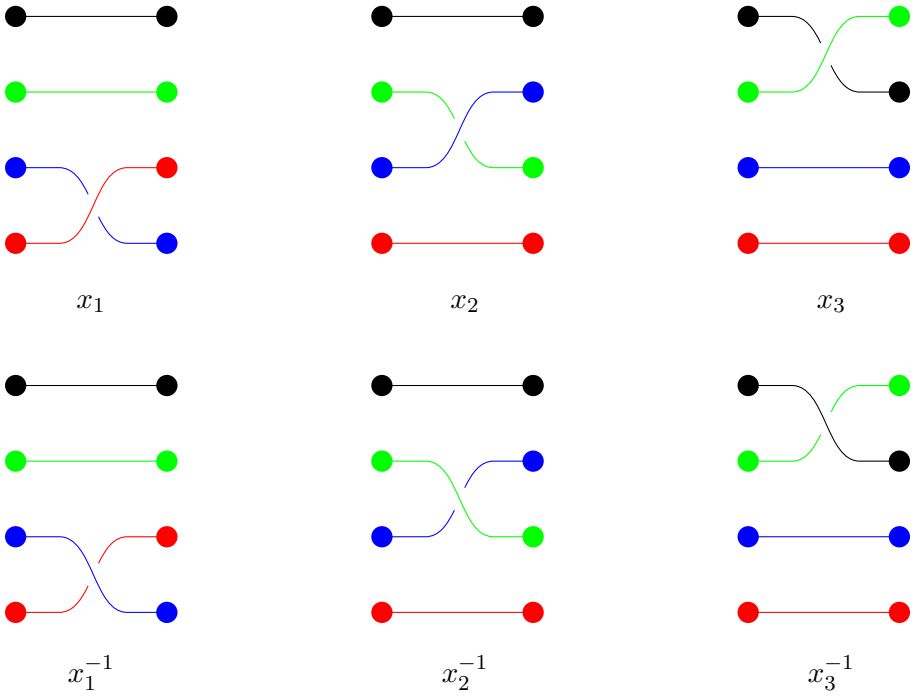
Το αντίστροφο ενός πλεξιδίου προκύπτει μέσω ανάκλασης του αρχικού, ως προς τον κάθετο άξονα. Για παράδειγμα:



u u^{-1}

Ένα πλεξίδιο μπορεί να θεωρηθεί ως μία ακολουθία διαπεπλεγμένων νημάτων. Θα λέμε ότι δύο νήματα διαπλέκονται με θετικό πρόσημο αν η κλίση του έμπροσθεν νήματος είναι θετική, διαφορετικά θα λέμε ότι το πρόσημο είναι αρνητικό. Για ένα πλεξίδιο με n το πλήθος νήματα υπάρχουν $n-1$ το πλήθος δυνατοί συνδυασμοί διασταυρώσεων των νημάτων. Συμβολίζουμε με x_i τη διασταύρωση, με θετικό πρόσημο, των νημάτων i και $i+1$.

Έτσι, έχουμε ότι:

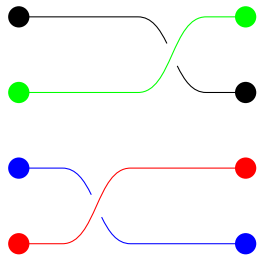


Επομένως, ένα πλεξίδιο της ομάδας B_n, ως ακολουθία διαπεπλεγμένων νημάτων, παράγεται από το σύνολο $\{x_1, \ldots, x_{n-1}\}$. Άμεσα προκύπτει ότι οι διασταυρώσεις των νημάτων $x_1, \ldots, x_{n-1}$ υπόκεινται στις σχέσεις:

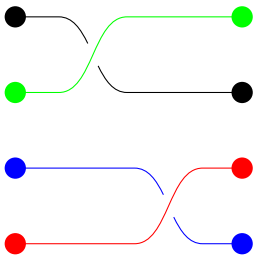
$$x_i x_j = x_j x_i \text{ για } i, j \text{ με } |i-j| > 1$$

$$x_i x_{i+1} x_i = x_{i+1} x_i x_{i+1} \text{ για } i \text{ με } 1 \leq i \leq n-2$$

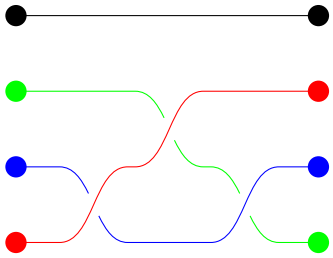
Παραδείγματος χάριν, στην ομάδα B_4 έχουμε ότι:



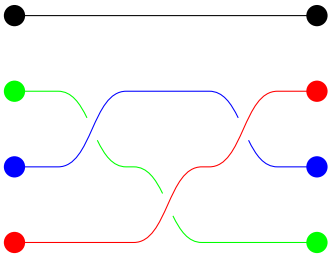
x_1x_3



x_3x_1



$x_1x_2x_1$



$x_2x_1x_2$

Ορισμός 2.2.3. Η ομάδα πλεξιδίων B_n είναι η ομάδα με την παράσταση:

$$B_n = \left\langle \quad x_1, \ldots, x_{n-1} \quad \middle| \begin{array}{ll} x_ix_jx_i = x_jx_ix_j & \text{αν } |i-j| = 1 \\ x_ix_j = x_jx_i & \text{αν } |i-j| > 1 \end{array} \right\rangle$$

Έστω G ομάδα και $f : B_n \to G$ ομομορφισμός ομάδων. Τότε τα στοιχεία $\{g_i = f(x_i)\}_{i=1,\ldots,n-1}$ της G ικανοποιούν τις σχέσεις:

$$x_ix_j = x_jx_i \text{ αν } |i-j| > 1$$

$$x_ix_{i+1}x_i = x_{i+1}x_ix_{i+1} \text{ για } 1 \leq i \leq n-2$$

Από την Καθολική Ιδιότητα του Θεωρήματος 1.3.3, προκύπτει άμεσα το παρακάτω πόρισμα.

Πόρισμα 2.2.4. Έστω $g_1, \ldots, g_{n-1} \in G$, τα οποία ικανοποιούν τις ορίζουσες σχέσεις της ομάδας πλεξιδίων B_n. Τότε υπάρχει μοναδικός ομομορφισμός $f : B_n \to G$ τέτοιος ώστε $g_i = f(x_i)$ για κάθε i με $1 \leq i \leq n-1$.

Εφαρμόζουμε το Πόρισμα 2.2.4 στην ομάδα μεταθέσεων S_n. Θεωρούμε τις μεταθέσεις της μορφής $(i\ \ i+1)$ για $1 \leq i \leq n-1$ και προκύπτει άμεσα ότι το σύνολο αυτών των μεταθέσεων ικανοποιεί τις ορίζουσες σχέσεις της ομάδας πλεξιδίων. Από το Πόρισμα 2.2.4 έπεται ότι υπάρχει μοναδικός ομομορφισμός ομάδων $\pi : B_n \to S_n$ τέτοιος ώστε $\pi(x_i) = (i\ \ i{+}1)$ για κάθε i με $1 \leq i \leq n{-}1$. Εφόσον το σύνολο των μεταθέσεων της μορφής $(i\ \ i+1)$, με $1 \leq i \leq n-1$ παράγει την S_n, έπεται ότι η π είναι επιμορφισμός ομάδων.

Λήμμα 2.2.5. Η ομάδα B_n είναι μη Αβελιανή, για $n \geq 3$.

Απόδειξη. Γνωρίζουμε ότι η ομάδα των μεταθέσεων S_n είναι μη Αβελιανή για $n \geq 3$, διότι $(1\ \ 2)(2\ \ 3) \neq (2\ \ 3)(1\ \ 2)$. Εφόσον η προβολή $\pi : B_n \to S_n$ είναι επιμορφισμός ομάδων έπεται ότι η ομάδα B_n είναι μη Αβελιανή για $n \geq 3$. □

Οι ομάδες πλεξιδίων παρουσιάζουν μία ακόμη καλή ιδιότητα, που καθιστά το πρόβλημα της λέξης επιλύσιμο σε αυτές. Την αναφέρουμε στο παρακάτω Θεώρημα, το οποίο παρουσιάζεται χωρίς απόδειξη.

Θεώρημα 2.2.6. Η ομάδα πλεξιδίων B_n και όλες οι υποομάδες της είναι προσεγγιστικά πεπερασμένες.

2.3 Κανονικές μορφές σε ομάδες πλεξιδίων

Η ύπαρξη κανονικών μορφών για τα στοιχεία μίας ομάδας είναι ιδιαίτερα χρήσιμη καθώς μας παρέχει τη δυνατότητα σύγκρισης των στοιχείων της ομάδας, και επομένως καθιστά επιλύσιμο το πρόβλημα της λέξης στην ομάδα που μελετάμε. Επίσης, μία κανονική μορφή μας παρέχει έναν αντιπρόσωπο από κάθε κλάση ισοδυναμίας μεταξύ των στοιχείων της ομάδας. Για τις ομάδες πλεξιδίων έχουν προταθεί δύο ειδών κανονικές μορφές οι οποίες παρουσιάζονται παρακάτω.

2.3.1 Κανονική μορφή του Garside

Ορισμός 2.3.1. Έστω w μία λέξη πλεξιδίων. Θα λέμε ότι η w είναι *θετικό πλεξίδιο* αν μπορεί να γραφεί ως γινόμενο θετικών δυνάμεων στοιχείων από το

σύνολο γεννητόρων $\{x_1, \ldots, x_{n-1}\}$. Το σύνολο των θετικών πλεξιδίων θα το συμβολίζουμε με B_n^+.

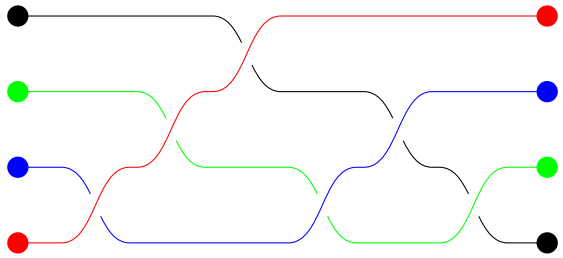
Παρατήρηση 2.3.2. Το τετριμμένο πλεξίδιο ϵ δεν είναι θετικό, αφού δε μπορεί να γραφεί ως γινόμενο θετικών δυνάμεων στοιχείων από το σύνολο γεννητόρων της B_n.

Ορισμός 2.3.3. Ορίζουμε το *θεμελιώδες πλεξίδιο* Δ_n με παράσταση:

$$\Delta_n = (x_1 \ldots x_{n-1})(x_1 \ldots x_{n-2}) \ldots x_1$$

Παρατήρηση 2.3.4. Γεωμετρικά, το Δ_n είναι το πλεξίδιο με n το πλήθος νήματα τα οποία, ανά δύο, τέμνονται ακριβώς μία φορά.

Για την ομάδα B_4, το πλεξίδιο Δ_4 απεικονίζεται στο παρακάτω σχήμα.



$$\Delta_4 = x_1x_2x_3x_1x_2x_1$$

Ιδιότητες: Το θεμελιώδες πλεξίδιο Δ_n έχει σημαντικές ιδιότητες μεταξύ των οποίων:

1. Για κάθε γεννήτορα x_i, με $1 \leq i \leq n-1$, έχουμε ότι:

$$\Delta_n = x_iA = Bx_i$$

όπου A, B είναι θετικά πλεξίδια.

2. Για κάθε γεννήτορα x_i, με $1 \leq i \leq n-1$, ισχύει:

$$\tau(x_i) = \Delta_n^{-1} x_i \Delta_n = x_{n-i}$$

όπου $\tau : B_n \to B_n$ ο επαγόμενος από το Δ_n εσωτερικός αυτομορφισμός της B_n, που καλείται απεικόνιση μετατόπισης.

3. Το στοιχείο Δ_n^2 ανήκει στο κέντρο της ομάδας B_n. Πράγματι, για κάθε i με $1 \leq i \leq n-1$, έχουμε ότι:

$$x_i\Delta_n^2 = x_i\Delta_n\Delta_n = \Delta_n x_{n-i}\Delta_n = \Delta_n\Delta_n x_i = \Delta_n^2 x_i$$

αφού

$$\Delta_n^{-1}x_i\Delta_n = x_{n-i} \Rightarrow \Delta_n^{-1}x_{n-i}\Delta_n = x_{n-(n-i)} = x_i$$

Αποδεικνύεται ότι, για $n > 2$, το κέντρο της ομάδας B_n είναι η κυκλική ομάδα που παράγεται από το στοιχείο Δ_n^2.

Προκειμένου να εισάγουμε την έννοια του απλού πλεξιδίου θα ορίσουμε μία σχέση μερικής διάταξης μεταξύ των στοιχείων της B_n.

Ορισμός 2.3.5. Έστω $A, B \in B_n$. Θα λέμε ότι το πλεξίδιο A είναι πρόθεμα του πλεξιδίου B και θα συμβολίζουμε $A \preceq B$ αν υπάρχει θετικό πλεξίδιο $C \in B_n^+$ τέτοιο ώστε $B = AC$.

Για τη μερική διάταξη $\preceq$ που ορίσαμε, ισχύουν οι ιδιότητες:

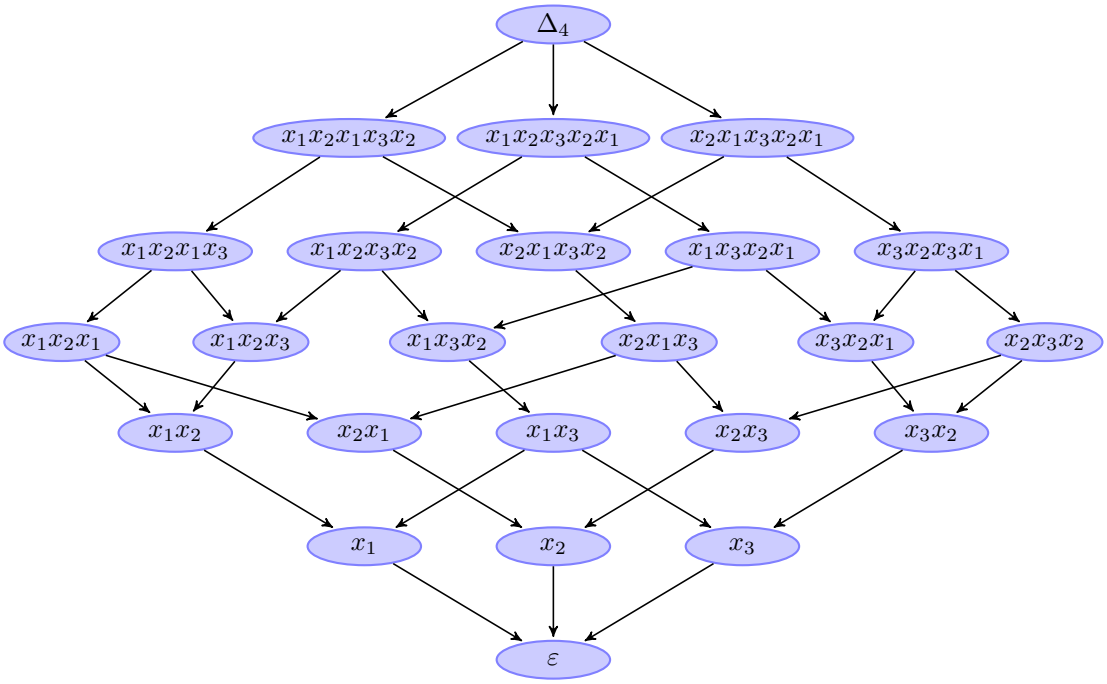
1. $B \in B_n^+ \Leftrightarrow \varepsilon \preceq B$ όπου ε το τετριμμένο πλεξίδιο.
2. $A \preceq B \Leftrightarrow B^{-1} \preceq A^{-1}$

Ορισμός 2.3.6. Έστω $P \in B_n$. Θα λέμε ότι το P είναι *απλό πλεξίδιο* αν ισχύει ότι $\varepsilon \preceq P \preceq \Delta_n$.

Παρατήρηση 2.3.7. Η απεικόνιση $\tilde{\pi} : P_n \to S_n$, όπου P_n το σύνολο των απλών πλεξιδίων, είναι 1-1 και επί. Επομένως υπάρχουν $n!$ το πλήθος απλά πλεξίδια. Εξ αυτού, τα απλά πλεξίδια λέγονται και μεταθετικά.

Γεωμετρικά, ένα απλό πλεξίδιο αποτελείται από n το πλήθος νήματα τα οποία, ανά δύο, διασταυρώνονται το πολύ μία φορά. Το σύνολο των απλών πλεξιδίων εφοδιασμένο με τη μερική διάταξη $\preceq$ αποκτά δομή συνδέσμου.

Στο παρακάτω σχήμα απεικονίζεται ο σύνδεσμος των απλών στοιχείων της ομάδας B_4.



ο σύνδεσμος των απλών στοιχείων της ομάδας B_4

Ορισμός 2.3.8. Έστω $P \in B_n$ ένα απλό πλεξίδιο. Ορίζουμε τα σύνολα:

$$S(P) = \{i : P = x_i P' \text{ για } P' \in B_n\} \text{ (σύνολο εκκίνησης)}$$

$$F(P) = \{i : P = P' x_i \text{ για } P' \in B_n\} \text{ (σύνολο τερματισμού)}$$

Δηλαδή, το σύνολο $S(P)$ (αντίστοιχα το σύνολο $F(P)$) είναι οι δείκτες των γεννητόρων της B_n που απαρτίζουν το αρχικό (αντίστοιχα τελικό) τμήμα μίας παράστασης του P.

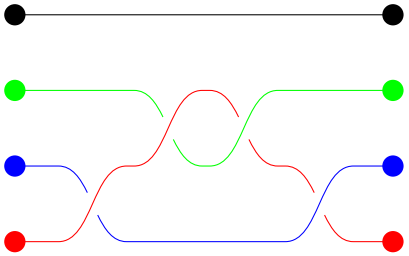
Παράδειγμα 2.3.9. $S(\Delta_n) = F(\Delta_n) = \{1, \ldots, n-1\}$

Ορισμός 2.3.10. Έστω $A \in B_n^+$ ένα θετικό πλεξίδιο. Μία ανάλυση του A σε απλά πλεξίδια, της μορφής:

$$A = P_1 P_2 \dots P_k$$

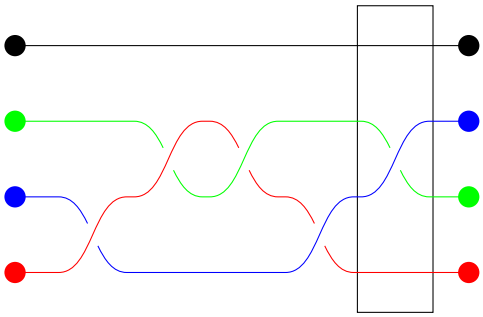
όπου τα P_i είναι απλά πλεξίδια και $S(P_{i+1}) \subset F(P_i)$ (δηλαδή κάθε προσθήκη ενός γεννήτορα από το P_{i+1} στο P_i μετατρέπει το P_i σε πλεξίδιο που δεν είναι απλό), καλείται *αριστερά βεβαρημένη*.

Παράδειγμα 2.3.11. *Το παρακάτω πλεξίδιο είναι αριστερά βεβαρημένο:*



το πλεξίδιο $x_1x_2x_2x_1$

Παράδειγμα 2.3.12. *Το παρακάτω πλεξίδιο δεν είναι αριστερά βεβαρημένο, λόγω της διασταύρωσης που βρίσκεται εντός του πλαισίου:*



το πλεξίδιο $x_1x_2x_2x_1x_2$

Αλγεβρικά, αυτό αποδεικνύεται ως εξής:

$$x_1x_2 \cdot x_2x_1x_2 = x_1x_2 \cdot x_1x_2x_1 = x_1x_2x_1 \cdot x_2x_1$$

Η κανονική μορφή του Garside για ένα πλεξίδιο δίνεται από το παρακάτω Θεώρημα.

Θεώρημα 2.3.13. Έστω $w \in B_n$ ένα πλεξίδιο. Τότε υπάρχει μοναδική παράσταση του w που δίνεται από τον τύπο:

$$w = \Delta_n^r P_1 P_2 \dots P_k$$

όπου $r \in \mathbb{Z}$ είναι η μεγαλύτερη δυνατή δύναμη του Δ_n που εμφανίζεται στο w, τα P_i με $1 \leq i \leq k$ είναι απλά πλεξίδια, $P_k \neq \varepsilon$ και η ανάλυση $P_1 P_2 \dots P_k$ είναι αριστερά βεβαρημένη.

Ο αλγόριθμος μετατροπής ενός πλεξιδίου στην κανονική μορφή του Garside αποτελείται από τα εξής βήματα:

1. Για κάθε αρνητική δύναμη ενός γεννήτορα αντικαθιστούμε το στοιχείο x_i^{-1} με το στοιχείο $\Delta_n^{-1} B_i$ όπου B_i είναι απλό πλεξίδιο.

2. Μετατοπίζουμε κάθε εμφάνιση του στοιχείου Δ_n προς τα αριστερά, χρησιμοποιώντας τη σχέση:

   $$\Delta_n^{-1} x_i \Delta_n = \tau(x_i) = x_{n-i}$$

   Τελικά έχουμε ότι $w = \Delta_n^{r'} \cdot A$, όπου $A \in B_n^+$ θετικό πλεξίδιο.

3. Αναλύουμε το A σε μία αριστερά βεβαρημένη παράσταση απλών πλεξιδίων. Αρχικά, διασπάμε την ανάλυση του A σε απλά πλεξίδια (δηλαδή παίρνουμε τις μεγαλύτερες δυνατόν ακολουθίες γεννητόρων που σχηματίζουν απλά πλεξίδια). Τότε έχουμε ότι $A = Q_1 Q_2 \dots Q_j$ όπου κάθε Q_i με $1 \leq i \leq j$ είναι απλό πλεξίδιο. Για κάθε i με $1 \leq i \leq j-1$ υπολογίζουμε τα σύνολα $F(Q_i)$ και $S(Q_{i+1})$. Αν $S(Q_{i+1}) \nsubseteq F(Q_i)$ τότε παίρνουμε ένα $x \in S(Q_{i+1}) \setminus F(Q_i)$ και, χρησιμοποιώντας τις ορίζουσες σχέσεις της ομάδας πλεξιδίων, μετατοπίζουμε το x από το Q_{i+1} στο Q_i. Τότε προκύπτει μία ανάλυση της μορφής:

   $$A = Q_1 Q_2 \dots Q_{i'} Q_{i'+1} \dots Q_j$$

   Συνεχίζουμε αυτή τη διαδικασία έως ότου να έχουμε ότι $S(Q_{i+1}) \subset F(Q_i)$ για κάθε i με $1 \leq i \leq j-1$ και τότε έχουμε τη ζητούμενη αριστερά βεβαρημένη παράσταση.

Παράδειγμα 2.3.14. *Έστω* $w = x_1 x_3^{-1} x_2 \in B_4$. *Η κανονική μορφή του* w *προκύπτει ως εξής:*

1. *Αντικαθιστούμε το* x_3^{-1} *με το* $\Delta_4^{-1} x_3 x_2 x_1 x_3 x_2$ *και έχουμε ότι*

$$w = x_1 \Delta_4^{-1} x_3 x_2 x_1 x_3 x_2 \cdot x_2$$

2. *Μετατοπίζουμε το* Δ_4 *προς τα αριστερά:*

$$w = \Delta_4^{-1} x_3 x_3 x_2 x_1 x_3 x_2 x_2$$

3. *Αναλύουμε το θετικό μέρος της παράστασης σε αριστερά βεβαρημένη μορφή:*

$$w = \Delta_4^{-1} x_2 x_1 x_3 x_2 x_1 \cdot x_1 x_2$$

Η πολυπλοκότητα του αλγορίθμου μετατροπής μίας λέξης $w \in B_n$ στην κανονική μορφή του Garside έχει αποδειχθεί ότι είναι της τάξης [2] $\mathcal{O}(|w|^2 nlogn)$ όπου $|w|$ το μήκος της λέξης w.

Ορισμός 2.3.15. Έστω $w \in B_n$ ένα πλεξίδιο. Ορίζουμε:

$$inf(w) = max\{r : \Delta_n^r \preceq w\}$$

$$sup(w) = min\{s : w \preceq \Delta_n^s\}$$

Άμεσα προκύπτει ότι αν $w = \Delta_n^m P_1 P_2 \dots P_k$ είναι η κανονική μορφή του Garside του πλεξιδίου w τότε $inf(w) = m$ και $sup(w) = m + k$.

Ορισμός 2.3.16. Έστω $w \in B_n$ ένα πλεξίδιο. Ορίζουμε ως *κανονικό μήκος* (ή πολυπλοκότητα) του w, και το συμβολίζουμε με $l(w)$, τον αριθμό:

$$l(w) = sup(w) - inf(w)$$

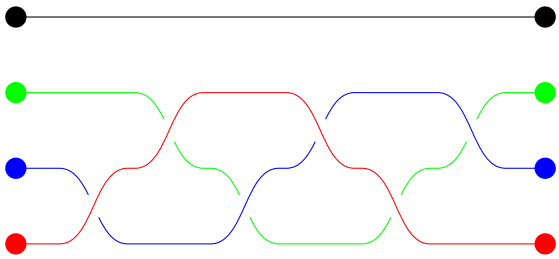
Επομένως, αν το w είναι στην κανονική μορφή του Garside τότε το κανονικό μήκος του w είναι το πλήθος των απλών πλεξιδίων στην παράσταση του w.

[2] Έστω $T(n)$ συνάρτηση. Ορίζουμε $T(n) \in \mathcal{O}(f(n))$ αν υπάρχουν σταθερές c και n_0 τέτοιες ώστε $T(n) \leq cf(n)$ για κάθε $n \geq n_0$. Αν $T(n) \in \mathcal{O}(f(n))$ τότε η συνάρτηση T καλείται της τάξης $f(n)$.

2.3.2 Κανονική μορφή του Dehornoy

Για την απόδειξη της επιλυσιμότητας του προβλήματος της λέξης σε ομάδες πλεξιδίων, ο P.Dehornoy παρουσίασε τη μέθοδο της αναγωγής λαβών σε ένα πλεξίδιο. Η διαδικασία αυτή μπορεί να θεωρηθεί ως μία γενίκευση της διαδικασίας αναγωγής λέξεων στις ελεύθερες ομάδες. Είναι σαφές ότι η διαδικασία της αναγωγής λέξεων στις ελεύθερες ομάδες, όπως ορίστηκε στο Κεφάλαιο 1, δεν επαρκεί για την επίλυση του προβλήματος της λέξης στην ομάδα B_n, καθώς υπάρχουν λέξεις ισοδύναμες με το μοναδιαίο στοιχείο $\varepsilon \in B_n$ που όμως δεν ανάγονται στην τετριμμένη λέξη.

Παράδειγμα 2.3.17. *Η λέξη $x_1x_2x_1x_2^{-1}x_1^{-1}x_2^{-1}$ αναπαριστά το τετριμμένο πλεξίδιο, όμως δεν επιδέχεται τετριμμένη αναγωγή.*



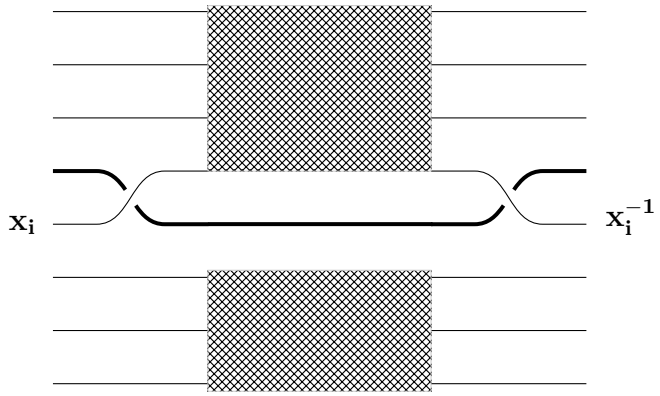
το πλεξίδιο $x_1x_2x_1x_2^{-1}x_1^{-1}x_2^{-1}$

Η διαδικασία της αναγωγής λαβών αφορά, εκτός από συλλαβές της μορφής xx^{-1} ή $x^{-1}x$, και περιπτώσεις λέξεων της μορφής $x_i \dots x_i^{-1}$ ή $x_i^{-1} \dots x_i$.

Ορισμός 2.3.18. Έστω w μία λέξη με γράμματα από το σύνολο γεννητόρων της ομάδας B_n. Μία x_i-λαβή είναι μία υπολέξη της w της μορφής:

$$x_i^{-\epsilon} u(x_1, \dots, x_{i-2}, x_{i+1}, \dots, x_n) x_i^{\epsilon} \qquad \epsilon = \pm 1$$

Γεωμετρικά, μία x_i-λαβή μπορεί να παρασταθεί ως εξής:



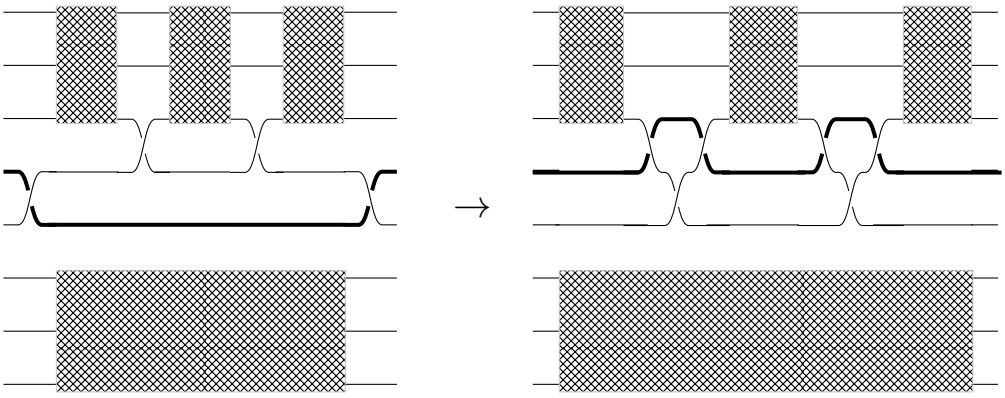
μία x_i-λαβή

Ορισμός 2.3.19. Έστω $x_i^{-\epsilon} w x_i^{\epsilon}$ μία x_i-λαβή με $w = w(x_1, \ldots, x_{i-2}, x_{i+1}, \ldots, x_n)$ και $\epsilon = \pm 1$. Η λαβή καλείται *επιτρεπτή* αν η w δεν περιέχει x_{i+1}-λαβές.

Ορισμός 2.3.20. Έστω v μία λέξη πλεξιδίων. Θα λέμε ότι η λέξη πλεξιδίων v' προκύπτει από τη v με εφάπαξ αναγωγή αν υπάρχει υπολέξη της v που είναι επιτρεπτή x_i-λαβή και η v' προκύπτει από τη v εφαρμόζοντας στα γράμματα της λαβής $x_i^{-\epsilon} w x_i^{\epsilon}$ τις εξής αντικαταστάσεις:

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

δηλαδή διαγράφοντας το αρχικό και το τελικό γράμμα $x_i^{\pm 1}$ και αντικαθιστώντας κάθε γράμμα $x_{i+1}^{\pm 1}$ με τη συλλαβή $x_{i+1}^{-\epsilon} x_i^{\pm 1} x_{i+1}^{\epsilon}$.



εφάπαξ αναγωγή μίας επιτρεπτής x_i-λαβής

Μέσω της διαδικασίας αναγωγής λαβών προκύπτει πλεξίδιο ισοδύναμο με το αρχικό. Επομένως, όπως και στη διαδικασία της αναγωγής στις ελεύθερες ομάδες, μία λέξη πλεξιδίων w είναι ισοδύναμη με το τετριμμένο πλεξίδιο ε αν υπάρχει ακολουθία αναγωγών της w στο ε, δηλαδή ακολουθία της μορφής $w = w_0 \to w_1 \to \cdots \to w_N = \varepsilon$ τέτοια ώστε η λέξη w_{k+1} να προκύπτει με αναγωγή λαβής από τη λέξη w_k, για κάθε $k = 0, \ldots, N-1$.

Ο βασικός ισχυρισμός σχετικά με τη διαδικασία της αναγωγής λαβών συνοψίζεται στο ακόλουθο Θεώρημα.

Θεώρημα 2.3.21. Έστω v μία λέξη πλεξιδίων. Τότε ισχύουν τα ακόλουθα:

- Μία ακολουθία από αναγωγές λαβών που εφαρμόζονται στη λέξη v τελικά τερματίζεται και παράγει μία λέξη πλεξιδίων v', απηλλαγμένη λαβών, η οποία αντιστοιχεί στο ίδιο στοιχείο της ομάδας B_n στο οποίο αντιστοιχεί και η v.

- Η λέξη v αναπαριστά το τετριμμένο στοιχείο της ομάδας B_n αν και μόνο αν με κάθε ακολουθία αναγωγής λαβών που εφαρμόζεται στη v προκύπτει το τετριμμένο στοιχείο της ομάδας B_n.

Η διαδικασία της αναγωγής λαβών έχει αποδειχθεί ιδιαιτέρως αποτελεσματική στην πράξη, καθώς στις περισσότερες περιπτώσεις τερματίζεται μετά από χρονικό διάστημα γραμμικό ως προς το μήκος της αρχικής λέξης πλεξιδίων.

Παρ΄ όλα αυτά δεν υπάρχει, ακόμα, κάποιος επαρκής υπολογισμός της θεωρητικής πολυπλοκότητας της μεθόδου. Διάφορες στρατηγικές για τη διαδικασία υλοποίησης της αναγωγής λαβών και προβληματισμοί σχετικά με θέματα πολυπλοκότητας αναφέρονται στο [9].

Σχόλιο

Όπως αποδείχθηκε από τους S.Bigelow[10] και D.Krammer[14], το 2001 και 2002 αντίστοιχα, οι ομάδες πλεξιδίων είναι γραμμικές, δηλαδή επιδέχονται αναπαράσταση στην ομάδα των πινάκων. Η απόδειξη τεκμηρίωσε τη δυνητική ευπάθεια των ομάδων πλεξιδίων σε γραμμικές αλγεβρικές επιθέσεις και κατέστησε επισφαλή τη χρήση τους σε εφαρμογές Κρυπτογραφίας. Πλέον, οι έρευνες εστιάζονται στη χρήση συσχετισμένων ομάδων πλεξιδίων (affine braid groups) [12] καθώς και σε εφαρμογές που υλοποιούνται με επιλογή κλειδιών από κατάλληλα επιλεγμένα υποσύνολα της αρχικής ομάδας.

Κεφάλαιο 3

Εισαγωγή στην Κρυπτογραφία

3.1 Εισαγωγή

Η λέξη "κρυπτογραφία" εισήχθη στην Ελληνική γλώσσα στα μέσα του 19ου αιώνα, ως αντιδάνειο από τη Γαλλική λέξη "cryptographie", που ετυμολογικά προκύπτει από τη σύνθεση των Ελληνικών λέξεων " κρυπτός " και "γράφω".

Η Κρυπτογραφία είναι η επιστήμη που περικλείει τη μελέτη, την ανάπτυξη και τη χρήση μεθόδων κρυπτογράφησης και αποκρυπτογράφησης, με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων. Ο σκοπός της Κρυπτογραφίας είναι η κατασκευή μηχανισμών που επιτρέπουν σε δύο ή περισσότερα μέρη να επικοινωνούν, χωρίς κάποιος άλλος να κατανοεί το περιεχόμενο της μεταδιδόμενης πληροφορίας.

Πολυάριθμα ιστορικά παραδείγματα καταδεικνύουν τη χρήση κρυπτογραφικών μεθόδων για τη μετατροπή της πληροφορίας από μία αντιληπτή μορφή σε έναν γρίφο, ο οποίος χωρίς τη γνώση του κρυφού μετασχηματισμού παρέμενε ακατανόητος. Στις πρωτοεμφανισθείσες μεθόδους, η κρυπτογράφηση του αρχικού κειμένου γινόταν, κατά βάση, με αλφαβητικούς μετασχηματισμούς (μετάθεση, αντικατάσταση).

Στις σύγχρονες μορφές, η Κρυπτογραφία βασίζεται στην αξιοποίηση μεθόδων που πηγάζουν από διάφορους τομείς των Μαθηματικών όπως η Θεωρία Αριθμών, τα Διακριτά Μαθηματικά, η Συνδυαστική, η Θεωρία Πιθανοτήτων, η

Στατιστική, η Υπολογιστική Πολυπλοκότητα και, εσχάτως, η Θεωρία Ομάδων.

Οι τέσσερις βασικές αρχές που εξυπηρετεί η χρήση κρυπτογραφικών μεθόδων είναι οι εξής:

- Εμπιστευτικότητα, δηλαδή απόκρυψη της πληροφορίας από μη εξουσιοδοτημένα μέρη.
- Ακεραιότητα δεδομένων, δηλαδή διασφάλιση του αμετάβλητου της πληροφορίας.
- Πιστοποίηση οντοτήτων, δηλαδή επικύρωση της ταυτότητας μίας οντότητας (ανθρώπου, τερματικού, πιστωτικής κάρτας κ.α.).
- Επικύρωση προέλευσης των δεδομένων, δηλαδή δέσμευση του αποστολέα ως προς την ταυτότητά του.

Μπορούμε να συνοψίσουμε τα παραπάνω στον ακόλουθο ορισμό.

Ορισμός 3.1.1. Η μελέτη των μαθηματικών μεθόδων που σχετίζονται με θέματα ασφάλειας των πληροφοριών καλείται *Κρυπτογραφία*.

3.2 Ιστορική αναδρομή

3.2.1 Η Κρυπτογραφία στους αρχαίους χρόνους

Τα πρώτα δείγματα χρήσης κρυπτογραφικών μεθόδων χρονολογούνται περίπου στο 1500 π.Χ., από πολιτισμούς που αναπτύχθηκαν στην περιοχή της Μεσοποταμίας. Σε μία σφηνοειδή επιγραφή που ανακαλύφθηκε στις όχθες του ποταμού Τίγρη, περιγραφόταν μία μέθοδος κατασκευής σμάλτων για αγγειοπλαστική. Σύμφωνα με ερευνητές[14], αυτή η επιγραφή θεωρείται ως το αρχαιότερο κρυπτογραφημένο κείμενο.

Στην αρχαία Ελλάδα, και ειδικότερα στη Σπάρτη, τον 5ο αιώνα π.Χ., γεννήθηκε η ιδέα της εφαρμογής κρυπτογραφικών μεθόδων για στρατιωτικούς σκοπούς.

Παράδειγμα 3.2.1. *Η Σπαρτιάτικη σκυτάλη : Σύμφωνα με αναφορές από τον Πλούταρχο, η σκυτάλη ήταν μία ράβδος από ξύλο ορισμένης διαμέτρου, επί της οποίας περιτυλιγόταν ελικοειδώς μία δερμάτινη λωρίδα. Το κείμενο γραφόταν κατά μήκος της σκυτάλης, χωρισμένο σε ένα γράμμα ανά έλικα. Η λωρίδα ξετυλιγόταν για να χρησιμοποιηθεί ως ζώνη και, εξαιτίας της αναδιάταξης των γραμμάτων, το κείμενο ήταν πλέον ακατάληπτο. Το κλειδί για την ανάγνωση του αρχικού μηνύματος ήταν η περιτύλιξη της λωρίδας σε σκυτάλη ίδιας διαμέτρου με την αρχική. Η κρυπτογράφηση μηνυμάτων με τη μέθοδο της σκυτάλης έχει ως βάση αυτό που πλέον αποκαλείται αλγόριθμος μετάθεσης.*

Αποδίδοντας "τα του Καίσαρος τω Καίσαρι", θα πρέπει να αναφέρουμε ότι και οι Ρωμαίοι γνώριζαν περί Κρυπτογραφίας.

Παράδειγμα 3.2.2. *Η μέθοδος κρυπτογραφίας του Καίσαρα : Ο Ιούλιος Καίσαρας, στην αλληλογραφία του με τον Κικέρωνα, εφάρμοζε τη μέθοδο της αντικατάστασης των γραμμάτων του κειμένου με τα αντίστοιχα γράμματα που βρίσκονται στην τρίτη επόμενη θέση του Λατινικού αλφάβητου. Έτσι, για παράδειγμα το γράμμα Α΄ αντικαθιστόταν από το γράμμα Δ΄, το γράμμα Β΄ από το γράμμα Ε΄, ενώ τα τρία τελευταία γράμματα του αλφάβητου αντικαθιστόνταν από τα τρία πρώτα. Η μέθοδος αυτή υιοθετήθηκε με διάφορες παραλλαγές και έχει ως βάση αυτό που πλέον αποκαλείται αλγόριθμος αντικατάστασης.*

3.2.2 Η Κρυπτογραφία στο Μεσαίωνα

Οι πρώτες μεθοδικές προσπάθειες αποκρυπτογράφησης κειμένων αποδίδονται στους Άραβες, περίπου τον 14ο αιώνα μ.Χ. Οι προσπάθειές τους επικεντρώνονταν σε πιθανοθεωρητική αναζήτηση της λύσης, με μέτρηση των συχνοτήτων εμφάνισης των γραμμάτων του κρυπτογραφημένου κειμένου και σύγκριση με τις αντίστοιχες συχνότητες εμφάνισης των γραμμάτων στην καθομιλουμένη γλώσσα.

Για παράδειγμα, έχει παρατηρηθεί, μέσω μετρήσεων, ότι το πιο συχνά εμφανιζόμενο γράμμα της Ελληνικής γλώσσας είναι το γράμμα Α΄. Αν σε κάποιο κρυπτογραφημένο κείμενο παρατηρηθεί ότι το πιο συχνά εμφανιζόμενο γράμμα

είναι το γράμμα Ή εφαρμόζεται αντικατάσταση του γράμματος Ή από το Ά, καθώς και άλλες, συχνοτικά σχετικές αντικαταστάσεις, με σκοπό την επίτευξη μίας κατανοητής μορφής κειμένου.

Η εξέλιξη αυτή επέφερε την ανάγκη επινόησης βελτιωμένων μορφών του αλγορίθμου αντικατάστασης, οι οποίες βασίζονταν στη χρήση πολλαπλών αλφάβητων για την εφαρμογή της κρυπτογράφησης. Σημαντική ήταν η συμβολή του Ιταλού Giovan Battista Bellaso καθώς και του Γάλλου Blaise de Vigenère, των οποίων η μέθοδος πολυαλφαβητικής αντικατάστασης χρησιμοποιείται μέχρι και στις μέρες μας.

Παράδειγμα 3.2.3. *Η μέθοδος κρυπτογράφησης του Vigenère : Η κρυπτογράφηση ενός κειμένου γίνεται με χρήση του πίνακα Vigenère (Πίνακας 3.1), ο οποίος είναι πίνακας "διπλής εισόδου". Ο πίνακας σχηματίζεται γράφοντας τα γράμματα του αλφάβητου σε γραμμές και εφαρμόζοντας διαδοχικές κυκλικές μεταθέσεις σε κάθε γραμμή, μετατοπίζοντας τα γράμματα μία θέση προς τα αριστερά. Η επάνω γραμμή και η αριστερή στήλη του πίνακα έχουν βοηθητικό ρόλο, λειτουργώντας ως σύστημα συντεταγμένων. Η κρυπτογράφηση του κειμένου γίνεται με χρήση μίας μυστικής, προσυμφωνημένης, λέξης και αντικατάσταση κάθε γράμματος του αρχικού κειμένου από το γράμμα το οποίο βρίσκεται στην αντίστοιχη θέση του πίνακα αντικατάστασης. Η αντίστοιχη θέση εντοπίζεται από το ζεύγος των συντεταγμένων (x, y), όπου x το γράμμα του αρχικου κειμένου και y το αντίστοιχο γράμμα της μυστικής λέξης.*

Εφαρμογή: Θεωρούμε ως αρχικό το κείμενο "ΕΠΙΘΕΣΗΤΟΠΡΩΙ" και ως μυστική τη λέξη "ΠΟΤΑΜΙ". Επεκτείνουμε με επαναλήψεις το μήκος της μυστικής λέξης, ώστε να είναι ίσο με το μήκος του αρχικού κειμένου. Στη συνέχεια σχηματίζουμε τα ζεύγη των αντίστοιχων συντεταγμένων για να εντοπίσουμε το γράμμα στο οποίο αντιστοιχεί η κρυπτογραφημένη εκδοχή του κειμένου. Έτσι, στο πρώτο ζεύγος συντεταγμένων (Ε,Π) διαπιστώνουμε ότι αντιστοιχεί το γράμμα Ύ κ.ο.κ.

Αρχικό κείμενο	Ε	Π	Ι	Θ	Ε	Σ	Η	Τ	Ο	Π	Ρ	Ω	Ι
Μυστική λέξη	Π	Ο	Τ	Α	Μ	Ι	Π	Ο	Τ	Α	Μ	Ι	Π
Κρυπτογραφημένο κείμενο	Υ	Ζ	Γ	Θ	Π	Β	Χ	Ι	Ι	Π	Δ	Θ	Ω

Για την αποκρυπτογράφηση του κειμένου χρησιμοποιούμε τα ζεύγη (y, z), όπου y το γράμμα της μυστικής λέξης και z το αντίστοιχο γράμμα του κρυπτογραφημένου κειμένου. Διατρέχουμε τη γραμμή που αντιστοιχεί στη συντεταγμένη y έως ότου εντοπίσουμε το κρυπτογραφημένο γράμμα. Η συντεταγμένη της στήλης στην οποία βρίσκεται το κρυπτογραφημένο γράμμα αποκαλύπτει το αντίστοιχο γράμμα του αρχικού κειμένου. Έτσι, για το πρώτο ζεύγος (Π,Υ), διατρέχουμε τη γραμμή με συντεταγμένη το γράμμα Π′ έως ότου εντοπίσουμε το γράμμα Υ′ του κρυπτογραφημένου κειμένου, το οποίο βρίσκεται στη στήλη με συντεταγμένη το γράμμα Έ′ κ.ο.κ.

	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω
Α	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω
Β	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α
Γ	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β
Δ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ
Ε	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ
Ζ	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε
Η	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ
Θ	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η
Ι	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ
Κ	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι
Λ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ
Μ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ
Ν	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ
Ξ	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν
Ο	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ
Π	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο
Ρ	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π
Σ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ
Τ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ
Υ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ
Φ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ
Χ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ
Ψ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ
Ω	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ

Πίνακας 3.1: Ο πίνακας Vigenère για το Ελληνικό αλφάβητο

Παρατήρηση 3.2.4. Μέσω του παραδείγματος γίνεται σαφής η έννοια της " πολυαλφαβητικής " αντικατάστασης, καθώς βλέπουμε ότι στις δύο εμφανίσεις του γράμματος Έ′ στο αρχικό κείμενο, αντιστοιχούν διαφορετικές εκδοχές κρυπτο-

γραφημένων γραμμάτων, το ΄Υ΄ και το Π΄ αντίστοιχα.

Σημαντική ήταν η συμβολή του Βρετανού επιστήμονα C.Wheatstone, στην εξέλιξη των μεθόδων αποκρυπτογράφησης, με την κατασκευή της πρώτης συσκευής αποκρυπτογράφησης, το 1867. Με χρήση αυτής της συσκευής έγινε δυνατή η αποκρυπτογράφηση των Αιγυπτιακών ιερογλυφικών, που αποτελούσαν, επί σειρά αιώνων, ένα άλυτο μυστήριο. Η ορθή ερμηνεία των ιερογλυφικών επιτεύχθηκε χάρη στην ανακάλυψη της περίφημης "στήλης της Rosetta" [1].

3.2.3 Η Κρυπτογραφία στον 20ο αιώνα

Η μεγάλη άνθηση της Κρυπτογραφίας συντελέστηκε κατά το πρώτο μισό του 20ου αιώνα, με τη θλιβερή αφορμή των δύο παγκοσμίων πολέμων. Η ανάγκη για ασφαλή μετάδοση πληροφοριών ζωτικής σημασίας οδήγησε στην ανάπτυξη νέων, περίπλοκων κρυπτογραφικών μεθόδων, η υλοποίηση των οποίων γινόταν με χρήση μηχανικών και ηλεκτρομηχανικών κατασκευών.

Οι Γερμανοί, κατά τη διάρκεια του 1ου παγκοσμίου πολέμου, στην προσπάθειά τους να υποκινήσουν πολεμική σύγκρουση μεταξύ των Η.Π.Α. και του Μεξικό, απέστειλαν ένα κρυπτογραφημένο τηλεγράφημα (που έγινε γνωστό ως τηλεγράφημα του Zimmermann), το οποίο υπέκλεψαν και αποκρυπτογράφησαν επιτυχώς οι Βρετανικές μυστικές υπηρεσίες. Η αποκάλυψη του περιεχομένου του μηνύματος εξόργισε την κοινή γνώμη της Αμερικής και συνέβαλε στην υποστήριξη της εμπλοκής των Η.Π.Α. στον πόλεμο.

Κατά τη διάρκεια του 2ου παγκοσμίου πολέμου, οι Γερμανοί έκαναν εκτεταμένη χρήση ενός συστήματος που έφερε το χαρακτηριστικό όνομα "Enigma". Η επικράτηση των συμμαχικών δυνάμεων κατέστη δυνατή λόγω της επιτυχημένης αποκρυπτογράφησης μηνυμάτων που είχαν κρυπτογραφηθεί από τη μηχανή Enigma. Επικεφαλής της πολυεθνικής ομάδας επιστημόνων που συνέβαλαν σε αυτήν την επιτυχία, ήταν ο Βρετανός μαθηματικός Alan Turing.

[1] Πέτρινη στήλη που χρονολογείται στο 2ο αιώνα π.Χ και προέρχεται από το ναό του Πτολεμαίου Ε΄. Η στήλη είχε χαραγμένο πάνω της το ίδιο κείμενο σε τρία συστήματα γραφής: στα ιερογλυφικά, στη δημώδη Αιγυπτιακή και στην Ελληνική.

Όμως, και στο άλλο μέτωπο του 2ου παγκοσμίου πολέμου, στον Ειρηνικό ωκεανό, η έγκυρη και έγκαιρη αποκρυπτογράφηση μηνυμάτων έκρινε καθοριστικά την έκβαση μίας από τις πιο φημισμένες συγκρούσεις του πολέμου, της ναυμαχίας του Midway.

Στην περίοδο ειρήνης που επακολούθησε, η ραγδαία ανάπτυξη των ηλεκτρονικών υπολογιστών, ιδιαίτερα κατά τις τελευταίες δεκαετίες, επέφερε νέες δυνατότητες που συνέβαλαν τα μέγιστα για την αλματώδη εξέλιξη των κρυπτογραφικών μεθόδων που χρησιμοποιούνται στις μέρες μας.

3.3 Κρυπτογραφία δημοσίου κλειδιού

Οι αλγόριθμοι μετάθεσης και αντικατάστασης, που αποτέλεσαν τη βάση για την ανάπτυξη των πρώτων κρυπτογραφικών μεθόδων, χαρακτηρίζονται από μία ιδιότητα που καθιστά αυτές τις μεθόδους ευάλωτες. Η γνώση του κλειδιού αποκρυπτογράφησης είναι ισοδύναμη (ή ταυτόσημη) με τη γνώση του κλειδιού κρυπτογράφησης και λόγω αυτής της ιδιότητας, οι αντίστοιχες μέθοδοι καλούνται *συμμετρικές*. Αυτή η χαρακτηριστική ιδιότητα των συμμετρικών μεθόδων εγείρει ζητήματα ασφάλειας ως προς τη μετάδοση του κλειδιού, καθώς δύο επικοινωνούντα μέρη πρέπει να συμφωνήσουν εκ των προτέρων στο κοινό μυστικό κλειδί, πριν την έναρξη της επικοινωνίας τους μέσω ανοιχτού διαύλου.

Η διαπίστωση αυτή οδήγησε στην ανάγκη ανάπτυξης κρυπτογραφικών μεθόδων για τις οποίες δεν απαιτείται μετάδοση του κλειδιού. Μία τέτοια μέθοδος καλείται *μέθοδος κρυπτογραφίας δημοσίου κλειδιού* (ή *ασύμμετρη*) και η υλοποίησή της γίνεται με τα παρακάτω βήματα:

- Οποιοσδήποτε επιθυμεί να λαμβάνει κρυπτογραφημένα μηνύματα δημοσιοποιεί ένα κλειδί, προς χρήση από κάθε πιθανό αποστολέα.
- Ο αποστολέας κρυπτογραφεί το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη.
- Ο παραλήπτης αποκρυπτογραφεί το μήνυμα χρησιμοποιώντας το μυστικό ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί με το οποίο έγινε η

κρυπτογράφηση του μηνύματος.

Παρατήρηση 3.3.1. Στις ασύμμετρες μεθόδους κρυπτογραφίας η γνώση του κλειδιού αποκρυπτογράφησης δεν είναι ισοδύναμη με τη γνώση του κλειδιού κρυπτογράφησης, μέσω κάποιου εφικτού υπολογισμού.

Η χρήση ασύμμετρων μεθόδων κρυπτογραφίας είναι ύψιστης σημασίας για την ασφαλή διεξαγωγή ηλεκτρονικών συναλλαγών μέσω του διαδικτύου, όπου είναι αδύνατη η χρήση ενός προκαθορισμένου κοινού μυστικού κλειδιού.

Μία από τις πλέον διαδεδομένες μεθόδους κρυπτογραφίας δημοσίου κλειδιού είναι η μέθοδος RSA, που επινοήθηκε από τους Rivest,Shamir και Adleman, το 1978.

Υλοποίηση της μεθόδου RSA:

- Ο παραλήπτης επιλέγει ένα ζεύγος πρώτων αριθμών p και q (π.χ. της τάξης του 10^{100}) καθώς και έναν αριθμό N σχετικά πρώτο με το γινόμενο $(p-1)(q-1)$. Ο παραλήπτης δημοσιοποιεί το γινόμενο $n = p \cdot q$ καθώς και έναν αριθμό M τέτοιον ώστε $MN \equiv 1 \mathrm{mod}(p-1)(q-1)$. Το ζεύγος (n, M) καλείται δημόσιο κλειδί.

- Ο αποστολέας, που επιθυμεί να στείλει ένα μήνυμα x στον παραλήπτη, μεταδίδει το ελάχιστο μη αρνητικό υπόλοιπο του $x^M \mathrm{mod} n$. Για τους αριθμούς x και x^M θα πρέπει να ισχύει : $0 \leq x, x^M < pq$.

- Ο παραλήπτης λαμβάνει έναν αριθμό y που αποτελεί την κρυπτογραφημένη εκδοχή του μηνύματος. Για την αποκρυπτογράφηση υπολογίζει το ελάχιστο μη αρνητικό υπόλοιπο του $y^N \mathrm{mod} n$, το οποίο είναι ίσο με τον αριθμό x που απεστάλη. Ο αριθμός N καλείται το μυστικό κλειδί για την αποκρυπτογράφηση.

Ο μηχανισμός της μεθόδου RSA βασίζεται σε μία γενίκευση του Euler για το μικρό Θεώρημα του Fermat, που είναι στοιχειώδες αποτέλεσμα της Θεωρίας Αριθμών. Η ασφάλεια της μεθόδου βασίζεται στη δυσκολία της παραγοντοποίησης ενός επαρκώς μεγάλου αριθμού σε γινόμενο πρώτων.

Η κεντρική ιδέα μίας μεθόδου κρυπτογραφίας δημοσίου κλειδιού στηρίζεται σε μία υποτιθέμενη μη-αντιστρεψιμότητα της διαδικασίας, που συνήθως αποκαλείται "καταπακτή" (trapdoor) ή *μονόδρομη συνάρτηση*.

Παράδειγμα 3.3.2. *Η μέθοδος RSA εκμεταλλεύεται την ευκολία στον υπολογισμό του γινομένου μεγάλων πρώτων αριθμών και, ταυτόχρονα, τη δυσκολία στην παραγοντοποίηση ενός μεγάλου αριθμού σε γινόμενο πρώτων.*

Ο αυστηρός μαθηματικός ορισμός της μονόδρομης συνάρτησης βασίζεται σε έννοιες υπολογιστικής πολυπλοκότητας και μπορεί να αναζητηθεί σε εξειδικευμένα συγγράμματα, όπως το [15].

Περιγραφικά, η τιμή μίας μονόδρομης συνάρτησης υπολογίζεται επαρκώς (δηλαδή σε χρόνο πολυωνυμικής τάξης ως προς την πολυπλοκότητα των δεδομένων που εισάγονται). Όμως, πιθανολογικά, δεν υπάρχει αλγόριθμος πολυωνυμικής τάξης για τον υπολογισμό των τιμών της αντίστροφης συνάρτησης, για ευρύ φάσμα δεδομένων.

Οι τρέχουσες εφαρμογές της κρυπτογραφίας δημοσίου κλειδιού περιλαμβάνουν ψηφιακές υπογραφές, πρωτόκολλα πιστοποίησης, ασφαλείς πολυμερείς υπολογισμούς κ.α. Θα εστιάσουμε στην έννοια των κρυπτογραφικών αρχεγόνων και, ειδικότερα, στους τρόπους εγκατάστασης ενός κοινού μυστικού κλειδιού, χωρίς προγενέστερη συμφωνία. Μία τέτοια διαδικασία καλείται *πρωτόκολλο εγκατάστασης κλειδιού*.

Παρατήρηση 3.3.3. Με την εγκατάσταση ενός κοινού μυστικού κλειδιού, δύο μέρη Α και Β μπορούν να επικοινωνούν χρησιμοποιώντας, πλέον, συμμετρικές μεθόδους κρυπτογραφίας, με προφανή οφέλη στην ταχύτητα των σχετικών υπολογισμών για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων.

3.4 Κρυπτογραφία μέσω εγκατάστασης κλειδιού

Υποθέτουμε ότι δύο μέρη $\mathcal{A}$ και $\mathcal{B}$ μοιράζονται ένα κοινό μυστικό κλειδί K, που είναι στοιχείο ενός συνόλου S, το οποίο καλείται *χώρος κλειδιών*.

Έστω $F : S \to \{0,1\}^n$, μία συνάρτηση από το σύνολο S στο σύνολο των δυαδικών ακολουθιών μήκους n. Επιλέγουμε ένα επαρκώς μεγάλο n, π.χ. τουλάχιστον ίσο με $log_2|S|$, αν το S είναι πεπερασμένο, ή ακόμη μεγαλύτερο αν το επιτρέπει η διαθέσιμη υπολογιστική ισχύς και το S είναι άπειρο. Μία τέτοια συνάρτηση καλείται *συνάρτηση κατακερματισμού*. Οι συναρτήσεις κατακερματισμού χρησιμοποιούνται επίσης σε εφαρμογές σχετικές με την ασφάλεια πληροφοριών, όπως ψηφιακές υπογραφές, διασφάλιση της ακεραιότητας των δεδομένων και άλλες μορφές επικύρωσης.

Κρυπτογράφηση: Το μέρος $\mathcal{A}$ κρυπτογραφεί ένα μήνυμα $m \in \{0,1\}^n$ μέσω του τύπου:

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

όπου η πρόσθεση $\oplus$ γίνεται με αριθμητική modulo 2.

Αποκρυπτογράφηση: Το μέρος $\mathcal{B}$ αποκρυπτογραφεί το μήνυμα μέσω του τύπου:

$$(m \oplus F(K)) \oplus F(K) = m \oplus (F(K) \oplus F(K)) = m$$

Παρατήρηση 3.4.1. Παρατηρούμε ότι αυτή η μέθοδος κρυπτογράφησης έχει παράγοντα επέκτασης ίσο με 1, με άλλα λόγια το κρυπτογραφημένο μήνυμα είναι ίδιου μήκους με το αρχικό. Για την περαιτέρω διασφάλιση της μεθόδου κρυπτογράφησης απαιτείται αύξηση του παράγοντα επέκτασης, ακόμα και έως την τάξη εκατοντάδων. Η αύξηση του όγκου της μεταδιδόμενης πληροφορίας είναι το τίμημα για την ασφαλέστερη κρυπτογράφηση των δεδομένων.

3.5 Το πρωτόκολλο Diffie-Hellman

Η μέθοδος εγκατάστασης κλειδιού των Diffie-Hellman[2] αποτελεί μία από τις πρώτες πρακτικές μεθόδους για την εγκατάσταση ενός κοινού μυστικού

[2]Ο M.Hellman, το 2002, αναγνωρίζοντας τη συμβολή του R.Merkle στην ανάπτυξη της θεωρίας διανομής δημοσίων κλειδιών, πρότεινε να προστεθεί το όνομα του Merkle στην ονομασία του πρωτοκόλλου.

κλειδιού, με επικοινωνία μέσω ανοικτού (μη ασφαλούς) διαύλου. Το κοινό μυστικό κλειδί που προκύπτει από τον αλγόριθμο των Diffie-Hellman μπορεί μετά να χρησιμοποιηθεί για την εφαρμογή συμμετρικών μεθόδων κρυπτογραφίας.

Η απλούστερη -και πρωτότυπη- υλοποίηση του πρωτοκόλλου Diffie-Hellman γίνεται επί της πολλαπλασιαστικής ομάδας των ακεραίων modulo p, όπου p πρώτος, και με ένα στοιχείο g που είναι πρωταρχική ρίζα mod$p$ (δηλαδή για κάθε ακέραιο a, που είναι σχετικά πρώτος με τον p υπάρχει k τέτοιο ώστε $g^k \equiv a \mathrm{mod} p$). Στη γενική περίπτωση η εφαρμογή του πρωτοκόλλου γίνεται επί μίας τυχαίας πεπερασμένης κυκλικής ομάδας.

Η υλοποίηση περιλαμβάνει τα παρακάτω βήματα:

1. Τα μέρη $\mathcal{A}$ και $\mathcal{B}$ προκαθορίζουν μία πεπερασμένη κυκλική ομάδα G και ένα γεννήτορα $g \in G$. Η G θεωρείται πολλαπλασιαστική ομάδα.

2. Ο $\mathcal{A}$ επιλέγει τυχαία ένα φυσικό αριθμό a και αποστέλλει το στοιχείο g^a στον $\mathcal{B}$.

3. Ο $\mathcal{B}$ επιλέγει τυχαία ένα φυσικό αριθμό b και αποστέλλει το στοιχείο g^b στον $\mathcal{A}$.

   Προφανώς, οι αριθμοί a, b θα πρέπει να είναι διαφορετικοί του $0 \mathrm{mod} |G|$.

4. Ο $\mathcal{A}$ υπολογίζει το στοιχείο $(g^b)^a = g^{ba}$.

5. Ο $\mathcal{B}$ υπολογίζει το στοιχείο $(g^a)^b = g^{ab}$.

Εφόσον η ομάδα $\mathbb{Z}$ είναι μεταθετική, έχουμε ότι $ba = ab$ και επομένως οι $\mathcal{A}$ και $\mathcal{B}$ διαθέτουν πλέον ένα κοινό στοιχείο K της ομάδας, το οποίο μπορεί να χρησιμοποιηθεί ως κοινό μυστικό κλειδί.

Το πρωτόκολλο θεωρείται ασφαλές ως προς τον κίνδυνο υποκλοπών, εφόσον η ομάδα G και το στοιχείο g επιλεγούν κατάλληλα. Ένας " ωτακουστής ", που παρεμβάλλεται στην επικοινωνία των $\mathcal{A}$ και $\mathcal{B}$, καλείται να επιλύσει το πρόβλημα Diffie-Hellman, δηλαδή να ανακτήσει το στοιχείο g^{ab} από τα στοιχεία g^a και g^b, προκειμένου να βρει το κοινό μυστικό κλειδί. Η επίλυση του προβλήματος θεωρείται δύσκολη εφόσον προηγηθεί "καλή" επιλογή των αρχικών παραμέτρων.

Μία λύση του προβλήματος Diffie-Hellman, που θα καθιστούσε τη χρήση του πρωτοκόλλου επισφαλή, θα μπορούσε να υλοποιηθεί με έναν επαρκή αλγόριθμο επίλυσης του προβλήματος διακριτού λογαρίθμου (δηλαδή την εύρεση του στοιχείου a από τα στοιχεία g και g^a). Ωστόσο, δεν έχει αποδειχθεί η ισοδυναμία του προβλήματος Diffie-Hellman με το πρόβλημα διακριτού λογαρίθμου.

Παρατήρηση 3.5.1. Η επίλυση του προβλήματος διακριτού λογαρίθμου θα μπορούσε να επιτευχθεί με μία μέθοδο " ωμής βίας ", δηλαδή με διαδοχικές δοκιμές όλων των φυσικών αριθμών, από το 1 έως το n, έως τον εντοπισμό του μεταδιδόμενου στοιχείου. Αυτή η διαδικασία απαιτεί $\mathcal{O}(|g|)$ το πλήθος πράξεις, όπου $|g|$ είναι η τάξη του στοιχείου g. Σε πρακτικές εφαρμογές υλοποίησης η τάξη του g είναι του μεγέθους 10^{300}, επομένως μία τέτοια μέθοδος θεωρείται υπολογιστικά ανεπαρκής.

Η παρατήρηση αυτή εγείρει ερωτήματα σχετικά με την υπολογιστική πολυπλοκότητα της μεθόδου, καθώς τα επικοινωνούντα μέρη φαίνεται να εκτελούν, επίσης, $\mathcal{O}(|g|)$ πράξεις για τον υπολογισμό των στοιχείων g^a και g^b. Ωστόσο, για αυτούς τους υπολογισμούς υπάρχει ταχύτερη μέθοδος που βασίζεται στον πολλαπλασιασμό τετραγώνων. Για παράδειγμα:

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

Επομένως, για τον υπολογισμό του στοιχείου g^a, απαιτούνται $\mathcal{O}(log_2 a)$ το πλήθος πράξεις και έτσι η μέθοδος θεωρείται υπολογιστικά επαρκής.

3.6 Το σύστημα κρυπτογραφίας ElGamal

Το σύστημα κρυπτογραφίας ElGamal αποτελεί μία μέθοδο κρυπτογραφίας δημοσίου κλειδιού, η οποία βασίζεται στο πρωτόκολλο Diffie-Hellman. Η μέθοδος ElGamal χρησιμοποιείται στο ελεύθερο λογισμικό (λογισμικό με γενική δημόσια άδεια χρήσης) Privacy Guard, στις νεότερες εκδόσεις του λογισμικού PGP (όνομα που προέρχεται από τα αρχικά των λέξεων Pretty Good Privacy) καθώς και σε άλλα συστήματα κρυπτογραφίας. Το πρωτόκολλο κρυπτογραφίας ElGamal εμπεριέχει τα παρακάτω βήματα:

1. Τα μέρη $\mathcal{A}$ και $\mathcal{B}$ προκαθορίζουν μία πεπερασμένη κυκλική ομάδα G και ένα στοιχείο $g \in G$ που είναι γεννήτορας της G.

2. Ο παραλήπτης $\mathcal{A}$ επιλέγει τυχαία ένα φυσικό αριθμό a και δημοσιοποιεί το στοιχείο $c = g^a$.

3. Ο αποστολέας $\mathcal{B}$, που επιθυμεί να στείλει ένα μήνυμα $m \in G$ στον $\mathcal{A}$, επιλέγει τυχαία ένα φυσικό αριθμό b και αποστέλλει στον $\mathcal{A}$ τα στοιχεία $m \cdot c^b$ και g^b. Παρατηρούμε ότι $c^b = (g^a)^b = g^{ab}$.

4. Ο $\mathcal{A}$ αποκρυπτογραφεί το μήνυμα m μέσω του τύπου:

$$m = (m \cdot c^b) \cdot ((g^b)^a)^{-1}.$$

Η μέθοδος κρυπτογραφίας ElGamal διαθέτει μία αξιοσημείωτη ιδιότητα: είναι μία πιθανολογική μέθοδος, δηλαδή υπάρχουν πολλές πιθανές εκδοχές για την κρυπτογραφημένη μορφή του ίδιου αρχικού κειμένου.

Παρατήρηση 3.6.1. Το σύστημα κρυπτογραφίας ElGamal έχει μέσο παράγοντα επέκτασης ίσο με 2 (δηλαδή το κρυπτογραφημένο μήνυμα έχει διπλάσιο μήκος από το αρχικό).

3.7 Επικύρωση

Ορισμός 3.7.1. Μία διαδικασία επαλήθευσης της ψηφιακής ταυτότητας του αποστολέα ενός μηνύματος καλείται *επικύρωση*.

Στην κρυπτογραφία δημοσίου κλειδιού, ιδιαίτερο ενδιαφέρον παρουσιάζουν οι μέθοδοι ταυτοποίησης " μηδενικής γνώσης ". Η πρακτική σημασία μίας τέτοιας μεθόδου είναι ότι το γεγονός μίας επιτυχούς ταυτοποίησης δεν αποκαλύπτει καμία άλλη πληροφορία, πέραν αυτής. Έτσι, το ένα μέρος επιθυμεί την απόδειξη της ταυτότητάς του στο άλλο μέρος, μέσω ενός μυστικού κλειδιού, χωρίς να μπορεί κάποιος να γνωρίζει οτιδήποτε σχετικά με το κλειδί.

Πολλά πρωτόκολλα εγκατάστασης κλειδιού μπορούν να τροποποιηθούν ελαφρώς, ώστε να προκύψουν πρωτόκολλα επικύρωσης. Η παρακάτω μέθοδος βασίζεται στο πρωτόκολλο Diffie-Hellman και εμπεριέχει τα εξής βήματα:

Υποθέτουμε ότι το μέρος $\mathcal{A}$ επιθυμεί να επικυρώσει την ταυτότητά του στο μέρος $\mathcal{B}$, έτσι ώστε ο $\mathcal{A}$ να πείσει τον $\mathcal{B}$ ότι γνωρίζει ένα μυστικό, χωρίς να αποκαλύψει το ίδιο το μυστικό.

1. Ο $\mathcal{A}$ δημοσιοποιεί μία πεπερασμένη κυκλική ομάδα G και ένα γεννήτορα g της G. Επίσης, επιλέγει τυχαία ένα φυσικό αριθμό a και δημοσιοποιεί το στοιχείο g^a.

2. Ο $\mathcal{B}$ επιλέγει τυχαία ένα φυσικό αριθμό b και αποστέλλει την "πρόκληση" g^b στον $\mathcal{A}$.

3. Ο $\mathcal{A}$ απαντά αποστέλλοντας την απόδειξη $P = (g^b)^a = g^{ba}$.

4. Ο $\mathcal{B}$ επαληθεύει ότι $(g^a)^b = P$.

Κεφάλαιο 4

Μη-μεταθετική Κρυπτογραφία

4.1 Εισαγωγή

Οι πιο διαδεδομένες μέθοδοι Κρυπτογραφίας δημοσίου κλειδιού καθώς και πρωτόκολλα εγκατάστασης δημοσίου κλειδιού που χρησιμοποιούνται στις μέρες μας, όπως ο αλγόριθμος RSA, το πρωτόκολλο Diffie-Hellman κ.λ.π., βασίζονται σε αποτελέσματα της Θεωρίας Αριθμών και επομένως στη δομή της Αβελιανής ομάδας των ακεραίων. Η ραγδαία ανάπτυξη των ηλεκτρονικών υπολογιστών, που επιφέρει σημαντική αύξηση της διαθέσιμης υπολογιστικής ισχύος, καθιστά τις μεθόδους αυτές θεωρητικά επισφαλείς και πλέον η έρευνα εστιάζεται στην ανάπτυξη κρυπτογραφικών μεθόδων και πρωτοκόλλων εγκατάστασης δημοσίου κλειδιού, που υλοποιούνται με χρήση μη-Αβελιανών ομάδων.

Σε αυτό το κεφάλαιο παρουσιάζονται κρυπτογραφικά αρχέγονα τα οποία υλοποιούνται με χρήση μη-Αβελιανών ομάδων και ταυτόχρονα, δεν παρεκκλίνουν από το παράδειγμα του πρωτοκόλλου κρυπτογραφίας δημοσίου κλειδιού το οποίο βασίζεται στην έννοια της μονόδρομης συνάρτησης. Αρχικά, παρουσιάζονται πρωτόκολλα τα οποία είναι κοντά στο πνεύμα των κλασσικών πρωτοκόλλων, που υλοποιούνται με χρήση Αβελιανών ομάδων. Η ταξινόμησή τους γίνεται με βάση τα αντίστοιχα αλγοριθμικά προβλήματα της Θεωρίας Ομάδων, τα οποία αξιοποιούνται για την κατασκευή μονόδρομων συναρτήσεων. Στη συνέχεια, παρουσιάζεται το πρωτοποριακό πρωτόκολλο Anshel-Anshel-Goldfeld, το οποίο

μπορεί να υλοποιηθεί με χρήση μίας τυχαίας μη-Αβελιανής ομάδας με επαρκώς υπολογίσιμες κανονικές μορφές, όπως για παράδειγμα, η ομάδα πλεξιδίων που παρουσιάστηκε στο 2ο κεφάλαιο.

Σε όλα τα παραδείγματα που ακολουθούν υποθέτουμε ότι η G είναι μία ομάδα με επιλύσιμο το πρόβλημα της λέξης. Για πρακτικούς λόγους υιοθετούμε τον παρακάτω συμβολισμό.

Συμβολισμός: Έστω G ομάδα και w, a δύο στοιχεία της G. Θα συμβολίζουμε με w^a το στοιχείο $a^{-1}wa$, δηλαδή το συζυγές του στοιχείου w ως προς το στοιχείο a.

4.2 Πρωτόκολλα με βάση το πρόβλημα αναζήτησης συζυγίας

Υπενθυμίζουμε ότι το *πρόβλημα της συζυγίας* είναι ένα *πρόβλημα απόφασης* για την ομάδα G και διατυπώνεται ως εξής:

Έστω G ομάδα και u, v δύο στοιχεία της G. Να εξεταστεί αν υπάρχει στοιχείο $x \in G$ τέτοιο ώστε $u^x = v$, δηλαδή αν τα στοιχεία u, v είναι συζυγή στοιχεία της G.

Αφ' ετέρου, το *πρόβλημα αναζήτησης συζυγίας* είναι ένα *πρόβλημα αναζήτησης* και διατυπώνεται ως εξής:

Έστω G ομάδα και u, v δύο στοιχεία της G. Να βρεθεί ένα στοιχείο $x \in G$ τέτοιο ώστε $u^x = v$, δεδομένου ότι υπάρχει τουλάχιστον ένα στοιχείο με αυτήν την ιδιότητα.

Το πρόβλημα της συζυγίας αποτελεί ένα θέμα που μελετάται στη Θεωρία Ομάδων. Από την άλλη μεριά, το πρόβλημα αναζήτησης συζυγίας είναι θέμα που μελετάται στη θεωρία υπολογιστικής πολυπλοκότητας και δεν αφορά τη Θεωρία Ομάδων. Αν γνωρίζουμε ότι ένα στοιχείο u είναι συζυγές ενός στοιχείου v, μπορούμε απλώς να διατρέξουμε τις λέξεις της μορφής u^x για κάθε $x \in G$ και, συγκρίνοντας κάθε αποτέλεσμα με το στοιχείο v, να αποφανθούμε για το

στοιχείο x που ικανοποιεί την εξίσωση $u^x = v$.[1]

Ωστόσο, αυτός ο στοιχειώδης αλγόριθμος απαιτεί εκθετικό χρόνο ως προς το μήκος της λέξης v και έτσι θεωρείται υπολογιστικά ανεπαρκής για πρακτικές εφαρμογές. Έτσι, αν δεν γνωρίζουμε την ύπαρξη κάποιου άλλου αλγορίθμου για την επίλυση του προβλήματος αναζήτησης συζυγίας, είναι βάσιμος ο ισχυρισμός ότι η συνάρτηση $x \mapsto u^x$ είναι μονόδρομη και, επομένως, μπορεί να χρησιμοποιηθεί ως βάση για την ανάπτυξη κρυπτογραφικού πρωτοκόλλου.

Το παρακάτω πρωτόκολλο υλοποιείται με χρήση μίας ομάδας πλεξιδίων και επινοήθηκε από τους Ko, Lee κ.α., το 2000. Τα βήματα που εμπεριέχει είναι τα εξής:

1. Δημοσιοποιείται η ομάδα G καθώς και ένα στοιχείο $w \in G$. Επίσης, δημοσιοποιούνται τα πεπερασμένα σύνολα γεννητόρων δύο υποομάδων A, B της G για τις οποίες ισχύει ότι

$$ab = ba \ \forall \ a \in A, b \in B$$

2. Ο $\mathcal{A}$ επιλέγει ένα μυστικό $a \in A$ και αποστέλλει το στοιχείο $w^a \in G$ στον $\mathcal{B}$.

3. Ο $\mathcal{B}$ επιλέγει ένα μυστικό $b \in B$ και αποστέλλει το στοιχείο $w^b \in G$ στον $\mathcal{A}$.

4. Ο $\mathcal{A}$ υπολογίζει το στοιχείο $(w^b)^a = w^{ba}$ ενώ ο $\mathcal{B}$ υπολογίζει το στοιχείο $(w^a)^b = w^{ab}$. Εφόσον $ab = ba$, οι $\mathcal{A}$ και $\mathcal{B}$ διαθέτουν πλέον ένα κοινό μυστικό κλειδί, το στοιχείο $K = w^{ab} = w^{ba}$.

Η υλοποίηση του πρωτοκόλλου μπορεί να γίνει με χρήση της ομάδας πλεξιδίων B_n, η οποία διαθέτει *μετατιθέμενες υποομάδες*, δηλαδή υποομάδες που τα στοιχεία της μίας μετατίθενται με τα στοιχεία της άλλης.

[1] Χρησιμοποιούμε, σιωπηρά, το επιχείρημα ότι μία ομάδα με επιλύσιμο το πρόβλημα της συζυγίας έχει επίσης επιλύσιμο το πρόβλημα της λέξης.

Παράδειγμα 4.2.1. *Θεωρούμε δύο ακεραίους d, u και την ομάδα πλεξιδίων B_{d+u}. Θεωρούμε επίσης τις υποομάδες $B_d =< x_1, \ldots, x_{d-1} >$ και $B_u = < x_{d+1}, \ldots, x_u >$. Τότε για κάθε $a \in B_d$ και $b \in B_u$ έχουμε ότι $ab = ba$.*

Η επιλογή μίας ομάδας που μπορεί να χρησιμοποιηθεί ως μοντέλο για την ανάπτυξη αυτού του πρωτοκόλλου θα πρέπει να γίνει έτσι ώστε να πληρούνται οι εξής προϋποθέσεις:

(Π0) Η ομάδα πρέπει να είναι γνωστή. Ειδικότερα, το πρόβλημα αναζήτησης συζυγίας στην ομάδα θα πρέπει να έχει μελετηθεί καλά ή να ανάγεται σε κάποιο άλλο γνωστό πρόβλημα.

Η προϋπόθεση (Π0) είναι θεμελιώδης για τη χρήση του πρωτοκόλλου σε πρακτικές εφαρμογές και περιορίζει, ήδη, σε κάποιο βαθμό τις διαθέσιμες επιλογές.

(Π1) Το πρόβλημα της λέξης για την ομάδα G πρέπει να είναι επιλύσιμο μέσω ενός επαρκώς γρήγορου αλγορίθμου (γραμμικής ή τετραγωνικής τάξης). Η ύπαρξη επαρκώς υπολογίσιμης κανονικής μορφής για τα στοιχεία της G αποτελεί προτέρημα.

Η προϋπόθεση (Π1) είναι απαραίτητη για την αποτελεσματική εξαγωγή κλειδιών μέσω ενός πρωτοκόλλου εγκατάστασης κλειδιών καθώς και για το βήμα επαλήθευσης σε ένα πρωτόκολλο επικύρωσης.

(Π2) Το πρόβλημα αναζήτησης συζυγίας θα πρέπει να μην είναι επιλύσιμο μέσω ενός ντετερμινιστικού αλγορίθμου [2] υποεκθετικής τάξης.

Θα πρέπει να σημειωθεί ότι η απόδειξη ότι μία ομάδα G πληροί την ιδιότητα (Π2) έχει υψηλό βαθμό δυσκολίας (πρόκειται για ένα "πρόβλημα του ενός εκατομμυρίου δολαρίων"). Έτσι, η ιδιότητα (Π2) θα πρέπει να εξετάζεται σε συνδυασμό με την ιδιότητα (Π0), δηλαδή η μόνη ρεαλιστική απόδειξη για μία ομάδα G ότι πληροί την προϋπόθεση (Π2) να συνίσταται από

[2] Ένας αλγόριθμος που για μία συγκεκριμένη τιμή εισόδου δίνει πάντοτε την ίδια τιμή εξόδου, μέσω της ίδιας ακολουθίας καταστάσεων της μηχανής υπολογισμού, καλείται ντετερμινιστικός.

την επαρκή μελέτη της ομάδας (από επαρκές πλήθος ερευνητών και για επαρκές χρονικό διάστημα).

(Π3) Πρέπει να υπάρχει σαφής τρόπος διάκρισης των στοιχείων της G έτσι ώστε να είναι αδύνατη η εύρεση του στοιχείου x από το στοιχείο w^x, μέσω απλού ελέγχου.

Ένας τρόπος για την επίτευξη αυτού του σκοπού είναι η χρήση κανονικής μορφής για την παράσταση των στοιχείων της G, που σημαίνει την ύπαρξη ενός αλγορίθμου ο οποίος μετασχηματίζει μία λέξη u_{in} σε μία λέξη u_{out} έτσι ώστε $u_{in} = u_{out}$, χωρίς αυτό να διαπιστώνεται μέσω απλού ελέγχου.

(Π4) Το πλήθος των λέξεων μήκους n, με στοιχεία από την ομάδα G, θα πρέπει να αυξάνεται με ρυθμό μεγαλύτερο από οποιοδήποτε πολυώνυμο του n, π.χ. εκθετικά.

Η προϋπόθεση (Π4) είναι απαραίτητη για την αποτροπή επιθέσεων που αποσκοπούν στην πλήρη εξάντληση του χώρου των διαθέσιμων κλειδιών.

Παράδειγμα 4.2.2. *Η ομάδα πλεξιδίων B_n, με $n \geq 3$, πληροί την προϋπόθεση (Π4) καθώς έχει ελεύθερες υποομάδες. Για παράδειγμα, η υποομάδα $F_2 =< x_1^2, x_2^2 >$ είναι ελεύθερη.*

Υπάρχουν παραδείγματα ομάδων που πληρούν τις προϋποθέσεις (Π1),(Π4), πιθανώς την (Π2) και σε ικανοποιητικό βαθμό την (Π3). Πρόκειται για ομάδες στις οποίες είναι επιλύσιμο το πρόβλημα της λέξης, όχι όμως και το πρόβλημα της συζυγίας. Καθώς το πρόβλημα αναζήτησης συζυγίας δε μελετάται στη Θεωρία Ομάδων, κρίνεται χρήσιμο να επανεξεταστούν παραδείγματα ομάδων στις οποίες το πρόβλημα της συζυγίας αποδείχθηκε μη επιλύσιμο, αφού τέτοιες ομάδες πληρούν δυνητικά την προϋπόθεση (Π2) και επομένως είναι υποψήφια μοντέλα για την υλοποίηση του παραπάνω πρωτοκόλλου.

4.3 Πρωτόκολλα με βάση το πρόβλημα διάσπασης

Υπενθυμίζουμε ότι μία γενικευμένη εκδοχή του προβλήματος αναζήτησης συζυγίας αποτελεί το πρόβλημα αναζήτησης διάσπασης, που διατυπώνεται ως εξής:

Έστω G ομάδα, w, w' δύο στοιχεία της G και $A \subseteq G$. Να βρεθούν δύο στοιχεία $x, y \in A$ τέτοια ώστε $xwy = w'$, δεδομένου ότι υπάρχει τουλάχιστον ένα τέτοιο ζεύγος στοιχείων.

Παρατήρηση 4.3.1. Αν το σύνολο A είναι υποομάδα της G τότε το πρόβλημα καλείται επίσης *πρόβλημα διπλού συμπλόκου*.

Παρατήρηση 4.3.2. Παρατηρούμε ότι υπάρχει πάντοτε τουλάχιστον ένα ζεύγος στοιχείων x, y που ικανοποιούν τη σχέση $xwy = w'$, π.χ. τα $x = 1$ και $y = w^{-1}w'$. Επομένως, το ζητούμενο για τα στοιχεία x, y είναι να ανήκουν στο A. Έτσι, για να έχει νόημα το πρόβλημα, η λύση θα αναζητείται πάντοτε μεταξύ των υποομάδων της G.

Σε επόμενη παράγραφο, αποδεικνύεται ότι το πρόβλημα αναζήτησης συζυγίας στο οποίο βασίζεται το πρωτόκολλο των Ko,Lee κ.α. της παραγράφου 4.2, ανάγεται στο φαινομενικά απλούστερο πρόβλημα αναζήτησης διάσπασης. Η παρατήρηση αυτή είχε γίνει εξ αρχής, στην παρουσίαση του πρωτοκόλλου, όμως η σημασία της υποβαθμίστηκε.

Θα πρέπει να σημειωθεί ότι ενδέχεται να υπάρχουν υποσύνολα A για τα οποία δεν είναι εύκολη η επαλήθευση της συνθήκης $x, y \in A$. Το αντίστοιχο πρόβλημα είναι γνωστό και ως *πρόβλημα (αναζήτησης) μέλους*. Στην αρχική παρουσίαση του πρωτοκόλλου της παραγράφου 4.2, δεν υπήρξε πρόβλεψη για την αντιμετώπιση αυτού του προβλήματος. Αντ΄ αυτού αναφέρεται ότι μπορεί να χρησιμοποιηθεί μία μέθοδος " ωμής βίας " ώστε, διατρέχοντας τα στοιχεία του A, να επιτευχθεί η ζητούμενη συνθήκη. Όμως αυτό δεν είναι απαραίτητο σε ενδεχόμενες πρακτικότερες μορφές επιθέσεων.

Παρατηρούμε επίσης ότι το πρόβλημα αναζήτησης συζυγίας αποτελεί ειδική περίπτωση του προβλήματος διάσπασης, όπου το w' είναι συζυγές του w και

$x = y^{-1}$. Είναι διαισθητικά προφανής ο ισχυρισμός ότι το πρόβλημα αναζήτησης διάσπασης είναι απλούστερο, καθώς θεωρείται, γενικά, πιο εύκολη η επίλυση μίας εξίσωσης με δύο αγνώστους σε σχέση με μία ειδική περίπτωση της ίδιας εξίσωσης, με έναν άγνωστο. Ωστόσο, υπάρχουν και εξαιρέσεις σε αυτόν το γενικό κανόνα.

Ένα τυπικό πρωτόκολλο βασισμένο στο πρόβλημα διάσπασης, μπορεί να περιγραφεί με τα εξής βήματα:

1. Δημοσιοποιούνται μία ομάδα G, ένα στοιχείο $w \in G$ και δύο υποομάδες $A, B \leq G$ τέτοιες ώστε να ισχύει

$$ab = ba \ \forall \ a \in A, b \in B$$

2. Ο $\mathcal{A}$ επιλέγει τυχαία στοιχεία $a_1, a_2 \in A$ και αποστέλλει το στοιχείο $a_1 w a_2$ στον $\mathcal{B}$.

3. Ο $\mathcal{B}$ επιλέγει τυχαία στοιχεία $b_1, b_2 \in B$ και αποστέλλει το στοιχείο $b_1 w b_2$ στον $\mathcal{A}$.

4. Ο $\mathcal{A}$ υπολογίζει το στοιχείο $K_{\mathcal{A}} = a_1 b_1 w b_2 a_2$ ενώ ο $\mathcal{B}$ υπολογίζει το στοιχείο $K_{\mathcal{B}} = b_1 a_1 w b_2 a_2$.

Εφόσον $a_i b_j = b_j a_i$ στην G έχουμε ότι $K_{\mathcal{A}} = K_{\mathcal{B}} = K$ στην G και το K είναι το κοινό μυστικό κλειδί των $\mathcal{A}$ και $\mathcal{B}$.

4.3.1 Παραλλαγή : ένα "στρεβλό" πρωτόκολλο

Το πρωτόκολλο που παρουσιάζεται παρακάτω επινοήθηκε από τους Shpilrain, Ushakov και βασίζεται σε μία γενικευμένη εκδοχή του προβλήματος αναζήτησης διάσπασης, η οποία διατυπώνεται ως εξής:

Έστω G ομάδα, A, B δύο υποομάδες της G και w, w' δύο στοιχεία της G. Να βρεθούν στοιχεία $x \in A$ και $y \in B$ τέτοια ώστε $xwy = w'$, δεδομένου ότι υπάρχει τουλάχιστον ένα τέτοιο ζεύγος στοιχείων.

Το πρωτόκολλο εμπεριέχει τα εξής βήματα:

1. Δημοσιοποιούνται μία ομάδα G, ένα στοιχείο $w \in G$ καθώς και δύο υποομάδες $A, B \leq G$ τέτοιες ώστε

$$ab = ba \ \forall \ a \in A, b \in B$$

2. Ο $\mathcal{A}$ επιλέγει τυχαία δύο μυστικά στοιχεία $a_1 \in A$,$b_1 \in B$ και αποστέλλει το στοιχείο $a_1 w b_1$ στον $\mathcal{B}$.

3. Ο $\mathcal{B}$ επιλέγει τυχαία δύο μυστικά στοιχεία $b_2 \in B$,$a_2 \in A$ και αποστέλλει το στοιχείο $b_2 w a_2$ στον $\mathcal{A}$.

4. Ο $\mathcal{A}$ υπολογίζει το στοιχείο $K_{\mathcal{A}} = a_1 b_2 w a_2 b_1 = b_2 a_1 w b_1 a_2$ ενώ ο $\mathcal{B}$ υπολογίζει το στοιχείο $K_{\mathcal{B}} = b_2 a_1 w b_1 a_2$.

Εφόσον $a_i b_j = b_j a_i$ στην G έχουμε ότι $K_{\mathcal{A}} = K_{\mathcal{B}} = K$ στην G και το K είναι το κοινό μυστικό κλειδί των $\mathcal{A}$ και $\mathcal{B}$.

Η συγκεκριμένη παραλλαγή του πρωτοκόλλου της παραγράφου 4.3, φαίνεται να είναι ασφαλέστερη απέναντι σε επιθέσεις κατά μήκος, εκ των αποτελεσμάτων από πειράματα που διεξήχθησαν[5].

4.4 Πρωτόκολλο με βάση το πρόβλημα αναζήτησης παραγοντοποίησης

Το πρωτόκολλο που παρουσιάζεται σε αυτήν την παράγραφο, βασίζεται στο πρόβλημα αναζήτησης παραγοντοποίησης, που υπενθυμίζουμε ότι διατυπώνεται ως εξής:

Έστω G ομάδα, w στοιχείο της G και $A, B \leq G$ δύο υποομάδες της G. Να βρεθούν στοιχεία $a \in A$ και $b \in B$ τέτοια ώστε $ab = w$.

Το πρωτόκολλο υλοποιείται με τα παρακάτω βήματα:

1. Δημοσιοποιούνται μία ομάδα G καθώς και δύο υποομάδες A, B της G τέτοιες ώστε

$$ab = ba \ \forall \ a \in A, b \in B$$

2. Ο $\mathcal{A}$ επιλέγει τυχαία δύο μυστικά στοιχεία $a_1 \in A, b_1 \in B$ και αποστέλλει το στοιχείο $a_1 b_1$ στον $\mathcal{B}$.

3. Ο $\mathcal{B}$ επιλέγει τυχαία δύο μυστικά στοιχεία $a_2 \in A, b_2 \in B$ και αποστέλλει το στοιχείο $a_2 b_2$ στον $\mathcal{A}$.

4. Ο $\mathcal{A}$ υπολογίζει το στοιχείο $K_{\mathcal{A}} = b_1(a_2 b_2)a_1 = a_2 b_1 a_1 b_2 = a_2 a_1 b_1 b_2$ ενώ ο $\mathcal{B}$ υπολογίζει το στοιχείο $K_{\mathcal{B}} = a_2(a_1 b_1)b_2 = a_2 a_1 b_1 b_2$.

Εφόσον $a_i b_j = b_j a_i$ στην G έχουμε ότι $K_{\mathcal{A}} = K_{\mathcal{B}} = K$ στην G και το K είναι το κοινό μυστικό κλειδί των $\mathcal{A}$ και $\mathcal{B}$.

Παρατήρηση 4.4.1. Ένας " ωτακουστής " που γνωρίζει τα στοιχεία $a_1 b_1$ και $a_2 b_2$, προφανώς μπορεί να υπολογίσει τα στοιχεία

$$(a_1 b_1)(a_2 b_2) = a_1 b_1 a_2 b_2 = a_1 a_2 b_1 b_2$$
$$(a_2 b_2)(a_1 b_1) = a_2 a_1 b_2 b_1$$

Όμως κανένα από αυτά τα στοιχεία δεν ισούται με το K εφόσον $a_1 a_2 \neq a_2 a_1$ και $b_1 b_2 \neq b_2 b_1$ (οι υποομάδες A, B είναι μη-Αβελιανές). Εδώ, προϋποθέτουμε κατάλληλη επιλογή των a_1, a_2 (και αντίστοιχα των b_1, b_2) ώστε να εξασφαλίσουμε ότι $a_1 \neq a_2$ (αντίστοιχα $b_1 \neq b_2$).

Αξίζει να σημειωθεί ότι το πρόβλημα απόφασης παραγοντοποίησης, που θέτει το ερώτημα για την ύπαρξη παραγοντοποίησης ενός στοιχείου σε γινόμενο στοιχείων υποομάδων, αποτελεί ένα νέο, μη τετριμμένο πρόβλημα της Θεωρίας Ομάδων που προήλθε από την Κρυπτογραφία, αποδεικνύοντας έτσι την αλληλοτροφοδότηση των δύο αντικειμένων.

4.5 Σχέσεις μεταξύ των υποκειμένων προβλημάτων

Στην παράγραφο αυτή εξετάζονται οι σχέσεις μεταξύ των υποκειμένων προβλημάτων στα πρωτόκολλα τα οποία παρουσιάστηκαν.

Αναφορικά με το πρωτόκολλο των Ko,Lee κ.α. που περιγράφηκε στην παράγραφο 4.2, παρατηρούμε τα εξής:

Ο $\mathcal{A}$ επιλέγει ένα μυστικό στοιχείο $a \in A$ και αποστέλλει το στοιχείο w^a στον $\mathcal{B}$. Αντίστοιχα, ο $\mathcal{B}$ επιλέγει ένα μυστικό στοιχείο $b \in B$ και αποστέλλει το στοιχείο w^b στον $\mathcal{A}$. Για τις υποομάδες A, B γνωρίζουμε ότι ισχύει $ab = ba$ για κάθε $a \in A, b \in B$.

Υποθέτουμε ότι ένας επιτιθέμενος εντοπίζει στοιχεία $a_1, a_2 \in A$ τέτοια ώστε $a_1 w a_2 = a^{-1} w a$ καθώς και στοιχεία $b_1, b_2 \in B$ τέτοια ώστε $b_1 w b_2 = b^{-1} w b$. Τότε, μπορεί να υπολογίσει το στοιχείο:

$$a_1 b_1 w b_2 a_2 = a_1 b^{-1} w b a_2 = b^{-1} a_1 w a_2 b = b^{-1} a^{-1} w a b = K$$

δηλαδή το κοινό μυστικό κλειδί των $\mathcal{A}$ και $\mathcal{B}$. Θα πρέπει να υπογραμμιστεί ότι τα στοιχεία a_1, a_2 και b_1, b_2 δε συσχετίζονται με τα μυστικά στοιχεία a και b, που επιλέγονται από τους $\mathcal{A}$ και $\mathcal{B}$, και έτσι η αναζήτησή τους απλοποιείται ουσιωδώς.

Θα πρέπει επίσης να επισημανθεί ότι αρκεί για τον επιτιθέμενο να εντοπίσει μόνο ένα ζεύγος στοιχείων $a_1, a_2 \in A$, ώστε να υπολογίσει το κοινό μυστικό κλειδί, αφού:

$$a_1 (b^{-1} w b) a_2 = b^{-1} a_1 w a_2 b = b^{-1} a^{-1} w a b = K$$

Συνοψίζοντας τα παραπάνω, συμπεραίνουμε ότι για να υπολογίσει ένας επιτιθέμενος το κοινό μυστικό κλειδί K, δεν απαιτείται η επίλυση του προβλήματος αναζήτησης συζυγίας, καθώς αρκεί μία λύση στο, φαινομενικά απλούστερο, πρόβλημα αναζήτησης διάσπασης, που διατυπώθηκε στην παράγραφο 4.3.

Σχετικά με το πρωτόκολλο των Shpilrain, Ushakov που παρουσιάστηκε στην παράγραφο 4.3.1, παρατηρούμε ότι ένας επιτιθέμενος μπορεί να ακολουθήσει την εξής προσέγγιση:

Έστω $w' = awb$. Πολλαπλασιάζοντας από αριστερά με το γνωστό στοιχείο w^{-1} (δηλαδή το αντίστροφο του δημοσιοποιημένου στοιχείου w) έχουμε το στοιχείο $w'' = w^{-1} awb = (w^{-1} aw)b$.

Αν συμβολίσουμε με A^w την υποομάδα των συζυγών, ως προς το w, στοιχείων του A, παρατηρούμε ότι ο επιτιθέμενος καλείται πλέον να επιλύσει ένα πρόβλημα αναζήτησης παραγοντοποίησης στις υποομάδες A^w και B.

Στην αρχική παρουσίαση του πρωτοκόλλου Ko,Lee κ.α. η υλοποίηση γίνεται με χρήση μίας μόνο υποομάδας, δηλαδή ισχύει ότι $A = B$. Αν η υποομάδα A είναι κανονική, τότε έχουμε ότι $A^w = A$ και το πρόβλημα αναζήτησης παραγοντοποίησης μετασχηματίζεται ως εξής:

Έστω $w' \in A$. Να βρεθούν στοιχεία $a_1, a_2 \in A$ τέτοια ώστε $w' = a_1 a_2$.

Το παραπάνω πρόβλημα είναι τετριμμένο, αφού για τυχόν $a_1 \in A$ μπορούμε να θέσουμε $a_2 = a_1^{-1} w'$. Επομένως, για την ασφαλέστερη υλοποίηση των πρωτοκόλλων που περιγράφονται στις παραγράφους 4.2 και 4.3, θα πρέπει να αποφευχθεί η επιλογή κανονικών υποομάδων.

Μία διαφορετική στρατηγική επίθεσης σε ένα πρωτόκολλο που βασίζεται στο πρόβλημα αναζήτησης διάσπασης μπορεί να υλοποιηθεί μέσω ενός τεχνάσματος, με το οποίο γίνεται αναγωγή στο πρόβλημα αναζήτησης συζυγίας.

Έστω G ομάδα και $w' = awb$ ένα στοιχείο της G. Ο επιτιθέμενος καλείται να εντοπίσει τα στοιχεία $a \in A$ και $b \in B$, όπου A, B είναι μετατιθέμενες υποομάδες της G. Ο επιτιθέμενος επιλέγει τυχαία ένα $b_1 \in B$ και υπολογίζει το στοιχείο:

$$[awb, b_1] = b^{-1}w^{-1}a^{-1}b_1^{-1}awbb_1 = b^{-1}w^{-1}b_1^{-1}wbb_1 = (b_1^{-1})^{wb}b_1 = ((b_1^{-1})^w)^b b_1$$

Εφόσον ο επιτιθέμενος γνωρίζει το στοιχείο b_1, μπορεί να πολλαπλασιάσει το στοιχείο $((b_1^{-1})^w)^b b_1$ με το b_1^{-1} από δεξιά, προκειμένου να λάβει το στοιχείο $w'' = ((b_1^{-1})^w)^b$.

Το πρόβλημα πλέον μετασχηματίζεται στο εξής:

Να βρεθεί το στοιχείο $b \in B$ από τα στοιχεία $w'' = ((b_1^{-1})^w)^b$ και $(b_1^{-1})^w$.

Όμοια, για τον εντοπισμό του στοιχείου $a \in A$, ο επιτιθέμενος επιλέγει ένα στοιχείο $a_1 \in A$ και υπολογίζει το στοιχείο:

$$[(awb)^{-1},(a_1)^{-1}] = awba_1b^{-1}w^{-1}a^{-1}a_1^{-1} = awa_1w^{-1}a^{-1}a_1^{-1} = (a_1)^{w^{-1}a^{-1}}a_1^{-1} = ((a_1)^{w^{-1}})^{a^{-1}}a_1^{-1}$$

Πολλαπλασιάζοντας από δεξιά με το γνωστό στοιχείο a_1, ο επιτιθέμενος λαμβάνει το στοιχείο $w''' = ((a_1)^{w^{-1}})^{a^{-1}}$ και το πρόβλημα μετασχηματίζεται στο εξής:

Να βρεθεί το στοιχείο $a \in A$ *από τα στοιχεία* $w''' = ((a_1)^{w^{-1}})^{a^{-1}}$ *και* $(a_1)^{w^{-1}}$.

Δεδομένου ότι μία λύση του προβλήματος αναζήτησης συζυγίας δεν είναι κατ΄ ανάγκη μοναδική, η επίλυση των δύο επί μέρους προβλημάτων που προέκυψαν δεν οδηγεί απαραίτητα στη σωστή λύση του αρχικού προβλήματος διάσπασης. Ωστόσο, για $b' \in B$ τέτοιο ώστε $w'' = ((b_1^{-1})^w)^{b'}$ και $b'' \in B$ τέτοιο ώστε $w'' = ((b_1^{-1})^w)^{b''}$ έχουμε ότι:

$$\begin{gathered} b'^{-1}(b_1^{-1})^w b' = w'' = b''^{-1}(b_1^{-1})^w b'' \Rightarrow \\ (b_1^{-1})^w b' = b'b''^{-1}(b_1^{-1})^w b'' \Rightarrow \\ b' = ((b_1^{-1})^w)^{-1}b'b''^{-1}(b_1^{-1})^w b'' \Rightarrow \\ b'b''^{-1} = ((b_1^{-1})^w)^{-1}b'b''^{-1}(b_1^{-1})^w \Rightarrow \\ b'b''^{-1} \in C_G((b_1^{-1})^w) \Rightarrow \\ b'b''^{-1} = c \ , \ \ c \in C_G((b_1^{-1})^w) \end{gathered}$$

Δηλαδή, δύο διαφορετικές λύσεις του πρώτου προβλήματος αναζήτησης συζυγίας συνδέονται μέσω ενός στοιχείου της κεντροποιούσας του $(b_1^{-1})^w$. Όμως, η κεντροποιούσα του στοιχείου $(b_1^{-1})^w$ ενδέχεται να έχει τετριμμένη τομή με την υποομάδα B.

Χρησιμοποιώντας το ίδιο τέχνασμα, ένας επιτιθέμενος μπορεί επίσης να μετασχηματίσει το πρόβλημα αναζήτησης παραγοντοποίησης στο πρόβλημα αναζήτησης συζυγίας, κάνοντας τους σχετικούς υπολογισμούς:

Ο επιτιθέμενος επιλέγει ένα στοιχείο $b_1 \in B$ και υπολογίζει το στοιχείο

$$[ab,b_1] = b^{-1}a^{-1}b_1^{-1}abb_1 = (b_1^{-1})^b b_1$$

Εφόσον ο επιτιθέμενος γνωρίζει το στοιχείο b_1 μπορεί να πολλαπλασιάσει το παραπάνω στοιχείο με το b_1^{-1} από δεξιά και να λάβει το στοιχείο $w'' = (b_1^{-1})^b$. Έτσι, το πρόβλημα μετασχηματίζεται σε πρόβλημα αναζήτησης συζυγίας οπότε, επιλύοντάς το, ο επιτιθέμενος μπορεί να εντοπίσει το μυστικό στοιχείο $b \in B$.

Με το ίδιο ακριβώς τέχνασμα μπορεί να αντιμετωπιστεί και το ίδιο το πρόβλημα αναζήτησης συζυγίας. Έστω $w' = a^{-1}wa$. Ο επιτιθέμενος αναζητεί το στοιχείο $a \in A$ και για τον εντοπισμό του επιλέγει τυχαία ένα b από την κεντροποιούσα του A. Ειδικότερα, το στοιχείο b μπορεί να επιλέγει από τη δημοσιοποιημένη υποομάδα B, της οποίας τα στοιχεία μετατίθενται με τα στοιχεία της A. Στη συνέχεια, ο επιτιθέμενος υπολογίζει το στοιχείο:

$$[w', b] = [a^{-1}wa, b] = a^{-1}w^{-1}ab^{-1}a^{-1}wab = a^{-1}w^{-1}b^{-1}wab = (b^{-w})^a b$$

Πολλαπλασιάζοντας από δεξιά με το γνωστό στοιχείο b^{-1} ο επιτιθέμενος λαμβάνει το στοιχείο $(b^{-w})^a$ και πλέον το πρόβλημα μετασχηματίζεται σε πρόβλημα αναζήτησης συζυγίας για το στοιχείο b^{-w}. Το πρόβλημα ενδέχεται να είναι πλέον πιο εύκολο από το αρχικό, λόγω της ευελιξίας στην επιλογή του στοιχείου $b \in B$. Ειδικότερα, μία εφικτή επίθεση μπορεί να υλοποιηθεί με επιλογή διαφόρων στοιχείων $b \in B$. Με παράλληλες δοκιμές για καθένα από αυτά, εξετάζεται αν ταυτόχρονα επιλύεται το μετασχηματισμένο πρόβλημα, μέσω μίας γενικής μεθόδου (π.χ. επίθεση μήκους). Οι πιθανότητες συνηγορούν υπέρ της επιτυχίας της επίθεσης, για τουλάχιστον ένα $b \in B$.

4.6 Το πρωτόκολλο Anshel-Anshel-Goldfeld

Ιδιαίτερη αναφορά αξίζει το πρωτόκολλο Anshel-Anshel-Goldfeld το οποίο αποτελεί ένα πρωτόκολλο εγκατάστασης κλειδιού που υλοποιείται με χρήση μίας τυχαίας μη-Αβελιανής ομάδας με επιλύσιμο το πρόβλημα της λέξης. Η ουσιώδης διαφορά του από τα άλλα πρωτόκολλα που παρουσιάστηκαν είναι ότι δεν προϋποθέτει την ύπαρξη μετατιθέμενων υποομάδων της αρχικής ομάδας. Το πρωτόκολλο εμπεριέχει τα παρακάτω βήματα.

1. Δημοσιοποιούνται μία ομάδα G και στοιχεία $a_1, \ldots, a_k, b_1, \ldots, b_m \in G$.

2. Ο $\mathcal{A}$ επιλέγει ένα μυστικό $x \in G$ που είναι λέξη των $a_1, \ldots, a_k$ (δηλαδή $x = x(a_1, \ldots, a_k)$) και αποστέλλει τα στοιχεία $b_1^x, \ldots, b_m^x$ στον $\mathcal{B}$.

3. Ο $\mathcal{B}$ επιλέγει ένα μυστικό $y \in G$ που είναι λέξη των $b_1, \ldots, b_m$ και αποστέλλει τα στοιχεία $a_1^y, \ldots, a_k^y$ στον $\mathcal{A}$.

4. Ο $\mathcal{A}$ υπολογίζει το στοιχείο $x(a_1^y, \ldots, a_k^y) = x^y = y^{-1}xy$ ενώ ο $\mathcal{B}$ υπολογίζει το στοιχείο $y(b_1^x, \ldots, b_m^x) = y^x = x^{-1}yx$.

5. Ο $\mathcal{A}$ πολλαπλασιάζει το στοιχείο $y^{-1}xy$ με το x^{-1} από αριστερά, ενώ ο $\mathcal{B}$ πολλαπλασιάζει το στοιχείο $x^{-1}yx$ με το y^{-1} από αριστερά και στη συνέχεια υπολογίζει το αντίστροφο $(y^{-1}x^{-1}yx)^{-1} = x^{-1}y^{-1}xy$.

Οι $\mathcal{A}$,$\mathcal{B}$ διαθέτουν πλέον ένα κοινό μυστικό κλειδί, το στοιχείο:

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

Εκ πρώτης όψεως φαίνεται πως ένας επιτιθέμενος μπορεί να υπολογίσει το μυστικό κλειδί επιλύοντας ταυτόχρονα τα προβλήματα αναζήτησης συζυγίας των στοιχείων $b_1^x, \ldots, b_m^x, a_1^y, \ldots, a_k^y$ στην G. Ωστόσο, στο βήμα 4 του πρωτοκόλλου είναι σαφές ότι ο επιτιθέμενος θα πρέπει να γνωρίζει το στοιχείο x (αντίστοιχα το στοιχείο y), όχι ως λέξη των γεννητόρων της G, αλλά ως λέξη των στοιχείων $a_1, \ldots, a_k$ (αντίστοιχα των στοιχείων $b_1, \ldots, b_m$). Διαφορετικά, είναι αδύνατη η εύρεση του στοιχείου x^y από τα στοιχεία $a_1^y, \ldots, a_k^y$. Με άλλα λόγια, ο επιτιθέμενος θα πρέπει επίσης να επιλύσει το πρόβλημα αναζήτησης ιδιότητας μέλους, που διατυπώνεται ως εξής:

Έστω G ομάδα και $x, a_1, \ldots, a_k$ στοιχεία της G. Να βρεθεί έκφραση του στοιχείου x ως λέξη των $a_1, \ldots, a_k$.

Το αντίστοιχο πρόβλημα απόφασης για την ιδιότητα μέλους διατυπώνεται ως εξής:

Έστω G ομάδα και $x, a_1, \ldots, a_k$ στοιχεία της G. Να εξεταστεί αν ισχύει ότι $x \in < a_1, \ldots, a_k >$.

Σε πολλά παραδείγματα ομάδων, το πρόβλημα αυτό παρουσιάζει σημαντική δυσκολία ως προς την επίλυσή του. Για παράδειγμα, στην ομάδα πλεξιδίων B_n το πρόβλημα είναι μη επιλύσιμο, για $n \geq 6$, καθώς μία τέτοια ομάδα πλεξιδίων περιέχει υποομάδες ισόμορφες με το γινόμενο $F_2 \times F_2$, όπου F_2 η ελεύθερη ομάδα επί ενός συνόλου με πληθάριθμο 2 (π.χ. $F_2 \times F_2 =< x_1^2, x_2^2, x_4^2, x_5^2 >$). Σε μία ομάδα $F_2 \times F_2$ το πρόβλημα απόφασης για την ιδιότητα μέλους έχει αποδειχθεί μη επιλύσιμο αλγοριθμικά, από την K.A.Mihailova, το 1958.

Παρατηρούμε επίσης ότι αν ο επιτιθέμενος εντοπίσει κάποιο στοιχείο $x' \in G$ τέτοιο ώστε $b_1^x = b_1^{x'}, \ldots, b_m^x = b_m^{x'}$ αυτό δε 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 της κεντροποιούσας του συνόλου των b_i. Τότε έχουμε ότι $b_i^x = b_i^{x'}$ για κάθε i, επομένως $b^x = b^{x'}$ για κάθε στοιχείο b της υποομάδας που παράγεται από τα b_i, για $1 \leq i \leq m$. Ειδικότερα, $y^x = y^{x'}$.

Όμως, αν το στοιχείο x' (αντίστοιχα το στοιχείο y') δεν ανήκει στην υποομάδα $A =< a_1, \ldots, a_k >$ (αντίστοιχα στην υποομάδα $B =< b_1, \ldots, b_m >$) τότε ο επιτιθέμενος ενδέχεται να μην εντοπίσει το σωστό μυστικό κλειδί K. Από την άλλη μεριά, αν το στοιχείο x' (αντίστοιχα το στοιχείο y') ανήκει στην υποομάδα A (αντίστοιχα στην υποομάδα B) τότε ο επιτιθέμενος θα μπορούσε, υπό προϋποθέσεις, να εντοπίσει το σωστό μυστικό κλειδί K ακόμα και αν τα στοιχεία x', y' είναι διαφορετικά από τα x, y, αντιστοίχως. Πράγματι, έστω ότι $x' = c_b x, y' = c_a y$ όπου c_b είναι στοιχείο της κεντροποιούσας του συνόλου B και c_a στοιχείο της κεντροποιούσας του συνόλου A. Τότε έχουμε ότι:

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

εφόσον ισχύουν τα παρακάτω:

$c_b y = y c_b$ (αφού $y \in B =< b_1, \ldots, b_m >$)

$c_b c_a = c_a c_b$ (διότι $c_a \in B$, αφού $y' = c_a y \in B$ και όμοια έχουμε ότι $c_b \in A$)

$c_a x = x c_a$ (αφού $x \in A =< a_1, \ldots, a_k >$)

Θα πρέπει να υπογραμμιστεί ότι ο επιτιθέμενος μπορεί να εντοπίσει το σωστό μυστικό κλειδί K *αν και μόνο αν* τα στοιχεία c_b, c_a μετατίθενται. Ο μόνος εμφανής τρόπος για την εξασφάλιση αυτής της προϋπόθεσης είναι η κατάλληλη επιλογή των x', y' έτσι ώστε να ισχύει $x' \in A$ και $y' \in B$. Χωρίς επαλήθευση τουλάχιστον της μίας από αυτές τις δύο συνθήκες δε φαίνεται να υπάρχει τρόπος εξασφάλισης της ορθότητας του κλειδιού που εντοπίστηκε.

Επομένως, αν ένας επιτιθέμενος επιλέξει να επιλύσει το πρόβλημα αναζήτησης συζυγίας στην ομάδα G ώστε να εντοπίσει τα στοιχεία x, y θα πρέπει στη συνέχεια να αντιμετωπίσει είτε το πρόβλημα αναζήτησης της ιδιότητας μέλους ή το πρόβλημα απόφασης για την ιδιότητα μέλους. Όπως αναφέρθηκε στο παράδειγμα της ομάδας πλεξιδίων, το πρόβλημα απόφασης για την ιδιότητα μέλους ενδέχεται να μην επιλύεται αλγοριθμικά σε μία δεδομένη ομάδα. Τελικά, ο επιτιθέμενος θα πρέπει να επιλύσει μία δύσκολη εκδοχή του προβλήματος αναζήτησης συζυγίας, η οποία διατυπώνεται ως εξής:

Έστω G ομάδα, $A \leq G$ υποομάδα της G και $g, h \in G$ στοιχεία της G. Να βρεθεί στοιχείο $x \in A$ τέτοιο ώστε $h = x^{-1}gx$, δεδομένου ότι υπάρχει τουλάχιστον ένα τέτοιο x.

Οι παραπάνω διαπιστώσεις δεν αφορούν ευρετικές επιθέσεις στο πρωτόκολλο Anshel-Anshel-Goldfeld, όπως έχουν προταθεί από διάφορους ερευνητές. Οι επιθέσεις αυτού του είδους βασίζονται σε ευρετικούς αλγόριθμους "αναζήτησης γειτονίας" και αποσκοπούν στην εύρεση μίας λύσης για μία δεδομένη εξίσωση (ή ένα σύστημα εξισώσεων) που εκφράζεται ως λέξη των δημοσιοποιημένων στοιχείων.

Συμπερασματικά, ακόμα και αν βρεθεί ένας γρήγορος (πολυωνυμικής τάξης) ντετερμινιστικός αλγόριθμος για την επίλυση του προβλήματος της συζυγίας στις ομάδες πλεξιδίων, δε θα επαρκεί για την παραβίαση του πρωτοκόλλου Anshel-Anshel-Goldfeld μέσω μίας ντετερμινιστικής επίθεσης.

Επίλογος

Εν είδει επιλόγου, θα ήταν χρήσιμο να αναφέρουμε μερικά πιθανά θέματα για περαιτέρω έρευνα στο αντικείμενο της Κρυπτογραφίας.

Οι προϋποθέσεις που απαιτούνται για μία υποψήφια ομάδα-μοντέλο για την ανάπτυξη κρυπτογραφικών πρωτοκόλλων (όπως παρουσιάστηκαν στο κεφάλαιο 4, παράγραφος 4.2) καλύπτονται από αρκετές κλάσεις ομάδων, όπως η ομάδα του Thompson, οι ομάδες πινάκων, οι επιλύσιμες ομάδες κ.α. Με κατάλληλα στοχευμένη έρευνα και αξιολόγηση των σχετικών δοκιμών, πιθανώς ένα από τα παραπάνω μοντέλα ομάδων να αποδειχθεί περισσότερο αξιόπιστο ως προς την ασφάλεια των κρυπτογραφικών πρωτοκόλλων, σε σχέση με το παράδειγμα της ομάδας πλεξιδίων που παρουσιάστηκε.

Σημαντική θα ήταν επίσης η έρευνα σε θέματα υπολογιστικής πολυπλοκότητας των αλγορίθμων με τους οποίους υλοποιούνται τα κρυπτογραφικά πρωτόκολλα. Η επάρκεια, η ταχύτητα και η ευρωστία των αλγορίθμων υλοποίησης αποτελούν τους πλέον καθοριστικούς παράγοντες για την επιτυχή ολοκλήρωση μίας πλατφόρμας λογισμικού, πριν τη διάθεσή της για ευρεία χρήση.

Καθώς η έννοια της ασφάλειας παραμένει η υψηλότερη απαίτηση από ένα κρυπτογραφικό πρωτόκολλο, είναι σαφές ότι θα συνεχιστούν οι προσπάθειες για τη μαθηματική θεμελίωση των προτύπων ασφάλειας, για τα πρωτόκολλα που βασίζονται στη χρήση άπειρων ομάδων. Η συνεισφορά άλλων πεδίων των μαθηματικών - όπως η Θεωρία Μέτρου, η Θεωρία Πιθανοτήτων και η Στατιστική - μπορεί να αποδειχθεί πολύτιμη για την επίτευξη αυτού του στόχου.

Η παρούσα εργασία γράφτηκε στο σύστημα LaTeX με το πρόγραμμα Kile, σε περιβάλλον KDE βασισμένο σε Arch Linux. Τα σχήματα της εργασίας έγιναν με το πακέτο TiKZ, ενώ τα σχήματα των πλεξιδίων έγιναν με το πακέτο Braids.

Ευχαριστίες

Θα ήθελα να εκφράσω τις ευχαριστίες μου σε όσους συνέβαλαν καθοριστικά στη διαμόρφωση της μαθηματικής παιδείας μου.

Στους Δασκάλους μου: Σπύρο Αργυρό, Δημήτρη Βάρσο, Ευστάθιο Βασιλείου, Απόστολο Γιαννόπουλο, Σπύρο Ζαφειρόπουλο, Βασίλη Ιωάννου, Αριστείδη Κατάβολο, Γιώργο Κουμουλλή, Μιχάλη Μαλιάκα, Παναγιώτη Παυλάκο, Ευάγγελο Ράπτη, Αθανάσιο Τσαρπαλιά.

Στους συναδέλφους μου: Λεωνίδα Αρτόπουλο, Κατερίνα Δανιήλ, Λεωνίδα Θεοδώρου, Παναγιώτα Μπίρμπα, Βασιλική Παναγάκου, Αλκαίο Σουγιούλ, καθώς και στον αγαπητό Στάθη.

Επίσης, θα ήθελα να ευχαριστήσω ιδιαιτέρως αυτούς που συμπαραστάθηκαν στη διαδρομή μου.

Τους γονείς μου: Αριστοτέλη Ζαμπετάκη και Ευαγγελία Καπετάνου.

Τον αδερφό μου: Γιάννη Ζαμπετάκη.

Το **Λίνο Κουντουρά**.

Τους φίλους μου: Δημήτρη Γιαννακόπουλο, Μυρτώ Ιωάννου, Αντώνη Καλαμούτσο & Ράνια Πάλλα, Ελένη Λάσκαρη & Μίνω Πανάγο.

Τον **Πατέρα Γεννάδιο**.

Και, ειδικότερα, την **Αγγελική**, για την έμπνευση που προσφέρει στη ζωή μου.

Βιβλιογραφία

[1] Pierre Antoine Grillet, *"Abstract Algebra"*, Springer, 2007.

[2] Derek Robinson, *"A course in the theory of groups"*, Springer, 1996.

[3] Roger Lyndon, Paul Schupp, *"Combinatorial Group Theory"*, Springer-Verlag, 1977.

[4] Wilhelm Magnus, Abraham Karass, Donald Solitar, *"Combinatorial Group Theory"*, Dover, 1976.

[5] Alexei Myasnikov, Vladimir Shpilrain, Alexander Ushakov, *"Group-based cryptography"*, Birkhäuser Verlag, 2008.

[6] Christian Kassel, Vladimir Turaev, *"Braid Groups"*, Springer, 2008.

[7] David Garber, *"Braid Group Cryptography"*, arXiv:0711.3941v2, 2008.

[8] Patrick Dehornoy, Ivan Dynnikov, Dale Rolfsen, Bert Wiest, *"Why are braids orderable?"*, Société Mathématique de France, 2002.

[9] David Epstein, James Cannon, Derek Holt, Silvio Levy, Michael Paterson, William Thurston, *"Word processing in groups"*, Jones and Bartlett Publishers, 1992.

[10] Stephen Bigelow, *"Braid groups are linear"*, Journal of the American Mathematical Society 14, pp. 471- 486, 2001.

[11] Daan Krammer, *"Braid groups are linear"*, Annals of Mathematics 155 pp. 131-156, 2002.

[12] Ping Zhu, Qiaoyan Wen, *"Affine braid groups: a better platform than braid groups for cryptology?"*, Applicable Algebra in Engineering, Communication and Computing Volume 22 Issue 5-6 pp. 375-391, Springer, 2011.

[13] Alfred Menezes, Paul van Oorschot, Scott Vanstone, *"Handbook of applied cryptography"*, CRC Press, 1996.

[14] David Kahn, *"The codebreakers"*, Scribner, 1996.

[15] John Talbot, Dominic Welsh, *"Complexity and cryptography : an introduction"*, Cambridge University Press, 2006.

[16] Paul Garrett, *"Making, breaking codes : introduction to Cryptology"*, Prentice Hall, 2001.

[17] Donald Davis, *"The nature and power of mathematics"*, Dover, 2004.

[18] Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Jusung Kang, Choonsik 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.

[19] Iris Anshel, Michael Anshel, Dorian Goldfeld, *"An algebraic method for public-key cryptography"*, Mathematical Research Letters 6 pp. 287-291, 1999.

[20] Hartley Rogers, *"Theory of recursive functions and effective computability"*, McGraw-Hill, 1967.

Ευρετήριο