Κρυπτογραφία και Μαθηματικά

ΣΩΤΗΡΙΟΣ Δ. ΧΑΣΑΠΗΣ
Σ. ΔΑΒΑΚΗ 19 – 18757 ΚΕΡΑΤΣΙΝΙ
ΠΕΙΡΑΙΑΣ, ΑΤΤΙΚΗ
shasapis@gmail.com

Στην εργασία αυτή παρουσιάζονται κάποιες βασικές ιδέες της κρυπτογραφίας και ειδικότερα της μη μεταθετικής κρυπτογραφίας με βάση υλοποίησης τον δακτύλιο των τυπικών δυναμοσειρών. Γίνεται λόγος για σύγχρονα κρυπτοσυστήματα και κρυπτογραφικά μοντέλα, τα οποία βασίζονται σε διάφορες περιοχές των μαθηματικών. Κύριος στόχος της εργασίας είναι η διερεύνηση της αξιοποίησης των θεωρητικών μαθηματικών, συγκεκριμένα της θεωρίας ομάδων, στην ανάπτυξη μοντέλων κρυπτογράφησης ως εφαρμογής των μαθηματικών. Σ' αυτό το πλαίσιο παρουσιάζεται μία απλουστευμένη εφαρμογή της μεθόδου προσαρμοσμένη σε λυκειακό γνωστικό επίπεδο (πολυώνυμα και ταυτότητες). Τελικά, χρησιμοποιείται ένας κλάδος της κρυπτογραφίας ως μία συμβολή στα αναλυτικά προγράμματα των μαθηματικών στο πλαίσιο καθημερινών εφαρμογών τους.

Εισαγωγή – Σύντομη ιστορική αναδρομή

Εισαγωγή – Βασικές έννοιες

Πριν από χιλιετίες πρωτοεμφανίστηκε το πρόβλημα της κρυπτογράφησης ενός μυστικού μηνύματος σε έναν κώδικα και με τέτοιο τρόπο, ώστε: α) να μπορεί να μεταφερθεί μέσω ενός συστήματος επικοινωνιών ευρείας πρόσβασης, όπως το διαδίκτυο στη σημερινή εποχή ή κάθε τύπου αγγελιοφόρος παλαιότερα και β) να αποκωδικοποιείται από τον παραλήπτη με χρήση κάποιου είδους πληροφορίας (μυστικό κλειδί) που είναι γνωστό μόνο σε αποστολέα και παραλήπτη. Το ζήτημα, λοιπόν, ήταν να βρεθεί ένα μοντέλο κρυπτογράφησης, γνωστό σε αποστολέα και παραλήπτη, ώστε να μπορούν να ανταλλάξουν πληροφορίες μέσω ενός μη ασφαλούς καναλιού επικοινωνίας.

Η Κρυπτογραφία (Cryptography) ως ελληνική λέξη ετυμολογικά προέρχεται από τις λέξεις **κρυπτός + γράφω** και αναφέρεται στη δυνατότητα να καταγράψουμε μία πληροφορία με τέτοιο τρόπο που να μην μπορεί κάποιος να την αναγνωρίσει αν δεν του δοθούν οι απαραίτητες προσβάσεις – πληροφορίες. Ως επιστήμη είναι ένας επιστημονικός κλάδος που ασχολείται με την μελέτη, την ανάπτυξη και την χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων. Ο πιο διαδεδομένος ορισμός της επιστήμης της κρυπτογραφίας στην παγκόσμια βιβλιογραφία ([1],[17]) αναφέρει : «Η κρυπτογραφία μελετά τρόπους με τους οποίους μπορούμε να μετασχηματίσουμε ένα μήνυμα σε φαινομενικά ακατάληπτη μορφή». Τέτοιοι τρόποι παρέχονται κατεξοχήν από τα μαθηματικά.

Αρχικό ή **απλό κείμενο** (**plaintext**) ονομάζεται το κείμενο, το οποίο επιθυμεί κάποιος να κρυπτογραφήσει. **Κρυπτοκείμενο** (**ciphertext**) ονομάζεται το κείμενο, το οποίο έχει κρυπτογραφηθεί μέσω κάποιου αλγορίθμου κρυπτογράφησης. **Κρυπτογράφηση (encryption)** ονομάζεται η διαδικασία μετατροπής

του αρχικού κειμένου σε κρυπτοκείμενο. Ο μετασχηματισμός του κρυπτοκειμένου σε απλό κείμενο ονομάζεται **αποκρυπτογράφηση (decryption).** Η επιπλέον πληροφορία που είναι απαραίτητη για την κρυπτογράφηση και αποκρυπτογράφηση ενός κειμένου ονομάζεται **κλειδί (key). Κρυπτανάλυση (cryptanalysis)** είναι η επιστήμη που ασχολείται με την αποκρυπτογράφηση του κρυπτοκειμένου χωρίς την κατοχή του κλειδιού, η οποία όταν είναι αποτελεσματική για ένα κρυπτοκείμενο, τότε υπάρχει **αποτυχία πρωτοκόλλου κρυπτογράφησης** (**protocol failure**), αφού βεβαίως ο στόχος της κρυπτογράφησης είναι να μην μπορεί κάποιος να κάνει την αποκρυπτογράφηση χωρίς τη γνώση του κλειδιού. **Κρυπτοσύστημα** είναι το σύνολο των διαδικασιών κρυπτογράφησης και αποκρυπτογράφησης. Σε κάθε κρυπτοσύστημα θεωρείται αποδεκτό ότι ισχύει η **αρχή Kerchoff** σύμφωνα με την οποία ο σχεδιαστής του συστήματος πρέπει να υποθέτει ότι το μόνο άγνωστο στοιχείο του κρυπτοσυστήματος είναι το κλειδί και ο στόχος κάθε εισβολέα είναι να το αποκτήσει.

Ένα κρυπτοσύστημα πρέπει να διέπεται από τις εξής βασικές αρχές ([17]) :

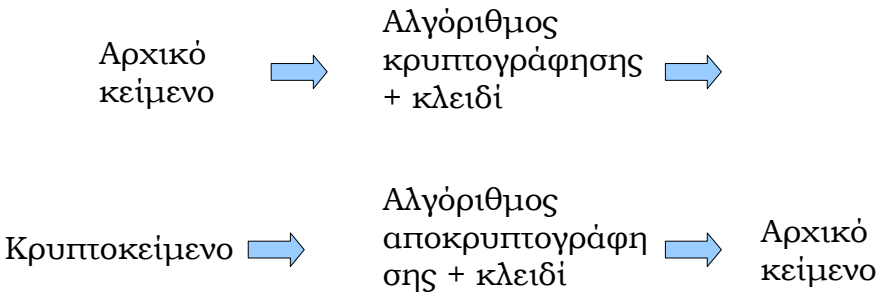
Εμπιστευτικότητα (Confidenciality): Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη. Η πληροφορία είναι ακατανόητη σε κάποιον τρίτο.

Ακεραιότητα (Data integrity): Η πληροφορία δεν μπορεί να αλλοιώνεται από μη εξουσιοδοτημένα άτομα χωρίς την ανίχνευση της αλλοίωσης.

Μη άρνηση (Non-repudiation): Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.

Πιστοποίηση (Authentication): Αποστολέας και παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητές τους καθώς και την πηγή και τον προορισμό της πληροφορίας.

Ένα τυπικό σύστημα κρυπτογράφησης μπορεί να περιγραφεί από το παρακάτω σχεδιάγραμμα :



Σύντομη ιστορική αναδρομή

Η αναγκαιότητα για κρυπτογράφηση δεδομένων εμφανίστηκε από τους αρχαίους χρόνους. Σύμφωνα με μία μικρή σφηνοειδή επιγραφή, που ανακαλύφθηκε στις όχθες του ποταμού Τίγρη, οι πολιτισμοί που αναπτύχθηκαν στην Μεσοποταμία ασχολήθηκαν με την κρυπτογραφία ήδη από το 1500 π.Χ. Η επιγραφή αυτή περιγράφει μία μέθοδο κατασκευής σμάλτων για αγγειοπλαστική και θεωρείται ως το αρχαιότερο κρυπτογραφημένο κείμενο σύμφωνα με τον Kahn [10]. Οι αρχικές προσπάθειες κρυπτογράφησης βασίζονταν σε απλά εργαλεία ή τεχνικές, γι' αυτό σήμερα εύκολα αποκρυπτογραφούνται τέτοια κρυπτογραφημένα κείμενα. Αυτό αφορά την **πρώτη περίοδο** της κρυπτογραφίας έως το 1900 μ.Χ. περίπου.

Η **δεύτερη περίοδος** της κρυπτογραφίας οριοθετείται μεταξύ των αρχών του 20ου αιώνα και φτάνει μέχρι το 1950, καλύπτοντας τους δύο παγκόσμιους πολέμους, στους οποίους οι στρατιωτικές ανάγκες για ασφαλή μετάδοση πληροφορίων συνέβαλαν ουσιαστικά στην ευρεία ανάπτυξή της. Έτσι αναπτύσσονται κρυπτοσυστήματα που απαιτούν πολλούς υπολογισμούς και στηρίζονται σε διάφορες μηχανικές κατασκευές. Για παράδειγμα οι Γερμανοί έκαναν εκτενή χρήση της κρυπτομηχανής Enigma, η οποία παραβιάστηκε από τον Marian Rejewski με χρήση **θεωρητικών μαθηματικών** το 1932. Γενικότερα, η κρυπτανάλυση των συστημάτων και αυτής της περιόδου υπήρξε επιτυχημένη.

Η **τρίτη περίοδος** της κρυπτογραφίας εκκινεί τη δεκαετία

του 1950, όταν ο Claude Shannon θεμελίωσε μαθηματικά την κρυπτογραφία και την κρυπτανάλυση. Όλα τα κρυπτοσυστήματα έως τότε βασίζονταν στη χρήση ενός κοινού κλειδιού για αποστολέα - κρυπτογράφο και παραλήπτη - αποκρυπτογράφο (κρυπτογραφία συμμετρικού κλειδιού). Η επόμενη μεγάλη συμβολή στη θεωρία της κρυπτογραφίας προήλθε από τους W. Diffie και M. Hellman στο άρθρο τους *New directions in cryptography* [7] το 1976, όπου εισάγουν την κρυπτογραφία **ασύμμετρου κλειδιού** (Asymmetric Cryptography) ή κρυπτογραφία **δημοσίου κλειδιού** (Public Key Cryptography). Η βασική ιδέα είναι ότι η κρυπτογράφηση και αποκρυπτογράφηση δε γίνονται με τη χρήση ενός κοινού κλειδιού για αποστολέα και παραλήπτη, όπως στην κρυπτογραφία συμμετρικού κλειδιού, αλλά με δύο διαφορετικά κλειδιά το **ιδιωτικό κλειδί** (**private key**) και το **δημόσιο κλειδί** (**public key**), τα οποία σχετίζονται μαθηματικά μεταξύ τους. Το ιδιωτικό κλειδί είναι διαφορετικό και κρυφό για κάθε χρήστη, ενώ το δημόσιο κλειδί γνωστό σε όλους και κοινοποιήσιμο, χρησιμοποιούνται για την κρυπτογράφηση και την αποκρυπτογράφηση αντίστοιχα, αλλά η γνώση του δημοσίου κλειδιού δεν επιτρέπει πρακτικά την εύρεση του ιδιωτικού κλειδιού κρυπτογράφησης. Κατ' αυτόν τον τρόπο λύνεται το βασικό πρόβλημα της κρυπτογράφησης συμμετρικού κλειδιού που είναι ο τρόπος αποστολής του κλειδιού από τον αποστολέα του μηνύματος στον παραλήπτη, ώστε να μπορέσει ο δεύτερος να αποκρυπτογραφήσει το μήνυμα. Για την κρυπτογράφηση χρησιμοποιείται μία **μονόδρομη απεικόνιση (one way function)** f, η οποία έχει την ιδιότητα να είναι πρακτικά αδύνατο να υπολογιστεί η αντίστροφή της απεικόνιση f^{-1} χωρίς τη γνώση του επιπλέον ιδιωτικού κλειδιού. Έτσι μπορεί ο καθένας που γνωρίζει το δημόσιο κλειδί να προβεί στην κρυπτογράφηση μίας πληροφορίας, αλλά είναι πρακτικά αδύνατη η αποκρυπτογράφηση χωρίς τη γνώση του ιδιωτικού κλειδιού([17],[12]). Βασικοί αλγόριθμοι που στηρίζονται σε αυτήν την ιδέα είναι των Rivest, Samir και Adleman, ο λεγόμενος **RSA**, ο οποίος χρησιμοποιείται ακόμη και σήμερα σε πλήθος εφαρμογών αλλά και ο αλγόριθμος **διακριτού λογαρίθμου**. Η αποτελεσματικότητά τους

εξαρτάται από την πολυπλοκότητα πεπερασμένων αβελιανών ομάδων.

Η μαθηματική σχέση των κλειδιών, η οποία αναφέρθηκε παραπάνω, βρίσκεται στο επίκεντρο της μελέτης πολλών μαθηματικών από διαφορετικούς κλάδους : Θεωρία αριθμών, Θεωρία ομάδων, Θεωρία ελλειπτικών καμπυλών κλπ.

Μη μεταθετική κρυπτογραφία

Η μέθοδος κρυπτογράφησης με χρήση δημοσίου κλειδιού, όπως αναφέρθηκε, είναι ευρέως διαδεδομένη και χρησιμοποιείται τις τελευταίες δεκαετίες. Η βασική απαίτηση αφορά την ασφαλή μεταφορά μίας πληροφορίας μέσω κάποιου δικτύου επικοινωνιών ελεύθερης πρόσβασης (διαδίκτυο, τηλεφωνικό δίκτυο, αγγελιοφόροι κλπ). Η κύρια ιδέα έγκειται στην κρυπτογράφηση των προς μεταφορά δεδομένων με χρήση ενός κλειδιού, το οποίο είναι γνωστό σε αποστολέα, που κρυπτογραφεί την πληροφορία και σε παραλήπτη, ο οποίος αποκρυπτογραφεί την πληροφορία. Όλες οι λύσεις του προβλήματος αυτού υποκρύπτουν την ιδέα της χρήσης προβλημάτων τα οποία επιδέχονται ακριβείς λύσεις - γνωστές σε αποστολέα και παραλήπτη - αλλά κάποιος που απλώς παρακολουθεί, ακόμα κι αν έχει όλα τα δεδομένα (σύμφωνα και με την αρχή Kerchoff), δεν δύναται να βρει αυτή τη λύση. Η χρήση των διαφόρων σχετικών μεθόδων, όπως οι αλγόριθμοι RSA ([12],[17],[1]), Diffie – Hellman [7], μέθοδοι ελλειπτικών καμπυλών, έχουν αναπτυχθεί με χρήση αβελιανών ομάδων. Αν και οι μέθοδοι αυτές παραμένουν ασφαλείς (με κατάλληλες προσαρμογές και επεκτάσεις στη διάρκεια του χρόνου) και χρησιμοποιούνται ευρέως στην καθημερινή πρακτική (για διαρκή ενημέρωση επί των σχετικών ερευνητικών εξελίξεων βλ. [9]), εντούτοις ερευνώνται νέες ιδέες που θα βελτιώνουν την αποτελεσματικότητά τους και δε θα βασίζονται σε πεπερασμένες αβελιανές ομάδες [15]. Έτσι, γίνονται προσπάθειες για την ανάπτυξη διαδικασιών κρυπτογράφησης διαφορετικής φιλοσοφίας που θα είναι ασφαλέστερες.

Η ιδέα που παρουσιάζεται εδώ στηρίζεται σε μη μεταθετικές αλγεβρικές δομές ως βάση για την κρυπτογράφηση και γενικώς καλείται **μη μεταθετική αλγεβρική κρυπτογραφία (non-commutative algebraic cryptography)**. Η πρώτη εμφάνισή της [18] είχε αρκετές ατέλειες [6]. Στην ίδια κατεύθυνση έγινε χρήση των ιδιοτήτων των ομάδων πλεξιδίων του Artin [4] με χρήση του **προβλήματος της συζυγίας (conjugacy problem)** που ώθησε στην ανάπτυξη της κρυπτογραφίας με ομάδες πλεξιδίων (βλ. [3] και [11]). Όμως αυτή τελευταία τείνει να αποδειχθεί ανεπαρκής, αφού έχουν βρεθεί σημαντικές αδυναμίες [16]. Παρόλα αυτά οι βασικές ομαδοθεωρητικές ιδέες που χρησιμοποιούνται στην κρυπτογραφία στις παραπάνω περιπτώσεις είναι σημαντικές και αυτές χρησιμοποιούνται και στη μέθοδο των Baumslag, Brukhov, Fine, Rosenberger [5] με τη βοήθεια τυπικών δυναμοσειρών, η οποία περιγράφεται παρακάτω. Η κύρια ιδέα είναι η χρήση **προβλημάτων εύρεσης (search problems)** σε άπειρες μη μεταθετικές ομάδες, τα οποία αντιστοιχούν στα κλασικά **προβλήματα απόφασης (decision problems** [13]**)** και μπορούν να αποτελούν βάση για τη δημιουργία μίας μονόδρομης απεικόνισης. Τα κλασικά προβλήματα απόφασης στη θεωρία ομάδων, όπως διατυπώθηκαν από τον Max Dehn το 1911 [14] είναι :

Πρόβλημα λέξης (**word problem**): Για μία οποιαδήποτε λέξη W στους γεννήτορες μίας ομάδας G να αποφασιστεί σε πεπερασμένο πλήθος βημάτων αν είναι το ταυτοτικό στοιχείο της ομάδας G ή διαφορετικό από αυτό.

Πρόβλημα συζυγίας (**conjugacy problem**): Για δύο τυχαίες λέξεις W_1, W_2 στους γεννήτορες της ομάδας G να αποφασιστεί αν είναι συζυγή στοιχεία της ομάδας.

Πρόβλημα ισομορφισμού (**isomorphism problem**): Αν δύο ομάδες G, H ορίζονται με διαφορετικούς γεννήτορες να αποφασιστεί σε πεπερασμένο πλήθος βημάτων αν είναι ή όχι ισόμορφες μεταξύ τους.

Παρόλο που αυτά τα προβλήματα είναι λυμένα σε κάποιες

κατηγορίες ομάδων θεωρητικά, η πολυπλοκότητα της λύσης τους πρακτικά μπορεί να επιτρέπει τη χρήση τους στην κρυπτογραφία. Τα προβλήματα εύρεσης είναι εκείνα στα οποία, γνωρίζοντας την ύπαρξη λύσης για ένα πρόβλημα απόφασης, απαιτείται η εύρεση μίας τουλάχιστον συγκεκριμένης λύσης για αυτά. Για παράδειγμα, οι **ομάδες πλεξιδίων** (**braid groups** [4]), ως βάση για μη μεταθετικά κρυπτοσυστήματα, βασίζονται στην υπόθεση ότι το πρόβλημα της λέξης αυξάνεται πολυωνυμικά καθώς ο δείκτης των πλεξιδίων B_n αυξάνεται, ενώ δε συμβαίνει το ίδιο για το πρόβλημα της συζυγίας. Έτσι, ενώ και τα δύο προβλήματα (λέξης και συζυγίας) είναι πλήρως λυμένα για ομάδες πλεξιδίων, εντούτοις υπάρχει η υπόθεση της διαφορετικότητάς τους ως προς την πολυπλοκότητα.

Μία γενίκευση του προβλήματος του διακριτού λογαρίθμου σε ομάδες [12] αποτελεί το πρόβλημα της συζυγίας : δοθέντων δύο στοιχείων α, β μίας ομάδας G να βρεθεί ένα στοιχείο $x \in G$, ώστε να ισχύει: $x\alpha x^{-1} = b$. Η υπολογιστική δυσκολία του συγκεκριμένου προβλήματος για τις ομάδες πλεξιδίων ήταν αυτή που ώθησε τη χρήση τους σε κρυπτοσυστήματα ομάδων. Εντούτοις, τελευταία φαίνεται ότι η χρήση του προβλήματος αυτού ειδικά σε ομάδες πλεξιδίων μπορεί να μην παρέχει την απαιτούμενη ασφάλεια για μία ευρεία χρήση [19]. Σήμερα η έρευνα έχει στραφεί προς δύο κατευθύνσεις. Αφενός στην αναζήτηση ενός διαφορετικού προβλήματος στη συνδυαστική θεωρία ομάδων ικανής πολυπλοκότητας, ώστε να μπορεί να αποτελέσει τη βάση ενός νέου κρυπτοσυστήματος. Αφετέρου, στη χρήση άλλων ομάδων, πλην των πλεξιδίων και διάφορων άλλων που έχουν χρησιμοποιηθεί, οι οποίες να μπορούν να αποτελέσουν ασφαλή βάση για χρήση, μέσω του προβλήματος συζυγίας, στην καθημερινή πραγματικότητα.

Έτσι, διευρύνεται διαρκώς το σύνολο των μη μεταθετικών αλγεβρικών αντικειμένων που χρησιμοποιούνται στην κρυπτογραφία με τη διερεύνηση - μεταξύ άλλων – της χρήσης και του δακτυλίου των τυπικών δυναμοσειρών $R\langle\langle x_1, \ldots, x_n \rangle\rangle$ στις μη μετατιθέμενες μεταβλητές $x_1, \ldots, x_n$ ως βάσης για την ανάπτυξη

κρυπτοσυστημάτων, όπως αυτή παρουσιάστηκε από τους Baumslag, Brukhov, Fine και Rosenberger [5]. Ειδικότερα γίνεται χρήση του **θεωρήματος αναπαράστασης του Magnus** [14] σύμφωνα με το οποίο μία πεπερασμένα παραγόμενη ελεύθερη ομάδα F έχει μία πιστή αναπαράσταση σε ένα πηλίκο του δακτυλίου των τυπικών δυναμοσειρών στις μη μετατιθέμενες μεταβλητές.

Τυπικές δυναμοσειρές και η αναπαράσταση του Magnus

Έστω ο δακτύλιος των τυπικών δυναμοσειρών ([8],[14]) επί του δακτυλίου R : $A(R,n)=R\langle\langle x_1,\ldots,x_n\rangle\rangle$. Στη συνέχεια θα χρησιμο-ποιηθεί ως δακτύλιος οι ρητοί αριθμοί $R=\mathbb{Q}$. Δηλαδή λαμβάνεται ο δακτύλιος των τυπικών δυναμοσειρών $H=\mathbb{Q}\langle\langle x_1,\ldots,x_n\rangle\rangle=A(\mathbb{Q},n)$ στις μη μετατιθέμενες μεταβλητές $x_{1,},\ldots,x_n$. Η αναπαράσταση του Magnus [14] είναι μία πιστή αναπαράσταση μίας πεπερασμένα παραγόμενης ελεύθερης ομάδας σ' ένα πηλίκο της Η. Για $n\geq 2$ υπάρχουν ελεύθερες υποομάδες κάθε διάστασης σε αυτό το πηλίκο της Η.

Η αναπαράσταση του Magnus

Θεωρούμε $\overline{H}$ το πηλίκο που προκύπτει, αν στην $H=\mathbb{Q}\langle\langle x_{1,},\ldots,x_n\rangle\rangle$ προσάψουμε τις σχέσεις : $x_1^d=x_2^d=\ldots=x_n^d=0$ για $d>1, d\in\mathbb{Z}$. Οπότε τα στοιχεία του πηλίκου $\overline{H}$ είναι πολυώνυμα βαθμού $<d$ στις μη μετατιθέμενες μεταβλητές $x_{1,}x_{2,}\ldots,x_n$. Τότε τα μονώνυμα :

$$\alpha_1=1+x_{1,}\alpha_2=1+x_{2,}\ldots,\alpha_n=1+x_n$$

δίνουν μία πιστή αναπαράσταση μίας ελεύθερης ομάδας. Στην Η έχουμε ότι: $\frac{1}{1+x_i}=1-x_i+x_i^2-x_i^3+\ldots$ (Βλ. : [14] σελ.310 κ.εξ.).

Δηλαδή κάθε α_i είναι αντιστρέψιμο στοιχείο στην Η και κατά συνέπεια στην $\overline{H}$, όπου όμως θα είναι βαθμού $<d$ και θα

έχουμε ότι :

$$\frac{1}{1+x_i}=1-x_i+x_i^2-x_i^3+\ldots+(-1)^{d-1}x_i^{d-1}$$

Συνεπώς κάθε $\alpha_i=1+x_i\in U(\overline{H})$ που είναι η ομάδα των αντιστρέψιμων στοιχείων της $\overline{H}$.

Βασική παρατήρηση: Διατηρώντας τον ακέραιο d που αποτελεί την **ορίζουσα δύναμη** μυστικό, τότε τα αντίστροφα στοιχεία παραμένουν άγνωστα.

Θεώρημα Magnus Τα στοιχεία : $\alpha_1=1+x_1,\ldots,\alpha_n=1+x_n$ παράγουν ελεύθερα μία υποομάδα της $U(\overline{H})$. Συνεπώς η απεικόνιση :

$$\begin{aligned} y_1&\to\alpha_1\\ y_2&\to\alpha_2\\ &\vdots\\ y_n&\to\alpha_n \end{aligned}$$

ορίζει μία πιστή αναπαράσταση της ελεύθερης ομάδας με γεννήτορες $y_1,\ldots,y_n$ στην $\overline{H}$. Επιπλέον ισχύει ότι: $\alpha_i^{-1}=1-x_i+x_i^2-x_i^3+\ldots+(-1)^n x_i^n+\ldots$

Μέσω αυτής προκύπτει και ο αλγόριθμος κρυπτογράφησης.

Κάθε α_i αντιστρέφεται στην $\overline{H}$ και συνεπώς $\alpha_i\in U(\overline{H})$ οπότε το σύνολο $\{\alpha_1,\ldots,\alpha_n\}$ παράγει μία πολλαπλασιαστική υποομάδα της $U(\overline{H})$.

Ισχυρισμός: Καμία μη τετριμμένη ελεύθερα παραγόμενη ανηγμένη λέξη στα α_i δεν μπορεί να είναι η μονάδα και κατά συνέπεια η παραγόμενη από αυτά υποομάδα πρέπει να είναι μία ελεύθερη ομάδα.

Από το διωνυμικό ανάπτυγμα $(\alpha+\beta)^n=\sum_{k=0}^{n}\frac{n!}{k!(n-k)!}\alpha^{n-k}\beta^k$ για $n\in\mathbb{Z},n\neq 0$ και θέτοντας $\alpha=1,\beta=\alpha_i$ ισχύει :

$$(1+\alpha_i)^n=\sum_{k=0}^{n}\binom{n}{k}1^{n-k}\alpha_i^k=\sum_{k=0}^{n}\binom{n}{k}\alpha_i^k=\binom{n}{0}\alpha_i^0+\binom{n}{1}\alpha_i^1+\binom{n}{2}\alpha_i^2+\ldots\Rightarrow$$

$$(1+\alpha_i)^n=1+n\alpha_i+\textit{όροι μεγαλύτερου βαθμού}\quad .$$

Έστω $W(\alpha_{1,}\alpha_{2,}\ldots,\alpha_n)=\alpha_{i_1}^{n_1}\alpha_{i_2}^{n_2}\ldots\alpha_{i_k}^{n_k}$ μία ανηγμένη ελεύθερα παραγόμενη λέξη στα α_ι με $|n_i|\geq 1$ και $\alpha_{i_j}\neq\alpha_{i_{j+1}}$, για $j=1,\ldots,k-1$.

Ονομάζουμε τον αριθμό k **μήκος λέξης**.

Τότε:

$$W(\alpha_{1,}\alpha_{2,}\ldots,\alpha_n)=$$
$$(1+x_{i_1})^{n_1}\ldots(1+x_{i_k})^{n_k}=$$
$$(1+n_1x_{i_1}+\ldots\textit{Δυνάμεις του}\,x_{i_1})\ldots(1+n_kx_{i_k}+\ldots\textit{Δυνάμεις του}\,x_{i_k})$$

Σε αυτήν την παράσταση εμφανίζεται το μονώνυμο: $(n_1n_2\ldots n_k)(x_{i_1}x_{i_2}\ldots x_{i_k})$ το οποίο δεν απλοποιείται εφόσον δεν μετατίθενται οι μεταβλητές x_i μεταξύ τους. Αυτό το μονώνυμο είναι και το μεγίστου μήκους k μονώνυμο. Εφόσον κάθε $n_i\neq 0$ αυτός ο όρος πράγματι υπάρχει και συνεπώς η αρχική λέξη $W(\alpha_{1,}\alpha_{2,}\ldots,\alpha_n)$ δεν είναι τετριμμένη. Συνεπώς, πράγματι η παραγόμενη ομάδα από τα $\alpha_{1,}\alpha_{2,}\ldots,\alpha_n$ παράγεται ελεύθερα από αυτά.

Η παραπάνω αναπαράσταση του Magnus είναι πιστή[1] και η απόδειξή της οδηγεί σε δύο χρήσιμους αλγορίθμους για την ανάπτυξη του συγκεκριμένου κρυπτοσυστήματος με χρήση τυπικών δυναμοσειρών. Ο πρώτος δίνει για ένα πολυώνυμο στην $\overline{H}$ το οποίο ανήκει στην $\overline{F}=<\alpha_i, i\in I>\leq\overline{H}$, τη μοναδική του διάσπαση σε ελεύθερες ομάδες. Δηλαδή, δοθέντος ενός πολυωνύμου $f(x_{1,}x_{2,}\ldots,x_n)$ στις μη μετατιθέμενες μεταβλητές $x_{1,}x_{2,}\ldots,x_n$ που ανήκει στην $\overline{F}$ το ξαναγράφουμε ως $f=W(\alpha_{1,}\alpha_{2,}\ldots,\alpha_n)$. Γενικά, δεν υπάρχει αλγόριθμος παραγοντοποίησης στην $\overline{H}$. Για κάθε μονώνυμο $x_{i_1}x_{i_2}\ldots x_{i_k}\in\overline{H}$ ονο-

1 Μία αναπαράσταση φ καλείται **πιστή**, αν $ker\,\varphi=\{1\}$.

μάζουμε το k μήκος του μονωνύμου σε αναλογία με το μήκος μίας λέξης σε μία ελεύθερη ομάδα.

Θεώρημα **(Αλγόριθμος εύρεσης ελεύθερης διάσπασης σε ελεύθερες ομάδες στοιχείων της $\overline{F}$) :** Έστω $f=f(x_{1,}x_{2,}\ldots,x_n)\in\overline{H}\Rightarrow f\in\overline{F}$. Υπάρχει ένας αλγόριθμος με τον οποίο ξαναγράφουμε το f με τη βοήθεια των ελευθέρων γεννητόρων $\alpha_{1,}\ldots,\alpha_n$, δηλαδή: $f=W(\alpha_{1,}\ldots,\alpha_n)$.

Βήμα 1ο: Επισημαίνουμε στο πολυώνυμο f το μονώνυμο μεγίστου μήκους που εμφανίζεται: $n\,x_{i_1}\ldots x_{i_k}$ μεγίστου μήκους με $n\in\mathbb{Z}-\{0\}$, όπου κάθε μεταβλητή του f εμφανίζεται στο μονώνυμο αυτό με δύναμη 1. Το k δίνει το μήκος της λέξης που αντιστοιχεί στην ελεύθερη ομάδα. Επιπλέον, η λέξη αυτή πρέπει να έχει τη μορφή: $\alpha_{i_1}^{n_1}\ldots\alpha_{i_k}^{n_k}$ όπου n_i διαιρέτης του n .

Βήμα 2ο: Για κάθε διαιρέτη του $n_i\in\mathbb{Z}$ του n υπολογίζουμε το πολυώνυμο: $(1+x_i)^{-n_1}f$.

Σε ένα ακριβώς τέτοιο γινόμενο το μέγιστο μήκος θα είναι $k-1$ και θα υπάρχει μοναδικό μονώνυμο μήκους $k-1$, το οποίο θα περιέχει κάθε μεταβλητή του f εκτός ίσως του x_{i_1} με δύναμη 1. Τότε θα έχουμε: $f=(1+x_{i_1})^{n_1}f_1$, $f_1\in\overline{F}$.

Βήμα 3ο: Συνεχίζουμε τη διαδικασία με αυτόν τον τρόπο μέχρι να φτάσουμε στη μονάδα, οπότε θα έχουμε λάβει τη διάσπαση στην ελεύθερη ομάδα να είναι της μορφής : $f=(1+x_{i_1})^{n_1}\ldots(1+x_{i_k})^{n_k}=\alpha_{i_1}^{n_1}\ldots a_{i_k}^{n_k}$

Ο αλγόριθμος αυτός καθώς και ο επόμενος μαζί με πλήρεις αποδείξεις παρουσιάζονται στο σχετικό [5] σελ.6 κ.ε.

Ο δεύτερος αλγόριθμος δίνει τη δυνατότητα προσδιορισμού πότε ένα στοιχείο της $\overline{H}$ ανήκει στην $\overline{F}$ (membership problem).

Θεώρημα: (Αλγόριθμος υπολογισμού αν το $f\in\overline{H}$ συνεπάγεται $f\in\overline{F}$). Έστω $f=f(x_{1,}\ldots,x_n)\in\overline{H}$, τότε υπάρχει αλγόριθμος απόφανσης αν $f\in\overline{F}$ και δίνει γραφή του f με τη

βοήθεια των: $\alpha_i = 1 + x_i, i = 1,\ldots, n$.

Βήμα 1ο: Αν ο σταθερός όρος του f δεν είναι μονάδα, τότε: $f \notin \overline{F}$. Ακόμα, αν το f έχει μη ακέραιους συντελεστές, τότε $f \notin \overline{F}$.

Βήμα 2ο: Έστω ότι δεν προκύπτει συμπέρασμα από το προηγούμενο βήμα. Αν το f δεν περιέχει μοναδικό μονώνυμο $nx_{i_1}, \ldots, x_{i_k}$ μεγίστου μήκους για $n \in \mathbb{Z} - \{0\}$ και περιέχει όλες τις μεταβλητές του f σε δύναμη εκθέτη 1, τότε έχουμε ότι: $f \notin \overline{F}$.

Βήμα 3ο: Εφόσον ακόμα δεν έχει προκύψει συμπέρασμα και το f περιέχει μονώνυμο του βήματος 2: $nx_{i_1}, \ldots, x_{i_k}$ μεγίστου μήκους για $n \in \mathbb{Z} - \{0\}$, τότε αν $f \in \overline{F}$ ο k δίνει το μήκος της αντίστοιχης λέξης στην ελεύθερη ομάδα, η οποία θα έχει τη μορφή: $\alpha_{i_1}^{n_1} \ldots a_{i_k}^{n_k}, \text{όπου} : n_i | n$.

Βήμα 4ο: Για κάθε διαιρέτη n_i του n σχηματίζουμε διαδοχικά το πολυώνυμο $(1 + x_{i_1})^{-n_1}$. Αν σε ένα τέτοιο γινόμενο το μέγιστο μήκος είναι $k-1$ και δεν υπάρχει νέο μονώνυμο με τα προηγούμενα χαρακτηριστικά, τότε: $f \notin \overline{F}$.

Βήμα 5ο: Αν προκύψει η μονάδα, τότε $f \notin \overline{F}$ και η διαδικασία δίνει τη διάσταση σε ελεύθερο γινόμενο του f .

Για κάποιες εφαρμογές στην κρυπτογραφία θα χρησιμοποιήσουμε ολόκληρη την ομάδα των αντιστρέψιμων στοιχείων $U(\overline{H})$ της $\overline{H} = \langle\langle x_1, x_2, \ldots, x_n : x_i^d = 0, i = 1,2,\ldots, n \rangle\rangle$ η οποία επί του $\mathbb{Q}$ είναι ακριβώς εκείνα τα πολυώνυμα με μη μηδενικό σταθερό όρο, όπως αποδεικνύεται στο επόμενο:

Θεώρημα: Η ομάδα των μονάδων $U(\overline{H})$ επί του $\mathbb{Q}$ αποτελείται από εκείνα ακριβώς τα πολυώνυμα με μη μηδενικό σταθερό όρο.

Για τον πολλαπλασιασμό στην $\overline{H}$ δεν υπάρχει αλγόριθμος παραγοντοποίησης. Εντούτοις, αν $f \in \overline{H}$ είναι γνωστό και $g = fe, e \in \overline{F}$ είναι επίσης γνωστό, τότε μπορεί να προσδιοριστεί

το e , διότι, αν τα e, fe είναι γνωστά, τότε στο fe υπάρχει μοναδικό μονώνυμο που επεκτείνει τα μονώνυμα του f όπως και στο προηγούμενο θεώρημα. Αναγνωρίζοντας αυτό το μονώνυμο είναι δυνατό να βρεθεί η ελεύθερη διάσπαση του e .

Κρυπτοσυστήματα με δακτύλιους τυπικών δυναμοσειρών

Κρυπτοσυστήματα σε μη αβελιανές ομάδες

Έστω G μία πεπερασμένα παριστώμενη ομάδα, η οποία περιέχει δύο μεγάλες υποομάδες A_1, A_2 των οποίων τα στοιχεία μετατίθενται μεταξύ τους. Όταν γράφουμε μεγάλη εννοούμε ότι είναι δύσκολο να προσδιοριστεί αν ένα τυχαίο στοιχείο της G ανήκει στην A_1 ή στην A_2 και επιπλέον αυτές οι υποομάδες είναι αρκετά μεγάλες, ώστε να μπορούν να επιλεχθούν στοιχεία με τυχαίο τρόπο από αυτές.

Αν υποτεθεί ότι ο αποστολέας Β θέλει να επικοινωνήσει με ένα δέκτη Α, μέσω ενός μη ασφαλούς καναλιού (πχ διαδίκτυο), γίνεται κωδικοποίηση του μηνύματος μέσα στην πεπερασμένα παραγόμενη ομάδα G , με τις ιδιότητες που περιγράφηκαν παραπάνω. Οι δύο υποομάδες A_1, A_2 , των οποίων τα στοιχεία μετατίθενται κρατούνται μυστικές από αποστολέα και δέκτη. Μάλιστα θεωρείται ότι ο αποστολέας Β γνωρίζει μόνο την υποομάδα A_1 και ο δέκτης Α γνωρίζει μόνο την υποομάδα A_2 . Αν ο αποστολέας Β θέλει να στείλει το μήνυμα $M \in G$ (κωδικοποιημένο στην ομάδα G), στο δέκτη Α, επιλέγει τυχαία δύο στοιχεία $\beta_1, \beta_2 \in A_1$ και στέλνει στο δέκτη το μήνυμα: $\beta_1 M \beta_2$. Ο δέκτης Α επιλέγει δύο τυχαία στοιχεία $\alpha_1, \alpha_2 \in A_2$ και επιστρέφει το μήνυμα $\alpha_1 \beta_1 M \beta_2 \alpha_2$ στον Β. Αυτά τα μηνύματα εμφανίζονται στην αναπαράσταση της G , για παράδειγμα ως πίνακες ή ανηγμένες λέξεις, οπότε δεν εμφανίζονται ως μία απλή διαδοχή γραμμάτων και δεν είναι άμεσα αναγνωρίσιμα. Εφόσον τα στοιχεία των A_1, A_2 μετατίθενται ισχύει ότι:

$\alpha_1\beta_1 M\,\beta_2\alpha_2=\beta_1\alpha_1 M\,\alpha_2\beta_2$. Όμως ο αποστολέας Β γνωρίζει τα στοιχεία $\beta_{1,}\beta_2$ καθώς επίσης και τα αντίστροφά τους, οπότε πολλαπλασιάζοντας με τα αντίστροφα δημιουργεί το μήνυμα $\alpha_1 M\,\alpha_2$ το οποίο αποστέλλει εκ νέου στο δέκτη Α. Αυτός με τη σειρά του γνωρίζει τα στοιχεία $\alpha_{1,}\alpha_2$, οπότε, πολλαπλασιάζοντας με τα αντίστροφά τους λαμβάνει αυτούσιο το μήνυμα M . Προφανώς, για κάθε μήνυμα πηγή και δέκτης μπορούν να χρησιμοποιούν διαφορετικά στοιχεία των ομάδων $A_{1,}A_2$. Σχηματικά έχουμε το εξής :

$$\begin{array}{ccccc} & B:\beta_1,\beta_2\in A_1 & & A:\alpha_1,\alpha_2\in A_2 & \\ M & \longrightarrow & \beta_1 M\,\beta_2 & \longrightarrow & \alpha_1\beta_1 M\,\alpha_2=\beta_1\alpha_1 M\,\alpha_2\beta_2 \end{array}$$

$$\begin{array}{ccccc} & B:\beta_1^{-1},\beta_2^{-1}\in A_1 & & A:\alpha_1^{-1}\alpha_2^{-1} & \\ & \longrightarrow & \alpha_1 M\,\alpha_2 & \longrightarrow & =M \end{array}$$

Αυτή η μέθοδος αποτελεί μία γενίκευση της μεθόδου των Anshel, Anshel, Goldfeld [3] και Ko-Lee [11], οι οποίοι χρησιμοποίησαν ομάδες πλεξιδίων ως βάση. Για γενικότερη ενημέρωση ως προς τις μεθόδους κρυπτογράφησης που μπορούν να χρησιμοποιηθούν στη μη μεταθετική αλγεβρική κρυπτογραφία μπορεί κανείς να ανατρέξει στο [15]. Στη συνέχεια παρουσιάζεται μία απλουστευμένη εφαρμογή της μεθόδου με χρήση γνώσεων λυκείου.

Κρυπτογραφία δυναμοσειρών και η ταυτότητα $\alpha^v+\beta^v$

Η ουσία των μαθηματικών βρίσκεται και στη χρήση τους και την εξέλιξη που προσφέρουν στον ανθρώπινο πολιτισμό. Εξάλλου τα μαθηματικά συνεξελίσονται και επηρεάζονται και από τις άλλες επιστήμες, οι οποίες φαινομενικά παρουσιάζουν περισσότερες εφαρμογές στην καθημερινότητα, αλλά βέβαια, σχεδόν πάντα μεσολαβεί άμεσα ή έμμεσα μία μαθηματική θεωρία.

Φυσικά και οι μαθητές ενδιαφέρονται ιδιαιτέρως για τέτοιες εφαρμογές που προσδίδουν αξία στη γνώση τους, ιδιαίτερα μάλιστα στη μαθηματική γνώση. Δυστυχώς όμως ο περιορι-

σμένος χρόνος στη Β΄θμια εκπαίδευση, δεν επιτρέπει την παρουσίαση σε ικανοποιητική έκταση και μελέτη εφαρμογών των μαθηματικών που διδάσκονται. Η ενασχόληση των μαθητών με εφαρμογές όπως αυτή που ακολουθεί θα βοηθούσε, ώστε τόσο οι έννοιες που διδάσκονται να εμπεδωθούν καλύτερα, όσο και να καλλιεργηθεί η απαιτούμενη μαθηματική περιέργεια σε αυτές τις γόνιμες ηλικίες. Δηλαδή να αναπτύξουμε στη διαδικασία της μάθησης σε μία τάξη λυκείου έντονο ενδιαφέρον, ώστε να παρακινηθούν οι μαθητές [2].

Στη συνέχεια παρουσιάζεται ένα απλουστευμένο σχήμα του μοντέλου κρυπτογράφησης μέσω των τυπικών δυναμοσειρών, το οποίο αναλύθηκε στην προηγούμενη παράγραφο. Έχει προσαρμοστεί έτσι, ώστε να γίνεται κατανοητό από μαθητές Β' θμιας εκπαίδευσης, αλλά και να μπορεί να βοηθήσει στην κατανόηση της λειτουργίας αλγορίθμων κρυπτογράφησης τύπου Diffie – Hellman. Ταυτόχρονα θα δουν οι μαθητές μία χρηστική εφαρμογή της ταυτότητας:

$$\alpha^{\nu}+\beta^{\nu}=(\alpha+\beta)(\alpha^{\nu-1}\beta^{0}-\alpha^{\nu-2}\beta^{1}+\ldots+(-1)^{\nu-1}\beta^{\nu-1}),\ \nu\ \text{περιττός φυσικός}\ .$$

Το παράδειγμα υλοποίησης περιγράφεται όπως περίπου θα το παρουσίαζε ένας καθηγητής Β'θμιας εκπαίδευσης σε μία τάξη, πιθανώς δίνοντας κάποιες περισσότερες επεξηγήσεις όπου θα το έκρινε αναγκαίο.

Έστω η γνωστή από το γυμνάσιο ταυτότητα: $\alpha^3+\beta^3=(\alpha+\beta)(\alpha^2-\alpha\beta+\beta^2)$ [2]. Στόχος είναι να εφαρμοστεί σε έναν σύγχρονο αλγόριθμο κρυπτογράφησης με πολυώνυμα πολλών μεταβλητών. Ειδικότερα, θα γίνει χρήση αυτής για $\alpha=1$ και $\beta=x$, δηλαδή της $1+x^3=(1+x)(1-x+x^2)$.

Για το σκοπό της κρυπτογράφησης[3] θεωρείται ότι κάθε δύ-

2 Στη γενική μορφή της ταυτότητας η μέθοδος μπορεί να προσαρμοστεί κατάλληλα με αντίστοιχη ορίζουσα δύναμη $d=v$ αντί του 3.

3 Εδώ θα μπορούσαμε με κάποιο τρόπο να εξηγήσουμε την έννοια της τάξης ενός στοιχείου μίας ομάδας. Για παράδειγμα αναφερόμενοι σε διαδικασίες, όπως το γύρισμα ενός διακόπτη κουζίνας 4 φορές που είναι ισοδύναμο με τον να μην τον έχουμε γυρίσει καθόλου και γενικά παρόμοια παραδειγ-

ναμη του x μεγαλύτερη ή ίση του 3 είναι μηδέν, δηλαδή : $x^3=x^4=x^5=\ldots=0$, αλλά $x, x^2\neq 0$. Το ίδιο ισχύει και για τις άλλες μεταβλητές που θα χρησιμοποιηθούν, δηλαδή $y^3=y^4=\ldots=z^3=z^4=\ldots=0$ και $y, y^2, z, z^2,\ldots\neq 0$.

Έστω ότι θα κρυπτογραφηθεί και θα αποσταλεί ως μήνυμα Μ η λέξη Μ=ΜΑΘΗΜΑ.

Επιλέγεται μία αντιστοίχιση των γραμμάτων σε πρώτους αριθμούς όπως για παράδειγμα η παρακάτω :

$$\begin{array}{c} A\to 2\\ B\to 3\\ \Gamma\to 5\\ \Delta\to 7\\ E\to 11\\ Z\to 13\\ H\to 17\\ \Theta\to 19\\ \vdots\\ M\to 37\\ \vdots \end{array}$$

Επίσης ταξινομούνται οι δυνάμεις των μεταβλητών που θα χρησιμοποιηθούν και που ΔΕΝ θεωρούνται μηδενικές (όπως παραπάνω) ως εξής: $x, x^2, y, y^2, z, z^2,\ldots$ δηλαδή με λεξικογραφική διάταξη. Η λέξη μάθημα κωδικοποιείται τώρα στο «νέο αλφάβητο» ως εξής :

$$M=MA\Theta HMA=37x+2x^2+19y+17y^2+37z+2z^2$$

Δηλαδή σε κάθε γράμμα αντιστοιχεί ένας αριθμός, όπως στον προηγούμενο πίνακα και οι μεταβλητές σε λεξικογραφική διάταξη καθορίζουν τη σειρά των γραμμάτων.

Στη συνέχεια για να αποσταλεί το κωδικοποιημένο αυτό μήνυμα χωρίς να «προδοθεί» η ταυτότητα δύναμης 3 που χρησιμοποιήθηκε και το γεγονός ότι οι μεγαλύτερης δύναμης μεταβλητές «αγνοούνται» προσθέτουμε στο μήνυμα έναν παράγοντα

ματάκια της αριθμητικής mod n.

θορύβου Ν, ο οποίος περιλαμβάνει αθροίσματα δυνάμεων μεταβλητών με εκθέτη μεγαλύτερο ή ίσο του 3. Για παράδειγμα μπορούμε να θεωρήσουμε $N=2x^3+17x^4+2z^5$ ή οποιοδήποτε άλλο κατάλληλο. Έτσι το αρχικό μήνυμα Μ με την προσθήκη του Ν γίνεται το πρώτο μήνυμα προς αποστολή για τον δέκτη :

$$Q=M+N=37x+2x^2+2x^3+17x^4+19y+17y^2+27z+2z^2+2z^5$$

Για να επιτευχθεί η πρώτη απόκρυψη του μηνύματος ο αποστολέας Α πολλαπλασιάζει το αρχικό μήνυμα με ένα πολυώνυμο της μορφής[4] $A=1+x$, δηλαδή καταγράφει και αποστέλλει το μήνυμα :

$$AQ=$$
$$(1+x)Q=$$
$$(1+x)(37x+2x^2+2x^3+17x^4+19y+17y^2+27z+2z^2+2z^5)=$$
$$37x+39x^2+4x^3+19x^4+17x^5+19xy+17xy^2+27xz+2xz^2+2xz^5+$$
$$+19y+17y^2+27z+2z^2+2z^5$$

όπου ο υπολογισμός αυτός όπως και οι υπόλοιποι στη συνέχεια μπορούν να γίνονται από τους μαθητές με χρήση Η/Υ και είτε ενός σχετικού προγράμματος όπως το wxmaxima (ελεύθερο λογισμικό), είτε στο διαδίκτυο μέσω πχ του www.wolframalpha.com. Η πολυπλοκότητα των πράξεων και ο κίνδυνος αλλοίωσης του μηνύματος σε περίπτωση λάθους αναδεικνύουν την αναγκαιότητα χρήσης σχετικών λογισμικών.

Τώρα το μήνυμα AQ όπως παραπάνω είναι μη αναγνωρίσιμο[5] και μπορεί να αποσταλεί μέσω μη ασφαλούς καναλιού στον δέκτη Β, ο οποίος όμως δεν μπορεί να το αποκωδικοποιήσει διότι δε γνωρίζει τον παράγοντα Α και ούτε μπορεί να τον εξάγει εύκολα (όταν η πολυπλοκότητα του συστήματος που εξαρ-

4 Σε αντιστοιχία με τη μέθοδο των τυπικών δυναμοσειρών αυτό είναι ένα αντιστρέψιμο στοιχείο με αντίστροφο το συζυγές, όπως το γνωρίζουν οι μαθητές $1-x+x^2$ για τη συγκεκριμένη ταυτότητα της οποίας γίνεται χρηση.

5 Φυσικά σε αυτήν την απλουστεύμενη εκδοχή προς τους μαθητές η ορίζουσα δύναμη είναι μικρή και η κρυπτανάλυση με δοκιμές μπορεί να είναι επιτυχημένη.

τάται από το μέγεθος των εκθετών που χρησιμοποιούνται γίνει επαρκώς μεγάλη). Επομένως ο Β δεν μπορεί ούτε να το αναγνωρίσει, ούτε και να το αποκρυπτογράφηση.

Στο επόμενο βήμα ο Β πολλαπλασιάζει και αυτός με ένα παράγοντα από δεξιά αυτή τη φορά, της ίδιας μορφής, π.χ. τον $B=1+z$ οπότε δημιουργεί το μήνυμα AQB που είναι πάλι ένα πολυώνυμο τριών μεταβλητών x, y, z και το οποίο αποστέλλει στον Α.

Ο Α έχει στην κατοχή του το μη αναγνωρίσιμο κωδικοποιημένο μήνυμα AQB για το οποίο όμως γνωρίζει τον παράγοντα A με τον οποίο είχε πολλαπλασιάσει αρχικά από τα αριστερά, καθώς επίσης και τον συζυγή[6] του $A^{-1}=(1-x+x^2)$ οπότε, πολλαπλασιάζοντας με αυτόν λαμβάνει: $A^{-1}AQB=QB$

Τελικά ο Β έχει πλέον το κωδικοποιημένο, μη αναγνωρίσιμο μήνυμα QB για το οποίο γνωρίζει τον παράγοντα B με τον οποίο είχε πολλαπλασιάσει από δεξιά, οπότε γνωρίζει και τον συζυγή του ως προς την ταυτότητα και την ορίζουσα δύναμη που επιλέχθηκε, δηλαδή τον $B^{-1}=(1-z+z^2)$ με τον οποίο και πολλαπλασιάζει από δεξιά λαμβάνοντας τελικά: $QBB^{-1}=Q$ το οποίο είναι το αρχικό κωδικοποιημένο μήνυμα που ήθελε να του στείλει ο Α με τον παράγοντα θορύβου, δηλαδή το:

$Q=M+N=37x+2x^2+2x^3+17x^4+19y+17y^2+37z+2z^2+2z^5$ για το οποίο όμως μπορεί να «αγνοήσει» τα μονώνυμα με βαθμό μεγαλύτερο του 2, δηλαδή τον παράγοντα θορύβου N, οπότε να λάβει αυτούσιο το αρχικό μήνυμα M.

Επίλογος

Η κρυπτογραφία άπτεται πολλών επιστημονικών κλάδων: των μαθηματικών, της φυσικής (κβαντική κρυπτογραφία), της πληροφορικής, της πολυπλοκότητας κλπ., οπότε μπορεί να αποτελέσει τη βάση για σχέδια εργασίας (Project) με συνεργασία δια-

6 Ο οποίος συζυγής ως προς την ταυτότητα και την ορίζουσα δύναμη 3 που επιλέχθηκε έχει το ρόλο αντιστρόφου.

φόρων ειδικοτήτων καθηγητών Β΄θμιας εκπαίδευσης: Μαθηματικών, Φυσικών, Πληροφορικών, κ.ά.

Στα παραδείγματα που θα χρησιμοποιηθούν στη Β'θμια εκπαίδευση δεν είναι αναγκαίο να επιμείνει κανείς στην αποτελεσματικότητά τους και τη μη ύπαρξη αποτυχίας πρωτοκόλλου ή την πλήρη κρυπτανάλυση του συστήματος. Ο στόχος δεν είναι αυτός, αλλά να κατανοήσουν οι μαθητές κάποιους γενικότερους μηχανισμούς, (όπως τη σημασία της πολυπλοκότητας των κλειδιών πχ passwords, PINs, κ.ά. τα οποία χρησιμοποιούν στην καθημερινότητά τους για συναλλαγές). Επίσης να δουν εφαρμογές - έστω και απλουστευμένες - μαθηματικών αντικειμένων, τα οποία διαπραγματεύονται στο σχολείο ως αυτοτελή, ξεκομμένα από την πραγματική ζωή, ιδεολογήματα.

Συνεπώς, συντείνουμε με αυτόν τον τρόπο (και βέβαια με πλούτο εφαρμογών) στη δημιουργία κινήτρων μάθησης, μέσα από προβλήματα και δραστηριότητες της καθημερινότητας, αλλά και την δημιουργία ατμόσφαιρας μυστηρίου και έκπληξης στη σχολική τάξη [2]. Εκπληρώνεται δηλαδή και ο γενικότερος σκοπός της Β' θμιας εκπαίδευσης προς την απόκτηση ΠΑΙΔΕΙΑΣ και ΜΟΡΦΩΣΗΣ και όχι ως αυτοσκοπός η μελλοντική επαγγελματική αποκατάσταση σε βάρος παραγωγικών και δραστήριων πολιτών.

ABSTRACT

This study presents a concise review of the history of cryptography towards the fundamental ideas of the so-called non-commutative algebraic cryptography; in particular that one based on the ring of formal power series. The main objective is to explore an application of pure mathematics (group theory) on a cryptosystem. In this context a simplified method is presented - adjusted to high school cognitive level, using polynomials and algebraic identities - as a contribution to mathematics teaching, by highlighting some of their applications.

Βιβλιογραφία

1. Κάτος Β., Στεφανίδης, Γ., *Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης*, ΖΥΓΟΣ 2003.
2. Τουμάσης Μ., *Πώς να ενεργοποιήσουμε τα παιδιά στο μάθημα των μαθηματικών*, Κωστόγιαννος 2005.
3. Anshel I., Anshel M., Goldfeld D., *An algebraic method for public key cryptography, 1999.*, Math research letters 6 , No. 3-4 1999.
4. Birman Joan S., Brendle Tara E., *Braids*, A Survey 2004.
5. Baumslag Gilbert , Brukhov Yegor , Fine B., Rosenberger G., *Encryption Methods using Formal Power Series Rings*, Centre de Recerca Matematica(CRM), Catalan, December 2007 2007.
6. Birget J.C., Magliveras S.S., Sramka M., *On public-key cryptosystems based on combinatorial group theory*, Tatra Mountains Mathematical Publi-cations 33 (2006), pp. 137-148 2006.
7. Diffie W., Hellman M. E. , *New Directions in Cryptography* , IEEE Transactions on Information Theory, vol. IT-22, Nov. 1976, pp: 644–654. 1976.
8. Hungerford Thomas W. , *Algebra (Graduate Texts in Mathematics)*, Springer 1973.
9. *International Association for Cryptologic Research*, http://www.iacr.org/ .
10. Kahn D., *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*, http://david-kahn.com/book-david-kahn-code-codebreakers-cryptography.htm 1967, 1996.
11. Ko K. H., Lee S. J., Cheon J. H., Han J. W., Kang J., Park C., *New public-key cryptosystem using braid groups*, Advances in Cryptology CRYPTO 2000, Lecture Notes in Computer Science 1880, pp. 166-183.Springer, Berlin 2000.

12. Koblitz N., *A Course in Number Theory and Cryptography*, Graduate Texts in Math. No. 114, Springer-Verlag, New York 1987, 1994.
13. Miller C.F., *Decision problems for groups* , survey and reflections .
14. Magnus W., Karrass A., Solitar D., *Combinatorial Group Theory*, Dover 2004 2η έκδοση 1965.
15. Myasnikov A., Shpilrain V., Ushakov A., *Group Based Cryptography*, Birkhauser Verlag 2008.
16. Myasnikov A. G., Shpilrain V., Ushakov, *A practical attack on somebraid group based cryptographic protocols*, CRYPTO 2005, LectureNotes Comp. Sc. 3621 (2005),pp. 86-96. 2005.
17. Menezes A., vanOorschot P., Vanstone S. , *Handbook of Applied Cryptography Menezes*, CRC Press, 1996 www.cacr.math.uwaterloo.ca/hac 1996.
18. Magyarik M. R., Wagner N. R. , *A Public Key Cryptosystem Based on the Word Problem* , Advances in Cryptology, CRYPTO 1984, Lecture Notes in Computer Science 196, pp. 19-36. Springer, Berlin 1985.
19. Shpilrain Vladimir, Zapata Gabriel , *Combinatorial Group Theory and Public Key Cryptography*, Cryptology ePrint Archive, Report 2004/242 , http://eprint.iacr.org/ 2004.