Η ΤΕΧΝΙΚΗ ΤΗΣ ΜΕΡΙΚΗΣ ΣΥΛΛΑΒΙΚΗΣ ΑΝΤΙΚΑΤΑΣΤΑΣΗΣ ΣΕ ΕΦΑΡΜΟΓΕΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Δρ. Ευάγγελος Χ. Παπακίτσος

ΕΔΙΠ (Α), Τμήμα Μηχανικών Βιομηχανικής Σχεδίασης & Παραγωγής
Εξωτερικός συνεργάτης του Ερευνητικού Εργαστηρίου «Διαχείρισης Δεδομένων, Πληροφορίας και Γνώσης» του Τμήματος Μηχανικών Πληροφορικής & Υπολογιστών, Πανεπιστήμιο Δυτικής Αττικής, e-mail: papakitsev@uniwa.gr

Περίληψη

Η δημιουργία ενός κρυπτογραφημένου μηνύματος από τον αποστολέα του λέγεται κρυπτογράφηση, ενώ η επαναφορά του στην αρχική γραπτή μορφή από τον παραλήπτη του λέγεται αποκρυπτογράφηση. Η κρυπτογράφηση πραγματοποιείται συνήθως με την αντικατάσταση των γραμμάτων του αρχικού μηνύματος με άλλα, έτσι ώστε να αλλοιώνεται δραστικά η όψη του κειμένου. Το αντίμετρο της κρυπτογράφησης είναι η κρυπτανάλυση, δηλαδή το πώς κάποιος αντίπαλος θα αναγνώσει το αρχικό μήνυμα. Υπάρχουν δύο κύριοι μέθοδοι κρυπτογράφησης, αυτοί της μετάθεσης και της αντικατάστασης, με διαφορετικούς αλγορίθμους υλοποίησης. Αντίστοιχα με τους αλγορίθμους κρυπτογράφησης αναπτύχθηκαν και οι τεχνικές κρυπτανάλυσης. Οι βασικότερες τεχνικές κρυπτανάλυσης που επινοήθηκαν για την ανάγνωση της κρυπτογράφησης αντικατάστασης είναι η ανάλυση συχνοτήτων, η τεχνική του μέγιστου κοινού διαιρέτη και η τεχνική Babbage-Krasinski. Στην παρούσα εργασία περιγράφεται μια νέα τεχνική κρυπτογράφησης που πραγματοποιεί μερική συλλαβική αντικατάσταση, δηλαδή αντικαθιστά κάποιες συλλαβές με έναν χαρακτήρα, έτσι ώστε η κρυπτογράφηση να γίνεται ανθεκτικότερη στις τεχνικές κρυπτανάλυσης. Αυτή η νέα τεχνική κρυπτογράφησης βασίζεται στις προϊστορικές γραφές του Αιγαίου κατά τη 2η χιλιετία π.Χ., που περιλαμβάνουν τρία συλλαβάρια, δηλαδή συστήματα γραφής όπου το κάθε σημείο αντιστοιχεί σε μία συλλαβή, συνήθως της μορφής συμφώνου-φωνήεντος, και όχι σε έναν φθόγγο συμφώνου ή έναν φωνήεντος, όπως συμβαίνει συνήθως στο αλφάβητο.

Λέξεις-κλειδιά: *κρυπτογραφία, κρυπτογράφημα, κρυπτογράφηση, αποκρυπτογράφηση, κρυπτανάλυση, μερική συλλαβική αντικατάσταση.*

Abstract

Creating an encrypted message from its sender is called encryption, while restoring it to its original written form is called decryption. Encryption is usually done by replacing the letters of the original message with others, so as to drastically alter the appearance of the text. The countermeasure of encryption is cryptanalysis, namely, how an opponent will read the original message. There are two main methods of encryption, those of displacement and substitution, with different implementation algorithms. Cryptanalysis' techniques have also been developed along with the encryption algorithms. The most basic cryptanalysis' techniques, devised for reading substitution encryption, are the frequency analysis, the maximum common divisor technique, and the Babbage-Krasinski technique. In this work, a new encryption technique is described that performs partial syllabic substitution, namely, it replaces some syllables with a single character, so that the encryption becomes more resistant to cryptanalysis' techniques. This new encryption technique is based on the prehistoric scripts of the Aegean in the 2nd millennium BC, which include three syllabaries, namely writing systems where each sign corresponds to a syllable, usually of the consonant-vowel form, rather than to a single consonant or a single vowel, as is usually the case with the alphabet.

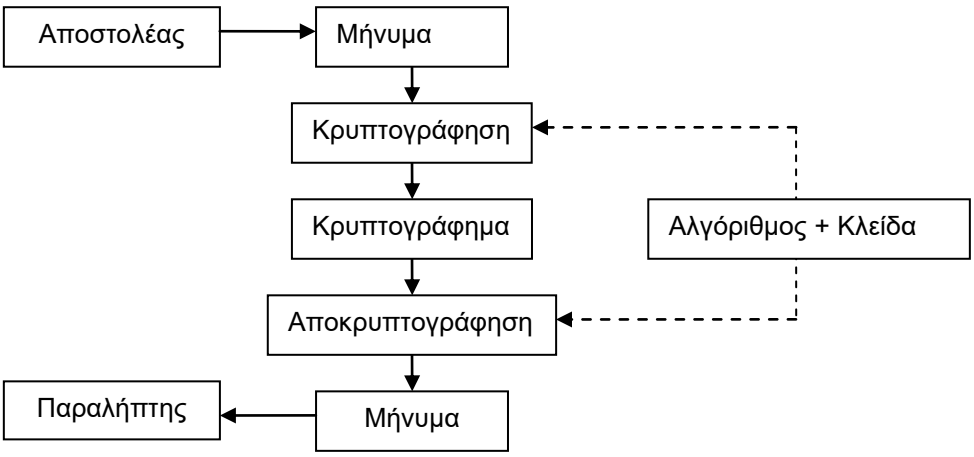
Keywords: *cryptography, cryptograph, encryption, decryption, cryptanalysis, partial syllabic substitution.*

1. Εισαγωγή

Η σχέση Γλώσσας και Μαθηματικών είναι αρχαία, διαρκής και πολύπλευρη, ειδικά μετά την καθιέρωση της Πληροφορικής ως διακριτής επιστήμης. Αρχίζει μαζί με την εφεύρεση της γραφής και σήμερα επεκτείνεται σε όλα τα επίπεδα γλωσσικής ανάλυσης (φωνητικό/φωνολογικό, μορφολογικό, συντακτικό, σημασιολογικό και πραγματολογικό), με διάφορους τρόπους. Αυτοί οι τρόποι αφορούν τις μεθόδους

κωδικοποίησης τόσο της περιγραφής του σημαίνοντος όσο και της ερμηνείας του σημαινόμενου. Μία από τις δύο αρχαιότερες σχέσεις Γλώσσας και Μαθηματικών είναι οι εφαρμογές των δεύτερων στις επικοινωνίες και ειδικά στην ασφαλή και εμπιστευτική μετάδοση μηνυμάτων: η *κρυπτογραφία* (και η αντίθετη της *κρυπτανάλυση*).

Σύμφωνα με το Λεξικό της Ισπανικής Βασιλικής Ακαδημίας, *κρυπτογραφία* είναι η τέχνη της γραφής με τη βοήθεια ενός μυστικού κλειδιού (*κλείδα*) ή με αινιγματικό τρόπο. Οι Μεσοποτάμιοι και οι Αιγύπτιοι χρησιμοποιούσαν κρυπτογραφικές μεθόδους, αλλά πρώτοι οι Έλληνες και οι Ρωμαίοι τις εφάρμοσαν πραγματικά, ως πολεμικοί λαοί, καθώς υπήρχε η ανάγκη για μυστικές επικοινωνίες, ώστε να εξασφαλίζεται η στρατιωτική επιτυχία (Gómez 2011). Η δημιουργία ενός κρυπτογραφημένου μηνύματος από τον αποστολέα του λέγεται *κρυπτογράφηση*, ενώ η επαναφορά του στην αρχική γραπτή μορφή από τον παραλήπτη του λέγεται *αποκρυπτογράφηση*. Η μετάδοση ενός *κρυπτογραφήματος* ακολουθεί γενικά τα βήματα του Σχ. 1, όπου τόσον ο αποστολέας όσο και ο παραλήπτης γνωρίζουν την κλείδα και τον αλγόριθμο κρυπτογράφησης-αποκρυπτογράφησης.



Σχεδιάγραμμα 1: Βήματα μετάδοσης κρυπτογραφήματος.

Το αντίμετρο της κρυπτογράφησης είναι η *κρυπτανάλυση*, δηλαδή το πώς ο αντίπαλος θα αναγνώσει από το κρυπτογράφημα το αρχικό μήνυμα. Αξίζει να αναφερθεί εδώ ότι η μετάφραση ενός κειμένου μίας άγνωστης γραφής-γλώσσας (όπως π.χ. τα σημεία στον Δίσκο της Φαιστού) συχνά αντιμετωπίζεται ως πρόβλημα κρυπτανάλυσης

(Παπακίτσος 2013β). Σε κάθε περίπτωση (κρυπτογράφησης/κρυπτανάλυσης) υπάρχουν αντίστοιχες μέθοδοι που περιλαμβάνουν ένα πλήθος σχετικών αλγορίθμων.

2. Μέθοδοι και Αλγόριθμοι Κρυπτογράφησης

Υπάρχουν δύο κύριοι μέθοδοι κρυπτογράφησης: η μέθοδος της *μετάθεσης* και η μέθοδος της *αντικατάστασης*. Στη μετάθεση το γράμμα αλλάζει θέση με την παρεμβολή άχρηστων γραμμάτων αλλά διατηρεί τη φωνητική του αξία, δηλαδή αποδίδει τον ίδιο φθόγγο τόσο στο πρωτότυπο όσο και στο κρυπτογράφημα. Στην αντικατάσταση το γράμμα διατηρεί τη θέση του αλλά αλλάζει η αξία του, δηλαδή έχει άλλη αξία στο πρωτότυπο και άλλη στο κρυπτογράφημα, καθώς αυτό αντικαθίσταται από κάποιο άλλο γράμμα στο κρυπτογράφημα. Στη συνέχεια ακολουθεί η παρουσίαση οκτώ βασικών ιστορικών αλγορίθμων κρυπτογράφησης, με παράδειγμα την κρυπτογράφηση του μηνύματος:

ΕΠΙΘΕΣΗ ΑΥΡΙΟ

Ο πρώτος αλγόριθμος (βλ. 2.1) ανήκει στη μέθοδο της μετάθεσης, ενώ οι υπόλοιποι (βλ. 2.2-8) είναι αλγόριθμοι αντικατάστασης (Gómez 2011).

2.1. Η σκυτάλη

Η κρυπτογραφία μετάθεσης βασίζεται στην αναδιοργάνωση των γραμμάτων ενός μηνύματος, πλήθους «ν». Αν δηλαδή υποθέσουμε ότι μεταθέτουμε τρία γράμματα (ν = 3): {Α, Β, Γ}, το ένα στη θέση του άλλου, τότε δημιουργούνται 6 τρόποι αναδιοργάνωσης: {ΑΒΓ, ΑΓΒ, ΒΑΓ, ΒΓΑ, ΓΒΑ, ΓΑΒ}. Οι δυνατοί συνδυασμοί 10 γραμμάτων (ν = 10) είναι: 10! = 3.628.800.

Ένας τέτοιος αλγόριθμος κρυπτογράφησης είναι η σκυτάλη, η γνωστή μας κυλινδρική ράβδος με δεδομένο μήκος και διάμετρο. Αποτελούσε τη μέθοδο κρυπτογράφησης του Σπαρτιατικού Στρατού. Βασιζόταν στην παρεμβολή άχρηστων γραμμάτων στο πρωτότυπο, που τα έγραφαν σε μία επιμήκη λωρίδα δέρματος/υφάσματος (Σχ. 2α). Το μήνυμα εμφανιζόταν μόλις η λωρίδα τυλιγόταν στη σκυτάλη (Σχ. 2β).

(α) ΕΚΠΑΙΡΘ ΕΤΣΖΗΗ ΘΑ ΥΛΡΒΙΒΟΙ

(β)

Ε	Π	Ι	Θ	Ε	Σ	Η		Α	Υ	Ρ	Ι	Ο
Κ	Α	Ρ		Τ	Ζ	Η	Θ		Λ	Β	Β	Ι

Σχεδιάγραμμα 2: Κρυπτογράφημα σκυτάλης.

Το κλειδί του αλγορίθμου είναι το μήκος και η διάμετρος της σκυτάλης. Χωρίς σκυτάλη ίδιου ακριβώς μεγέθους, το πρωτότυπο μήνυμα δεν αποκαλύπτεται.

2.2. Η τέχνη mlecchita-vikalpa

Περίπου τον 4^{ο} αιώνα π.Χ., ο Βραχμάνος Vatsyayana συγγράφει ένα τεράστιο έργο με θέματα, μεταξύ άλλων, τις γνώσεις που πρέπει να διαθέτει μία καλή σύζυγος. Ο γνωστός τίτλος του έργου είναι «Kama-Sutra» (αλλά άγνωστος και παρεξηγημένος είναι ο σκοπός του στη Δύση), το οποίο περιέχει τις 64 διαφορετικές δεξιότητες της καλής συζύγου (κατά τον Vatsyayana), ανάμεσα στις οποίες είναι η μαγειρική, η μουσική και το σκάκι. Η δεξιότητα που μας ενδιαφέρει εδώ είναι η 45^{η} και αφορά την τέχνη κρυπτογράφησης mlecchita-vikalpa, όπου προτείνονται διάφοροι τρόποι δημιουργίας κρυπτογραφημάτων. Ένας από αυτούς είναι η διαίρεση του αλφαβήτου σε δύο ίσα μέρη και η συνακόλουθη αντιστοίχηση των γραμμάτων ανά ζεύγη, με τυχαίο τρόπο (Πίν. 1).

Πίνακας 1: Αντικατάσταση mlecchita-vikalpa.

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

Έτσι κάθε {Α} του πρωτοτύπου αντικαθίσταται με {Ν} στο κρυπτογράφημα και αντιστρόφως. Με αυτόν τον αλγόριθμο, κάθε ζεύγος γραμμάτων αποτελεί κλειδί για την αποκρυπτογράφηση του πρωτοτύπου μηνύματος.

2.3. Το τετράγωνο του Πολύβιου

Ο γνωστός ιστορικός Πολύβιος (203–120 π.Χ) εφηύρε έναν από τους πρώτους αλγόριθμους αντικατάστασης, που ονομάστηκε έτσι προς τιμήν του. Αυτός ο αλγόριθμος βασίζεται σ' έναν πίνακα 5×5 στοιχείων, στον οποίο κατανέμονται τα γράμματα του αλφαβήτου. Οι γραμμές και οι στήλες του πίνακα προσδιορίζονται είτε με γράμματα (Σχ. 3α: Α-Ε) είτε με αριθμούς (Σχ. 3β: 1-5), που αποτελούν τις συντεταγμένες του. Κάθε γράμμα αντιστοιχείται με τις συντεταγμένες του στον πίνακα ως κλειδί (π.χ. Ε = ΑΕ / 15). Έτσι κρυπτογραφείται το πρωτότυπο μήνυμα. Παρόμοια μέθοδος είναι και η κρυπτογράφηση Playfair-Wheatstone.

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

(α)

	1	**2**	**3**	**4**	**5**
1	Α	Β	Γ	Δ	Ε
2	Ζ	Η	Θ	Ι	Κ
3	Λ	Μ	Ν	Ξ	Ο
4	Π	Ρ	Σ	Τ	Υ
5	Φ	Χ	Ψ	Ω	

(β)

ΑΕΔΑΒΔΒΓΑΕΔΓΒΒ ΑΑΔΕΔΒΒΔΓΕ	ΕΠΙΘΕΣΗ ΑΥΡΙΟ	15412423154322	1145422435

Σχεδιάγραμμα 3: Το τετράγωνο του Πολύβιου.

2.4. Η ομοπαραλληλική κρυπτογράφηση

Σε αυτόν τον αλγόριθμο κρυπτογράφησης, κάθε γράμμα του μηνύματος αντικαθίσταται από ένα άλλο στο κρυπτογράφημα, μετατοπισμένο κατά συγκεκριμένο αριθμό θέσεων {ν} ως προς το αρχικό. Ο αρχαιότερος γνωστός τύπος ομοπαραλληλικού κρυπτογραφήματος είναι ο «κώδικας του Καίσαρα», που τον χρησιμοποιούσε ο Ιούλιος Καίσαρας για την κρυπτογράφηση της προσωπικής του αλληλογραφίας, σύμφωνα με τον Σουετώνιο (75-150 μ.Χ.) στο έργο του «Οι Ζωές των Δώδεκα Καισάρων». Ο αριθμός των θέσεων μετατόπισης ήταν {ν = 3} (Σχ. 4).

Το κλειδί αυτού του αλγορίθμου είναι είτε ο αριθμός μετατόπισης θέσεων {ν} είτε το πρώτο γράμμα του κρυπτογραφημένου αλφάβητου (Σχ. 4: Δ).

	0	1	2	3	4	5	6	7	8	9	10	11
x	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ
K(x)	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο

	12	13	14	15	16	17	18	19	20	21	22	23
x	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω
K(x)	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ

ΕΠΙΘΕΣΗ ΑΥΡΙΟ = ΘΤΜΛΘΦΚ ΔΨΥΜΣ

Σχεδιάγραμμα 4: Ο κώδικας του Καίσαρα.

Η ομοπαραλληλική κρυπτογράφηση βασίζεται στην **αριθμητική υπολοίπων** ή «ωρολογιακή αριθμητική», η οποία στηρίζεται στην αριθμητική των πράξεων σε τέλεια αριθμητικά σύνολα, από τις εργασίες του Ευκλείδη (325-265 π.Χ.). Ο έλληνας Μαθηματικός θεωρείται ο πατέρας της Αναλυτικής Κρυπτογραφίας και το έργο του εκτιμούσαν ιδιαίτερα οι Άραβες, ως δεξιοτέχνες της κρυπτογραφίας, όπως επίσης αργότερα και οι Βενετοί. Η αριθμητική των υπολοίπων ασχολείται με τα υπόλοιπα των ακεραίων διαιρέσεων. Η εφαρμογή της στην κρυπτογραφία περιγράφεται από την ακόλουθη σχέση:

$$K(x) = (\lambda x + \nu) \bmod \alpha$$

όπου

- x: η θέση του γράμματος στο πρωτότυπο αλφάβητο
- K(x): η κρυπτογραφημένη θέση
- λ: συντελεστής
- ν: ο αριθμός των θέσεων μετατόπισης
- α: το πλήθος των γραμμάτων του αλφαβήτου (μήκος)

- mod: τελεστής του υπόλοιπου της ακεραίας διαίρεσης [(λx + ν)/α].

Επομένως για τον «κώδικα του Καίσαρα» (Σχ. 4), η σχέση K(x) διαμορφώνεται ως εξής:

$$K(x) = (x + 3) \bmod 24.$$

Η σχέση K(x) μπορεί να γίνει πολυπλοκότερη, πολλαπλασιάζοντας το {x} με έναν ακέραιο συντελεστή {λ}. Ο δυνητικός αριθμός κλειδιών που παράγεται είναι τέτοιος ώστε εξαλείφοντας τους περιορισμούς που υπάρχουν στη σειρά των γραμμάτων προκύπτουν:

$$24! = 620.448.401.733.239.439.360.000$$

πιθανά κωδικοποιημένα αλφάβητα.

2.5. Η λέξη-κλειδί

Για πολλούς αιώνες, ο πιο δημοφιλής αλγόριθμος αντικατάστασης ήταν αυτός με λέξη-κλειδί, χάρις στην απλότητα και την αξιοπιστία του. Είναι παρόμοιος με προηγούμενο αλγόριθμο (βλ. 2.2), με τη διαφορά ότι χρησιμοποιεί ολόκληρο το αρχικό αλφάβητο, το οποίο αντικαθίσταται με ένα άλλο, αρχίζοντας από μία λέξη (π.χ. ΔΙΠΛΟΣ) γνωστή τόσο στον αποστολέα όσο και στον παραλήπτη του κρυπτογραφήματος (Πίν. 2). Το ζητούμενο για τη λέξη-κλειδί (ή και φράση-κλειδί) είναι να μην έχει επαναλαμβανόμενα γράμματα. Στο παράδειγμα του Πίν. 2 χρησιμοποιείται η λέξη-κλειδί ΔΙΠΛΟΣ, όπου τα πρώτα έξι (6) γράμματα του αλφαβήτου (Α-Ζ) αντικαθίστανται από τα αντίστοιχα της λέξης-κλειδί (δηλαδή, το Α από το Δ έως και το Ζ από το Σ). Τα υπόλοιπα γράμματα του αλφαβήτου (Η-Ω) αντικαθίστανται από το επόμενο γράμμα του αλφαβήτου μετά το τελευταίο της λέξης-κλειδί (δηλαδή, το Η από το Τ) και κατόπιν με τη σειρά (Υ, Φ, Χ, ...) για όσα δεν βρίσκονται ήδη στη λέξη-κλειδί.

Πίνακας 2: Κρυπτογράφηση με λέξη-κλειδί.

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

2.6. Η πολυαλφαβητική κρυπτογράφηση

Αυτός ο αλγόριθμος αντικατάστασης εφευρέθηκε από τον μεγαλοφυή αρχιτέκτονα και Μαθηματικό της Αναγέννησης Leon Battista Alberti (1404-1472), περίπου το 1460, γι' αυτό και ονομάζεται επίσης *αλγόριθμος του Alberti*. Για την κρυπτογράφηση του αρχικού αλφαβήτου χρησιμοποιούσε εναλλάξ δύο άλλα, όπου το πρώτο γράμμα του πρωτοτύπου αντικαθίσταται από το αντίστοιχό του στο πρώτο κρυπτογραφημένο αλφάβητο, το δεύτερο γράμμα του πρωτοτύπου αντικαθίσταται από το αντίστοιχό του στο δεύτερο κρυπτογραφημένο αλφάβητο, κ.ο.κ. (Πίν. 3). Δηλαδή, η πρώτη εμφάνιση του {Α} στο πρωτότυπο κείμενο αντικαθίσταται (π.χ.) από το {Δ} (του {Β} από το {Ε}, κ.ο.κ.), ενώ η δεύτερη από (π.χ.) το {Η} (αντίστοιχα του {Β} από το {Θ}, κ.ο.κ.). Η τρίτη εμφάνιση του {Α} αντικαθίσταται πάλι από το {Δ}, επομένως οι μονής σειράς εμφανίσεις ($1^{η}$, $3^{η}$, 5η, ...) του {Α} αντικαθίστανται από το αντίστοιχό του στο πρώτο ομοπαραλληλικό αλφάβητο, ενώ οι ζυγής σειράς εμφανίσεις ($2^{η}$, $4^{η}$, $6^{η}$, ...) από το δεύτερο. Το μεγάλο πλεονέκτημα του αλγορίθμου αυτού είναι η αυξημένη ασφάλεια. Επειδή τα κρυπτογραφημένα αλφάβητα εναλλάσσονται, το ίδιο γράμμα στο κρυπτογράφημα (π.χ. το {Α}) μπορεί να αντιστοιχεί σε διαφορετικά γράμματα του πρωτοτύπου ({Χ}/{Τ}).

Πίνακας 3: Ο αλγόριθμος του Alberti.

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

2.7. Το τετράγωνο του Vigenére

Αν και ο Alberti εφηύρε την πολυαλφαβητική κρυπτογράφηση, ο ίδιος δεν ενδιαφέρθηκε να αξιοποιήσει την ιδέα του. Το έργο αυτό ανέλαβε ο Γάλλος διπλωμάτης και κρυπτογράφος Blaise de Vigenére (1523-1596), αναπτύσσοντας το «τετράγωνο του Vigenére». Η μέθοδος έχει διάφορες παραλλαγές. Βασίζεται στην

ύπαρξη αρκετών κρυπτογραφημένων αλφαβήτων, τα οποία χρησιμοποιούνται διαδοχικά για την αντικατάσταση των γραμμάτων του πρωτοτύπου. Τα κρυπτογραφημένα αλφάβητα ακολουθούν δυνητικά τόσο τον ομοπαραλληλικό αλγόριθμο (βλ. 2.4) όσο και τη λέξη-κλειδί (βλ. 2.5), όπως συμβαίνει στο επόμενο παράδειγμα (Πίν. 4) που υπάρχουν τόσα αλφάβητα αντικατάστασης όσα και τα γράμματα της λέξης-κλειδί (π.χ. με τη λέξη-κλειδί ΔΙΠΛΟΣ στην πρώτη στήλη χρησιμοποιούνται έξι αλφάβητα αντικατάστασης).

Πίνακας 4: Το τετράγωνο του Vigenére.

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

Ο Vigenére δημοσίευσε το έργο του το 1585 («Traite des chiffres»), ενώ η τεχνική του παρέμεινε ασφαλής για τρεις αιώνες, μέχρι το 1854, οπότε ο Charles Babbage (ο Βρετανός εφευρέτης της «διαφορικής μηχανής») ανακάλυψε έναν τρόπο κρυπτανάλυσής της. Παρόμοια μέθοδος (απλούστερη, άρα και λιγότερο ασφαλής) ήταν αυτή που επινοήθηκε τον 17^{ο} αιώνα από τον πρώτο Κόμη του Gronsfeld, Βέλγο Jose Maximilien de Bronckhorst.

2.8. Η τεχνική των συμβόλων

Στο κωδικοποιημένο αλφάβητο δεν χρησιμοποιείται για την κρυπτογράφηση ένα κανονικό αλφάβητο, όπως στις μονοαλφαβητικές αντικαταστάσεις (βλ. 2.2-5), αλλά ένα αντίστοιχο σύνολο συμβόλων, που αποτελούν την κλείδα του (Πίν. 5).

Πίνακας 5: Αντικατάσταση μέσω συμβόλων.

Α	Β	Γ	Δ	…	Ω
@	#	$	?	…	&

3. Τεχνικές Κρυπτανάλυσης

Όπου υπάρχει μέτρο, υπάρχει και αντίμετρο. Προφανώς, η επάρκεια μιας μεθόδου κρυπτογράφησης αξιολογείται ως προς την ανθεκτικότητά της στην κρυπτανάλυση. Έτσι για κάθε αλγόριθμο κρυπτογράφησης αναπτύχθηκε και μια τεχνική κρυπτανάλυσης. Οι βασικότερες τεχνικές κρυπτανάλυσης που επινοήθηκαν για την ανάγνωση των κρυπτογραφημάτων αντικατάστασης (βλ. 2.2-8) είναι η *ανάλυση συχνοτήτων*, η τεχνική του *μέγιστου κοινού διαιρέτη* και η τεχνική Babbage-Krasinski (Gómez 2011).

3.1. Η ανάλυση συχνοτήτων

Η πρώτη επιστημονική τεχνική κρυπτανάλυσης που ανακαλύφθηκε βασίζεται στην ανάλυση συχνοτήτων. Έκανε την εμφάνισή της τον 9^{ο} αιώνα μ.Χ., στο έργο του Άραβα λόγιου Al-Kindi, γεννημένου στη Βαγδάτη. Προέρχεται από την προσπάθεια ακριβούς χρονολόγησης των αποσπασματικών πρωτοτύπων γραπτών του Κορανίου. Ο Al-Kindi υπήρξε γιατρός, μαθηματικός, γλωσσολόγος και αστρονόμος. Η πρωτοπόρος εργασία του, ως κρυπταναλυτή, ανακαλύφθηκε μόλις το 1987, σε ένα αντίγραφο της σχετικής πραγματείας του («Εγχειρίδιο αποκρυπτογράφησης κρυπτογραφικών μηνυμάτων») στην Κωνσταντινούπολη.

Η τεχνική της ανάλυσης συχνοτήτων προκύπτει από το ότι για κάθε γλώσσα υπάρχει συγκεκριμένη ποσοστιαία συχνότητα εμφάνισης κάθε γράμματος στα κείμενα της (π.χ. για την Ελληνική: βλ. Mikros et al. 2005). Αν αυτή η συχνότητα δεν είναι γνωστή, τότε μπορεί να μετρηθεί από κείμενα κάποιας ικανής έκτασης. Κατόπιν ακολουθεί η κατάταξη των γραμμάτων του κρυπτογραφήματος κατά συχνότητα εμφάνισης, με φθίνουσα σειρά. Έπειτα πραγματοποιείται η αντιστοίχηση του πρώτου συχνότερου γράμματος του κρυπτογραφήματος με το πρώτο συχνότερο γράμμα των κειμένων της γλώσσας. Ο αλγόριθμος συνεχίζεται έτσι μέχρι την ολοκλήρωση της

αντιστοίχησης όλων των γραμμάτων, είναι δε εξαιρετικά αποτελεσματικός, συνήθως για κρυπτογραφήματα μεγαλύτερα των 100 γραμμάτων.

Όλοι οι μονοαλφαβητικοί αλγόριθμοι αντικατάστασης (βλ. 2.2-5) είναι ευάλωτοι στην ανάλυση συχνοτήτων, αφού το γράμμα αντικατάστασης εμφανίζεται στα κείμενα τόσες φορές όσες και το πρωτότυπο. Ευάλωτη επίσης είναι και η μέθοδος κρυπτογράφησης με την τεχνική των συμβόλων (βλ. 2.8) ή αλλιώς κωδικοποιημένο αλφάβητο. Ένα τέτοιο κωδικοποιημένο αλφάβητο χρησιμοποίησε η ομάδα των Καθολικών αριστοκρατών, που συνωμότησαν για τη δολοφονία της βασίλισσας Ελισάβετ της Α΄ της Αγγλίας, με σκοπό να πάρει τη βασιλεία η Μαρία της Σκωτίας. Η υπηρεσία αντικατασκοπίας της Ελισάβετ, με επικεφαλής τον λόρδο Walsingham, υπέκλεψε επιστολές της Μαρίας προς τον αρχηγό των συνωμοτών Anthony Babington, τις οποίες ο κορυφαίος κρυπταναλυτής της υπηρεσίας, Thomas Phelippes, αποκωδικοποίησε με τη μέθοδο της ανάλυσης συχνοτήτων. Στις 8 Φεβρουαρίου 1587, η Μαρία αποκεφαλίστηκε, αφού κρίθηκε ένοχη εσχάτης προδοσίας στη δίκη που προηγήθηκε. Η πολυαλφαβητική κρυπτογράφηση (βλ. 2.6-7) εφευρέθηκε ως αντίμετρο της τεχνικής ανάλυσης συχνοτήτων.

3.2. Ο Μέγιστος Κοινός Διαιρέτης

Ο μέγιστος κοινός διαιρέτης (εφεξής ΜΚΔ) είναι μια τεχνική κρυπτανάλυσης για την ανάγνωση των ομοπαραλληλικών κρυπτογραφημάτων (βλ. 2.4), ώστε να προσδιοριστεί ο αριθμός μετατόπισης {ν}. Η γενική σχέση του μετασχηματισμού κρυπτογράφησης είναι η

$$K(x) = (\lambda x + \nu) \bmod \alpha$$

όπου οι {λ, ν} είναι ακέραιοι αριθμοί μικρότεροι του {α}. Ένα ομοπαραλληλικό κρυπτογράφημα κρυπταναλύεται με μονοσήμαντο τρόπο μόνον όταν ισχύει η συνθήκη του Bezout:

$$\text{ΜΚΔ}(\lambda, \alpha) = 1$$

οπότε λέμε ότι οι αριθμοί {λ, α}, που είναι τα κλειδιά της κρυπτογράφησης, είναι πρώτοι μεταξύ τους. Διαφορετικά προκύπτουν περισσότερα του ενός αρχικά μηνύματα. Αν επομένως ισχύει η συνθήκη του Bezout, τότε υπάρχει η αντίστροφη σχέση της κρυπτανάλυσης, στην οποία αναζητούμε την τιμή του {x}:

$$\lambda\chi + \nu = \alpha\psi + K$$

όπου

- K: η σειρά του γράμματος αντικατάστασης και
- ψ: το πηλίκο της ακεραίας διαίρεσης (λx + ν)/α.

Ο αλγόριθμος κρυπτανάλυσης αντικατάστασης θα έπρεπε να αναλύσει $(\alpha-1)^2$ πιθανά κλειδιά, αφού

$$1 \leq \{\lambda, \nu\} \leq (\alpha-1)$$

δηλαδή για το ελληνικό αλφάβητο (α = 24) 529 συνδυασμούς. Όμως επειδή ο ΜΚΔ(λ, α) = 1, οι συνδυασμοί αυτοί είναι 184, γιατί μόνον οκτώ (8) ακέραιοι αριθμοί από το {1} μέχρι το {23} στη θέση του {λ} ικανοποιούν τη συνθήκη του Bezout (= {1 , 5 , 7 , 11 , 13 , 17 , 19 , 23}).

3.3. Η τεχνική Babbage-Krasinski

Η τεχνική Babbage-Krasinski προσπαθεί να βρει το μήκος της λέξης-κλειδί (βλ. 2.5), το οποίο προσδιορίζει και το πλήθος των κρυπτογραφικών αλφάβητων (βλ. 2.7). Ο αλγόριθμος κρυπτανάλυσης αρχίζει με τη δημιουργία μια λίστας από διγράμματα (δύο διαδοχικοί χαρακτήρες του κρυπτογραφήματος) που επαναλαμβάνονται στο κρυπτογράφημα. Μετριέται το πλήθος των γραμμάτων που παρεμβάλλονται από τη μία εμφάνιση του διγράμματος στην επόμενη (έστω διάκενο). Βρίσκονται οι ακέραιοι διαιρέτες για κάθε πλήθος διακένου. Το μήκος της λέξης-κλειδί είναι ένας από αυτούς τους κοινούς διαιρέτες, έστω το {6} (Πίν. 4). Έτσι καταλήγουμε σ' ένα πλήθος από έξι (6) μονοαλφαβητικά κρυπτογραφήματα. Η τεχνική αυτή είναι αποτελεσματική για κάθε πολυαλφαβητικό κρυπτογράφημα (βλ. 2.6-7).

Η κρυπτανάλυση ενός πολυαλφαβητικού κρυπτογραφήματος επιτεύχθηκε αρχικά το 1854, από τον Βρετανό διαπρεπή επιστήμονα και εφευρέτη Charles Babbage (1791-1871), ο οποίος όμως δεν δημοσίευσε ποτέ το αποτέλεσμα της ανακάλυψής του. Το επίτευγμά του αυτό αναγνωρίστηκε πρόσφατα, μετά από μελέτη των σημειώσεών του. Μέχρι τότε, μια παρόμοια τεχνική του Πρώσου αξιωματούχου Friedrich Krasinski ήταν γνωστή από το 1863.

4. Μερική Συλλαβική Αντικατάσταση

Η τεχνική κρυπτογράφησης με *μερική συλλαβική αντικατάσταση* (εφεξής ΜεΣΑ), είναι εμπνευσμένη από τις προϊστορικές γραφές που χρησιμοποιήθηκαν στην περιοχή του Αιγαίου κατά τη 2η χιλιετία π.Χ. (Παπακίτσος 2017, Papakitsos 2018) και περιλαμβάνουν τρία συλλαβάρια, δηλαδή συστήματα γραφής όπου το κάθε σημείο αντιστοιχεί σε μία συλλαβή, συνήθως της μορφής συμφώνου-φωνήεντος (CV), και όχι σε έναν φθόγγο συμφώνου (C) ή έναν φωνήεντος (V), όπως συμβαίνει συνήθως στο αλφάβητο (με εξαίρεση τα διπλά σύμφωνα {Ξ} και {Ψ}). Οι γραφές αυτές περιλαμβάνουν την Κρητική Ιερογλυφική, τη Γραμμική Α΄ και τη Γραμμική Β΄ (Davis 2010). Ένα πλήθος μελετών υποδεικνύουν την ύπαρξη μίας γραφής, της Κρητικής Πρωτογραμμικής, από την οποία προήλθαν τα παραπάνω συστήματα γραφής (Κενανίδης 1992, 2013, Papakitsos 2019, Willetts 1977).

Παρατηρώντας αναλυτικότερα την περίπτωση του συλλαβάριου, φαίνεται ότι σχεδόν κάθε συλλαβόγραμμα (Si) αντιπροσωπεύει δύο διαδοχικούς φθόγγους, δηλαδή ένα σύμφωνο (Ci) και ένα φωνήεν (Vi), έχοντας τον φωνητικό μορφότυπο: Si = CiVi. Έτσι σ' ένα αλφάβητο όπως το λατινικό, δύο διαδοχικά σύμβολα {CiVi} αντιστοιχούνται σε ένα σύμβολο {Si} του συλλαβάριου, όπως στο ακόλουθο παράδειγμα:

$$\{DA\} = \{\text{┣}\},\ \{PA\} = \{\text{╪}\}.$$

Στην κωδικοποίηση Unicode (ή UTF-8) υπάρχουν αρκετοί χαρακτήρες ώστε να γίνει η αντιστοίχηση ενός συλλαβικού ζεύγους χαρακτήρων της ελληνικής γλώσσας, με μορφότυπο {CV} (όπως π.χ. η συλλαβή {BA}), προς έναν χαρακτήρα Unicode (όπως π.χ. ο {ß}):

$$\{BA\} = \{ß\}.$$

Έτσι επιτυγχάνεται όχι μόνο μια συμπίεση του αρχικού αρχείου κειμένου αλλά και η κρυπτογράφησή του, σύμφωνα με την κλείδα αντιστοίχησης.

4.1. Η κλείδα

Ένα απλοποιημένο παράδειγμα κλείδας κρυπτογράφησης με τη μέθοδο ΜεΣΑ για την ελληνική γλώσσα φαίνεται στον Πίν. 6.

Πίνακας 6: Παράδειγμα κλείδας κρυπτογράφησης ΜεΣΑ.

	∅	**A**	**E**	**H**	**I**	**O**	**Y**	**Ω**
∅		Ṽ	Õ	Œ	R̂	Ë	Ő	Ḱ
B	Ẅ	ß	ŵ	b	w	û	v	þ
Γ	D̲	ý	ĝ	ś	ģ	å	ğ	š
Δ	ẑ	ď	ā	d	á	ġ	ă	đ
Z	Z̲	Ĉ	j	z	g	ŝ	ḡ	ş
Θ	ẋ	ð	ō	ķ	ó	ǩ	a	Ť
K	L̲	ħ	ḱ	k	o	ķ	õ	k̲
Λ	Ṁ	Ł	ï	l	ê	ň	ĭ	ł
M	Ṅ	Ď	ē	m	ľ	ė	ȟ	ä
N	Ẋ	ʼn	ń	c	ņ	n̲	ŀ	ñ
Ξ	Ṗ	Ĥ	e	x	ĵ	ĥ	q	o̲
Π	Ṙ	Ħ	ã	r	æ	î	r̈	ë
P	Ṡ	Þ	ŗ	p	ŕ	œ	ř	ě
Σ	Ṫ	ĉ	ć	s	n	ċ	č	ç
T	Ẁ	ť	ŧ	ő	ţ	ĩ	ţ	i
Φ	ẋ	ô	t	f	ò	ö	ŏ	O
X	Ẏ	ɦ	ḣ	y	ḥ	ü	h̲	ɧ
Ψ	Ẃ	Ý	ù	h	ú	ḧ	u	ÿ

Ο πίνακας της Κλείδας (Πίν. 6) αποτελείται από 8 στήλες και 18 γραμμές, χωρίς τις αντίστοιχες επικεφαλίδες γραμμών και στηλών (με έντονα γράμματα):

- Κάθε στήλη αντιστοιχεί σε ένα φωνήεν του οποίου προηγείται κάποιο σύμφωνο, με αλφαβητική σειρά, ενώ η πρώτη στήλη αντιστοιχεί σε κάθε σύμφωνο που δεν ακολουθείται από φωνήεν.

- Κάθε γραμμή αντιστοιχεί σε ένα σύμφωνο του οποίου ακολουθεί φωνήεν, με αλφαβητική σειρά, ενώ η πρώτη γραμμή αντιστοιχεί σε κάθε φωνήεν του οποίου δεν προηγείται κάποιο σύμφωνο.

Όταν στο κείμενο προς κρυπτογράφηση υπάρχει μια συλλαβή (δηλαδή ακολουθία χαρακτήρων) της μορφής {σύμφωνο+φωνέν} (π.χ. «κο»), τότε αυτή αντικαθίσταται στο κρυπτογράφημα με τον χαρακτήρα που βρίσκεται στη γραμμή του συμφώνου και στη στήλη του φωνήεντος («κο» = «ķ»). Σε κάθε άλλη περίπτωση, τα φωνήεντα αντικαθίστανται από τους αντίστοιχούς τους χαρακτήρες στην πρώτη γραμμή του πίνακα και τα σύμφωνα αντικαθίστανται από τους αντίστοιχούς τους χαρακτήρες στην πρώτη στήλη. Οι υπόλοιποι χαρακτήρες (σημεία στίξεως, κενά) αγνοούνται. Στην αποκρυπτογράφηση ακολουθείται η αντίστροφη διαδικασία, που όμως μετατρέπει τα πεζά γράμματα σε κεφαλαία.

4.2. Αποτελέσματα

Η παρουσιαζόμενη τεχνική κρυπτογράφησης (ΜεΣΑ) υλοποιήθηκε πειραματικά με τη γλώσσα προγραμματισμού Python (Αράπογλου κ.ά. 2017α, 2017β), αρχικά στην ελληνική γλώσσα με διαφορετική κλείδα (Παπακίτσος 2017) και αργότερα στην αγγλική γλώσσα (Papakitsos 2018). Στην παρούσα εφαρμογή παρατίθεται ως παράδειγμα το αποτέλεσμα της κρυπτογράφησης της ακόλουθης πρότασης (Αράπογλου κ.ά. 2017α: 3):

> «Αν παρατηρήσουμε τον κόσμο γύρω μας, θα διαπιστώσουμε ότι κατακλυζόμαστε από ποικίλες εφαρμογές υπολογιστών, που χρησιμοποιούμε καθημερινά μέσα από διαφορετικές συσκευές.»

Με τη χρήση της κλείδας του Πίν. 6, ο αλγόριθμος κρυπτογράφησης (Σχ. 1) παράγει το ακόλουθο κρυπτογράφημα:

> Ṽ Ẋ Ħ Þ ő p ċ Ő ē ĩ Ẋ ķ Ṫ ė ğ ě Ď Ṫ ð á Ṽ æ Ṫ i ċ Ő ē Ë ţ ħ ť Ļ ĭ ŝ Ď Ṫ ŧ Ṽ
> î î Ř o ï Ṫ Õ ô Ṡ ė ĝ Ṫ Ő î ň ġ Ṫ i Ẋ î Ő Ẏ p n ė î Ř Ë Ő ē ħ ķ ē ŕ ʼn ē ĉ Ṽ î
> á Ṽ ö ŗ ţ ḱ Ṫ č Ṫ ḱ Ő Õ Ṫ

μετά από αντικατάσταση των γραμμάτων και συλλαβών συμφώνου-φωνήεντος του αρχικού μηνύματος (για ευκρίνεια διαχωρίζονται με παύλα):

Α-ν-πα-ρα-τη-ρή-σο-υ-με-το-ν-κό-σ-μο-γύ-ρω-μα-ς-θα-δι-α-πι-σ-τώ-σο-υ-με-ό-τι-κα-τα-κ-λυ-ζό-μα-σ-τε-α-πό-πο-ι-κί-λε-ς-ε-φα-ρ-μο-γέ-ς-υ-πο-λο-γι-σ-τώ-ν-πο-υ-χ-ρη-σι-μο-πο-ι-ο-ύ-με-κα-θη-με-ρι-νά-μέ-σα-α-πό-δι-α-φο-ρε-τι-κέ-ς-συ-σ-κε-υ-έ-ς

Η διαδικασία αποκρυπτογράφησης (Σχ. 1) επαναφέρει το αρχικό κείμενο σε διαφορετική μεν αλλά κατανοητή μορφή (ανάλογη των αρχαίων ελληνικών επιγραφών):

ΑΝΠΑΡΑΤΗΡΗΣΟΥΜΕΤΟΝΚΟΣΜΟΓΥΡΩΜΑΣΘΑΔΙΑΠΙΣΤΩΣΟΥΜ
ΕΟΤΙΚΑΤΑΚΛΥΖΟΜΑΣΤΕΑΠΟΠΟΙΚΙΛΕΣΕΦΑΡΜΟΓΕΣΥΠΟΛΟΓΙΣ
ΤΩΝΠΟΥΧΡΗΣΙΜΟΠΟΙΟΥΜΕΚΑΘΗΜΕΡΙΝΑΜΕΣΑΑΠΟΔΙΑΦΟΡΕ
ΤΙΚΕΣΣΥΣΚΕΥΕΣ

Η κρυπτογράφηση του αρχικού μηνύματος με τη μορφή κεφαλαίων γραμμάτων αποτρέπει τη δυνατότητα αξιοποίησης στατιστικών για τη συχνότητα εμφάνισης των χαρακτήρων της ελληνικής γλώσσας σε γραπτά κείμενα (βλ. Mikros et al. 2005), με σκοπό την κρυπτανάλυση, εάν δεν είναι γνωστή η μέθοδος κρυπτογράφησης (ΜεΣΑ). Επιπροσθέτως, η παράληψη των κενών χαρακτήρων και των σημείων στίξεως στο κρυπτογράφημα παρεμποδίζει την αξιοποίηση των στατιστικών μεγέθους λέξεων (βλ. Παπακίτσος 2000) για τον εντοπισμό τους. Τέλος, ενώ το αρχικό μήνυμα έχει μέγεθος 168 χαρακτήρων (μαζί με τα κενά και τα σημεία στίξεως), το κρυπτογράφημα έχει μέγεθος 90 χαρακτήρων, γεγονός που επιτρέπει τη χρήση της ΜεΣΑ και ως μεθόδου συμπίεσης κειμένων.

5. Συμπεράσματα

Η ΜεΣΑ πραγματοποιεί μερική συλλαβική αντικατάσταση, δηλαδή αντικαθίστανται με έναν χαρακτήρα της κλείδας (Πίν. 6) μόνον εκείνες οι συλλαβές που έχουν τον φωνητικό μορφότυπο {σύμφωνο-φωνήεν}. Έτσι όμως στο πρόγραμμα κρυπτογράφησης, το πρωτότυπο κείμενο δεν κρυπτογραφείται ομοιόμορφα, αφού σε άλλες περιπτώσεις ένας χαρακτήρας του κώδικα κρυπτογράφησης αντικαθιστά ένα γράμμα του πρωτότυπου κειμένου ενώ σε άλλες περιπτώσεις αντικαθιστά ένα ζεύγος γραμμάτων (με τον φωνητικό μορφότυπο {σύμφωνο-φωνήεν}, όπως συμβαίνει με ένα συλλαβόγραμμα) του πρωτοτύπου από την κλείδα (Πίν. 6). Δηλαδή:

- Στην περίπτωση της κρυπτανάλυσης συχνοτήτων (βλ. 3.1) αλλοιώνεται δραστικά η συχνότητα εμφάνισης κάθε γράμματος του πρωτότυπου κειμένου, αφού στο κρυπτογράφημα π.χ. ένα {α} άλλοτε εμφανίζεται μόνο του και άλλοτε μαζί με 17 διαφορετικά σύμφωνα από τους συνδυασμούς συλλαβογραμμάτων της κλείδας (Πίν. 6).
- Στην περίπτωση της κρυπτανάλυσης ΜΚΔ (βλ. 3.2) δεν πρόκειται για ομοπαραλληλικό κρυπτογράφημα (βλ. 2.4), αφού άλλοτε έχουμε αντικατάσταση ενός γράμματος του πρωτότυπου κειμένου και άλλοτε δύο γραμμάτων μαζί (ζεύγος συμφώνου-φωνήεντος) από έναν χαρακτήρα-συλλαβόγραμμα.
- Στην περίπτωση της κρυπτανάλυσης Babbage-Krasinski (βλ. 3.3) δεν έχουμε πρωτότυπο κείμενο με σταθερά διγράμματα, αφού δύο διαδοχικοί χαρακτήρες του κρυπτογραφήματος άλλοτε αντιστοιχούν σε δύο διαδοχικά γράμματα του πρωτότυπου κειμένου και άλλοτε σε τρία (συλλαβόγραμμα + γράμμα).

Επιπλέον, με την παράληψη της αντικατάστασης των κενών χαρακτήρων και των σημείων στίξεως δεν μπορούν να αξιοποιηθούν εύκολα οι στατιστικές μεγέθους λέξεων (βλ. Παπακίτσος 2000) για τον εντοπισμό τους κατά την κρυπτανάλυση. Επομένως, η κρυπτογράφηση Μερικής Συλλαβικής Αντικατάστασης (ΜεΣΑ) είναι ιδιαίτερα ανθεκτική στις τεχνικές κρυπτανάλυσης (βλ. 3.1-3) και άρα εξαιρετικά επαρκής και χρήσιμη για το σκοπό που δημιουργήθηκε.

Παραπομπές

1. Αράπογλου Α., Βραχνός Ε., Κανίδης Ε., Λέκκα Δ., Μακρυγιάννης Π., Μπελεσιώτης Β., Παπαδάκης Σ. και Τζήμας Δ. (2017β). «Προγραμματισμός Υπολογιστών: Σημειώσεις Μαθητή (Γ΄ τάξη ημερησίων και Δ' τάξη εσπερινών ΕΠΑ.Λ., του Τομέα Πληροφορικής: Έκδοση 2η)», *Αθήνα, Ινστιτούτο Εκπαιδευτικής Πολιτικής*.
2. Αράπογλου Α., Βραχνός Ε., Κανίδης Ε., Μακρυγιάννης Π., Μπελεσιώτης Β. και Τζήμας Δ. (2017α). «Αρχές Προγραμματισμού Υπολογιστών: Σημειώσεις Μαθητή (Β΄ τάξη ημερησίων και Γ΄ τάξη εσπερινών ΕΠΑ.Λ., του Τομέα Πληροφορικής: Έκδοση 2η)», *Αθήνα, Ινστιτούτο Εκπαιδευτικής Πολιτικής*.

3. Κενανίδης Ι. (1992). «Ετεόκρητες Μεγαλήτορες», *Αθήνα, Εθνική Βιβλιοθήκη της Ελλάδος*.
4. Κενανίδης Ι. (2013). «Ιστορικές και γλωσσικές μελέτες: cwepeker.doc», *Καβάλα, Ε.Π. Λαζίδου*.
5. Παπακίτσος Ε.Χ. (2000). «Συμβολή στη Μορφολογική Επεξεργασία της Νέας Ελληνικής: Λειτουργική Αποσύνθεση - Καρτεσιανό Ηλεκτρονικό Λεξικό», Διδακτορική διατριβή, Τμήμα Πληροφορικής & Τηλεπικ/νιών του ΕΚΠΑ.
6. Παπακίτσος Ε.Χ. (2013β). «Φυσική Γλώσσα & Υπολογιστικά Μαθηματικά», *Αθήνα, Διεπιστημονικό Διαπανεπιστημιακό ΠΜΣ «Τεχνογλωσσία»* (ΕΚΠΑ & ΕΜΠ).
7. Παπακίτσος Ε.Χ. (2017). «Τεκμηρίωση λογισμικού συλλαβικής συμπίεσης ελληνικών κειμένων με πειραματική κρυπτογράφηση σε γλώσσα προγραμματισμού Python», *Αθήνα*, ISBN 978-618-83461-0-9.
8. Davis B. (2010). “Introduction to the Aegean Pre-Alphabetic Scripts”. *KUBABA*, 1 : 38-61.
9. Deulofeu J. (2011). «Ο κόσμος είναι μαθηματικά: Η θεωρία των παιγνίων», *Αθήνα, Εκδόσεις 4π*.
10. Gómez J. (2011). «Ο κόσμος είναι μαθηματικά: Κωδικοποίηση και κρυπτογραφία», *Αθήνα, Εκδόσεις 4π*.
11. Mikros G., Hatzigeorgiu N. and Carayannis G. (2005). “Basic Quantitative Characteristics of the Modern Greek Language Using the Hellenic National Corpus”. *Journal of Quantitative Linguistics*, 12(2-3) : 167-184.
12. Papakitsos E.C. (2018). “A software application of ancient syllabaries to cryptography”. *Journal of Software Engineering & Intelligent Systems*, 3(3): 348-353.
13. Papakitsos E.C. (2019). “Standardizing the Cretan Protolinear Syllabary”. *Migration & Diffusion*, 2019 : 1-11.
14. Willetts R.F. (1977). “The Civilization of Ancient Crete. California”, *University of California Press*.