



5^η Εργασία στη Θεματική Ενότητα ΠΛΗΣ-62 ("Εξειδικεύσεις Δικτύων και Επικοινωνιών")

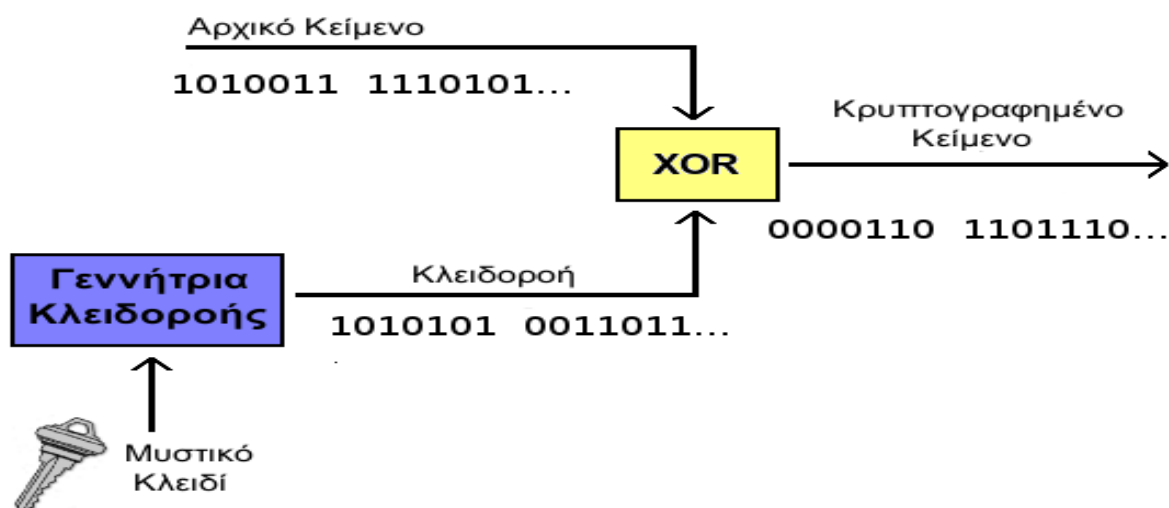
(Θέμα 1) Ο 7-bit κώδικας ASCII αναπαριστά γράμματα, ψηφία και σημεία στίξης σαν χαρακτήρες από το σύνολο των ακεραίων στο διάστημα 32...127. Τα γράμματα Α...Ζ συμβολίζονται με τα νούμερα 65...90 και τα γράμματα α...z με τα νούμερα 97...112 αντιστοίχως. Οι χαρακτήρες γράφονται βάσει του 2, ως επτάδες δυαδικών ψηφίων. Ανιχνεύετε τη συμβολοσειρά:

00001101101110101011111101110100110111100100111100001011
00010101010101

Υπάρχει η βάσιμη υποψία ότι πρόκειται για μήνυμα κωδικοποιημένο σε 7-bit ASCII χρησιμοποιώντας stream-cipher που βασίζεται σε καταχωρητή ολίσθησης. Τα πρώτα δύο γράμματα του μηνύματος είναι "Su". Να αποκρυπτογραφήσετε το μήνυμα.

Για να αποκρυπτογραφήσουμε το μήνυμα θα χρησιμοποιήσουμε έναν κρυπτογραφικό αλγόριθμο ροής (stream cipher). Οι κρυπτογραφικοί αλγόριθμοι ροής χρησιμοποιούνται για την κρυπτογράφηση μιας συνεχούς ροής δεδομένων (data stream). Για την κρυπτογράφηση επιλέγεται αρχικά μια γεννήτρια κλειδοροής (keystream generator) η οποία δέχεται ως είσοδο κάποιο μυστικό κλειδί και παράγει στην έξοδό της μια ψευδοτυχαία ακολουθία bits η οποία ονομάζεται κλειδοροή (keystream) όπως φαίνεται στο σχήμα 1. Στη συνέχεια εφαρμόζεται η συνάρτηση XOR ανάμεσα στο αρχικό κείμενο και στην κλειδοροή και το αποτέλεσμα της συνάρτησης είναι η τελική κρυπτογραφημένη ροή δεδομένων.

Σχήμα 1





Στην συγκεκριμένη άσκηση γνωρίζουμε την τελική συμβολοσειρά που έχουμε ανιχνεύσει, όπως επίσης και τα πρώτα 14 bits του αρχικού κειμένου, αφού ξέρουμε ότι τα πρώτα δύο γράμματα του μηνύματος είναι "Su". Άρα με XOR μπορούμε να υπολογίσουμε τα πρώτα 14 bits κλειδοροής.

Για το αρχικό μήνυμα έχουμε τα γράμματα:

S --> 83 δηλαδή σε δυαδική μορφή 1010011

u --> 117 δηλαδή 111101

Άρα το αρχικό κείμενο είναι:

1010011 1110101

Για το τελικό κρυπτογραφημένο κείμενο έχουμε τα πρώτα 14 bits:

0000110 1101110

Χρησιμοποιώντας την συνάρτηση XOR έχουμε για την κλειδοροή τα πρώτα 14 bits:

1010101 0011011

Όπως αναφέρεται στο Handbook of Applied Cryptography ένας σύγχρονος κρυπτογραφικός αλγόριθμος (κρυπταλγόριθμος) ροής είναι αυτός στον οποίο η κλειδοροή παράγεται ανεξάρτητα από το μήνυμα απλού κειμένου (plaintext) και από το κρυπτοκείμενο (ciphertext).

Από το ίδιο βιβλίο αναφέρουμε και τον παρακάτω ορισμό:

Ένας καταχωρητής ολίσθησης με γραμμική ανάδραση (LFSR – Linear Feedback Shift Register) μήκους L συνίσταται σε L στάδια (ή στοιχεία καθυστέρησης) αριθμητικά 0, 1, 2, ..., L, με το καθένα να είναι ικανό να αποθηκεύει 1 bit και να έχει μία είσοδο και μία έξοδο και ένα ρολόι το οποίο ελέγχει την κίνηση των δεδομένων. Κατά την διάρκεια κάθε μονάδας χρόνου εκτελούνται οι εξής λειτουργίες:

α) εξάγεται το περιεχόμενο του σταδίου 0 που αποτελεί και μέρος της ακολουθίας εξόδου,

β) το περιεχόμενο του σταδίου i μετακινείται στο στάδιο i-1 για κάθε $1 < i < L-1$ και

γ) το νέο περιεχόμενο του σταδίου L-1 είναι το bit ανάδρασης a_N το οποίο υπολογίζεται με πρόσθεση modulo 2 των προηγούμενων περιεχομένων ενός συγκεκριμένου υποσυνόλου των σταδίων 0, 1, ..., L. Οι καταχωρητές ολίσθησης με γραμμική πολυπλοκότητα μπορούν να παράγουν ψευδοτυχαίες ακολουθίες με ελεγχόμενη περίοδο. Εμείς θα προσδιορίσουμε το χαρακτηριστικό πολυώνυμο της γραμμικής συνάρτησης ανάδρασης χρησιμοποιώντας τον αλγόριθμο Berlekamp και Massey. Η δυαδική ακολουθία που έχουμε στην διάθεσή μας έχει



μήκος $n=14$ και είναι αυτή που προσδιορίσαμε χρησιμοποιώντας την συνάρτηση XOR δηλαδή η $a^{14} = [1010101\ 0011011]$.

Η παράθεση του αλγόριθμου γίνεται συνοπτικά με τα παρακάτω 10 βήματα:

- 1) Δίνουμε αρχικές τιμές στις παρακάτω μεταβλητές:
Στο χαρακτηριστικό πολυώνυμο $f(x)=1$
Στην προσωρινή μεταβλητή $b(x)=1$
Στο μέγεθος του καταχωρητή ολίσθησης $L=0$
Στον μετρητή $N=0$
Σε προσωρινή αποθήκευση μετρητή $m=-1$
- 2) Ελέγχουμε την τιμή του μετρητή N . Όσο αυτή η τιμή είναι μικρότερη του n τότε συνεχίζουμε, αλλιώς πηγαίνουμε στο βήμα 10.
- 3) Υπολογίζουμε την διαφορά της πρόβλεψης από την ακολουθία. Δίνουμε στην μεταβλητή d την τιμή

$$d = a_N + \sum_{i=1}^L c_i a_{N-i}$$

- 4) Υπάρχει διαφορά; Εάν όχι, δηλαδή $d=0$ πηγαίνουμε στο βήμα 9
- 5) Εάν υπάρχει διαφορά δηλαδή $d=1$ τότε αποθηκεύουμε αρχικά το πολυώνυμο

$$f'(x) = f(x)$$

και υπολογίζουμε την νέα του μορφή

$$f(x) = f(x) + b(x) \cdot x^{N-m}$$

- 6) Ελέγχουμε αν το μέγεθος του καταχωρητή είναι μεγαλύτερο του $N/2$
- 7) Εάν είναι δηλαδή $L > \frac{N}{2}$, τότε πηγαίνουμε στο βήμα 9
- 8) Εάν είναι $L \leq \frac{N}{2}$ τότε αυξάνουμε το μέγεθος του καταχωρητή ανάλογα δηλαδή $L = N + 1 - L$, αποθηκεύουμε το παλιό πολυώνυμο $b(x) = f'(x)$ και αποθηκεύουμε την τρέχουσα τιμή του N στην προσωρινή μεταβλητή m δηλαδή $m = N$



9) Αυξάνουμε την τιμή του N και πηγαίνουμε στο βήμα 2

10) Το χαρακτηριστικό πολυώνυμο είναι το $f(x)$. Τέλος!

Καθώς τερματίζει ο αλγόριθμος έχουμε τις μεταβλητές L και $f(x)$ που περιέχουν το μέγεθος του καταχωρητή ολίσθησης και το χαρακτηριστικό πολυώνυμο αντίστοιχα. Αυτές οι δύο παράμετροι καθορίζουν πλήρως έναν LFSR.

Τα αποτελέσματα των βημάτων του αλγόριθμου καθορισμού του χαρακτηριστικού πολυωνύμου συνοψίζονται στον παρακάτω πίνακα 1. Όπως φαίνεται από τον πίνακα 1 το χαρακτηριστικό πολυώνυμο βρέθηκε να είναι $f(x) = 1 + x + x^4 + x^6 + x^7$, ενώ το μέγεθος του καταχωρητή είναι 7 bits. Με αυτές τις πληροφορίες μπορούμε να κατασκευάσουμε την γεννήτρια όπως φαίνεται στο σχήμα 2.

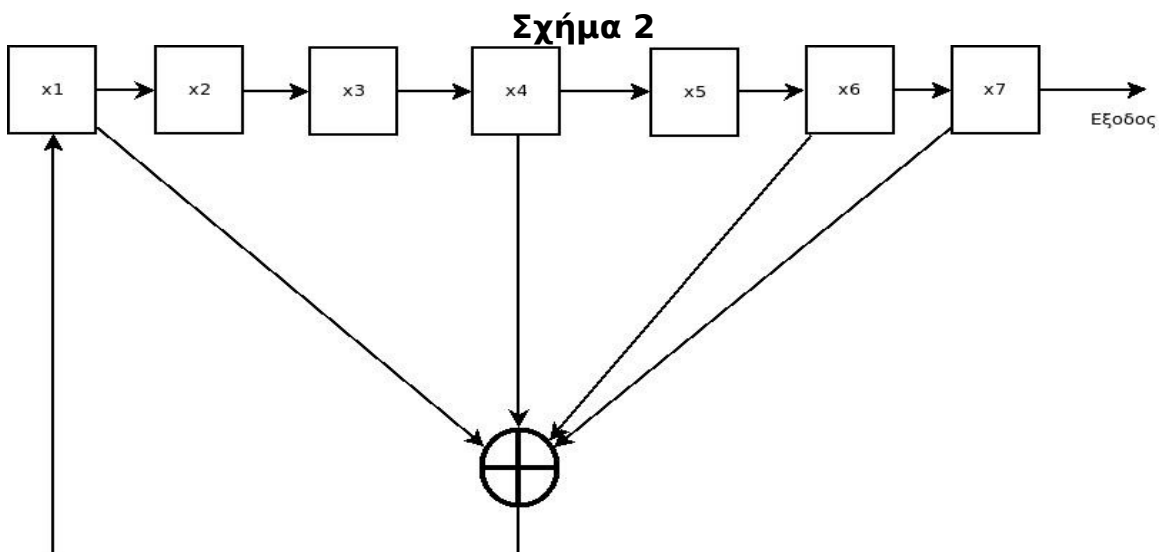
Η αρχική κατάσταση του καταχωρητή είναι η δυαδική ακολουθία 1010101. Τότε η έξοδος είναι 1 δηλαδή η δεξιότερη βαθμίδα. Την επόμενη χρονική στιγμή η κατάσταση θα είναι η 0101010 και η έξοδος είναι 0. Αυτή η κατάσταση 0101010 προκύπτει ως εξής: Το 0 είναι το XOR των x_1 , x_4 , x_6 και x_7 δηλαδή της 1^{ης}, 4^{ης}, 6^{ης} και 7^{ης} βαθμίδας ενώ όλα τα υπόλοιπα bits προήλθαν από μια ολίσθηση προς τα δεξιά των βαθμίδων.

Πίνακας 1

a_N	d	$f'(x)$	$f(x)$	L	m	$b(x)$	N
-	-	-	1	0	-1	1	0
1	1	1	$1+x$	1	0	1	1
0	1	$1+x$	1	1	0	1	2
1	1	1	$1+x^2$	2	2	1	3
0	0	1	$1+x^2$	2	2	1	4
1	0	1	$1+x^2$	2	2	1	5
0	0	1	$1+x^2$	2	2	1	6
1	0	1	$1+x^2$	2	2	1	7
0	0	1	$1+x^2$	2	2	1	8
0	1	$1+x^2$	$1+x^2+x^6$	7	8	$1+x^2$	9
1	1	$1+x^2+x^6$	$1+x+x^2+x^3+x^6$	7	8	$1+x^2$	10
1	1	$1+x+x^2+x^3+x^6$	$1+x+x^3+x^4+x^6$	7	8	$1+x^2$	11
0	1	$1+x+x^3+x^4+x^6$	$1+x+x^4+x^5+x^6$	7	8	$1+x^2$	12



1	0	$1+x+x^3+x^4+x^6$	$1+x+x^4+x^5+x^6$	7	8	$1+x^2$	13
1	1	$1+x+x^4+x^5+x^6$	$1+x+x^4+x^6+x^7$	7	8	$1+x^2$	14



Ο υπολογισμός ολόκληρης της κλειδοροής γίνεται στον πίνακα 2.

Πίνακας 2

x_1	x_2	x_3	x_4	x_5	x_6	x_7
1	0	1	0	1	0	1
0	1	0	1	0	1	0
0	0	1	0	1	0	1
1	0	0	1	0	1	0
1	1	0	0	1	0	1
0	1	1	0	0	1	0
1	0	1	1	0	0	1
1	1	0	1	1	0	0
0	1	1	0	1	1	0
1	0	1	1	0	1	1
0	1	0	1	1	0	1
0	0	1	0	1	1	0
1	0	0	1	0	1	1
0	1	0	0	1	0	1
1	0	1	0	0	1	0



ΕΛΛΗΝΙΚΟ ΑΝΟΙΚΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

0	1	0	1	0	0	1
0	0	1	0	1	0	0
0	0	0	1	0	1	0
0	0	0	0	1	0	1
1	0	0	0	0	1	0
0	1	0	0	0	0	1
1	0	1	0	0	0	0
1	1	0	1	0	0	0
0	1	1	0	1	0	0
0	0	1	1	0	1	0
0	0	0	1	1	0	1
0	0	0	0	1	1	0
1	0	0	0	0	1	1
1	1	0	0	0	0	1
0	1	1	0	0	0	0
0	0	1	1	0	0	0
1	0	0	1	1	0	0
0	1	0	0	1	1	0
1	0	1	0	0	1	1
1	1	0	1	0	0	1
1	1	1	0	1	0	0
1	1	1	1	0	1	0
1	1	1	1	1	0	1
1	1	1	1	1	1	0
1	1	1	1	1	1	1
0	1	1	1	1	1	1
1	0	1	1	1	1	1
0	1	0	1	1	1	1
1	0	1	0	1	1	1
1	1	0	1	0	1	1
0	1	1	0	1	0	1
1	0	1	1	0	1	0



1	1	0	1	1	0	1
1	1	1	0	1	1	0
0	1	1	1	0	1	1
1	0	1	1	1	0	1
1	1	0	1	1	1	0
1	1	1	0	1	1	1
1	1	1	1	0	1	1
0	1	1	1	1	0	1
0	0	1	1	1	1	0
0	0	0	1	1	1	1
1	0	0	0	1	1	1
1	1	0	0	0	1	1
1	1	1	0	0	0	1
0	1	1	1	0	0	0
1	0	1	1	1	0	0
0	1	0	1	1	1	0
0	0	1	0	1	1	1
0	0	0	1	0	1	1

Από την τελευταία στήλη του πίνακα έχουμε ουσιαστικά την έξοδο των bits και τον σχηματισμό της ακολουθίας της κλειδοροής. Ομαδοποιούμε ανά επτά όλα τα bits της κλειδοροής και χρησιμοποιούμε την συνάρτηση XOR με τις αντίστοιχες επτάδες της ακολουθίας του κρυπτοκειμένου όπως φαίνεται στον πίνακα 3. Η τελευταία στήλη του πίνακα μας δίνει την αποκρυπτογράφηση του μηνύματος.

Πίνακας 3

Κλειδοροή	Κρυπτοκειμένο	XOR	Dec	χαρακτήρας
1010101	0000110	1010011	83	S
0011011	1101110	1110101	117	u
0100101	1010111	1110010	114	r
0000101	1110111	1110010	114	r
1000011	0100110	1100101	101	e
0010111	1111001	1101110	110	n



1111010	0011110	1100100	100	d
1101110	0001011	1100101	101	e
1111000	0001010	1110010	114	r
1110100	1010101	0100001	33	!

Τελικά μας παραδόθηκε το αρχικό μήνυμα και είναι το

“Surrender!”

(Θέμα 2) Να βρείτε όλους τους ακραίους οι οποίοι αφήνουν υπόλοιπα 1, 2, 3 όταν διαιρεθούν με το 9, 8 και 7 αντιστοίχως.

Για να λύσουμε αυτό το θέμα θα κάνουμε χρήση του Γενικευμένου Αλγόριθμου του Ευκλείδη και του Κινέζικου Θεωρήματος Υπολοίπων. Ξεκινάμε με την έννοια της σχέσης ισοτιμίας modulo ενός φυσικού αριθμού. Αν θεωρήσουμε έναν φυσικό αριθμό m μεγαλύτερο του 1, τότε κάθε ακέραιος διαιρούμενος δια m αφήνει υπόλοιπο έναν από τους αριθμούς

1, 2, ..., $m-1$.

Όταν δύο ακέραιοι διαιρούμενοι δια m αφήνουν το ίδιο υπόλοιπο, τότε αυτοί ονομάζονται ισότιμοι ή ισοδύναμοι ως προς m (modulo m). Δηλαδή εάν a , b , m είναι ακέραιοι αριθμοί με $m > 1$ τότε λέμε ότι ο a είναι ισότιμος (ή ισοδύναμος) με τον b modulo m και γράφουμε

$$a \equiv b \pmod{m}$$

αν οι αριθμοί a και b αφήνουν το ίδιο υπόλοιπο, όταν διαιρεθούν δια m .

Τον γενικευμένο αλγόριθμο του Ευκλείδη θα τον χρησιμοποιήσουμε για να υπολογίσουμε πολλαπλασιαστικούς αντίστροφους φυσικών αριθμών ως προς κάποια σχέση ισοτιμίας.

Γενικευμένος Αλγόριθμος Ευκλείδη.

Υποθέτουμε ότι b και n είναι δύο φυσικοί με $b < n$ και θέλουμε να ελέγξουμε:

1) Αν υπάρχει αριθμός x τέτοιος ώστε

$$xb \equiv 1 \pmod{n}$$



2) Στην περίπτωση που υπάρχει θέλουμε και να υπολογίσουμε αυτόν τον πολλαπλασιαστικό αντίστροφο x .

Ο αλγόριθμος του Ευκλείδη μας δίνει άμεσα απάντηση στο πρώτο μέρος του προβλήματος. Συγκεκριμένα αν τον εφαρμόσουμε για τους φυσικούς $r_1 = b$, $r_2 = n$, τότε μετά από μια σειρά διαδοχικών διαιρέσεων:

$$r_0 = q_1 \cdot r_1 + r_2 \quad 0 \leq r_2 < r_1$$

$$r_1 = q_2 \cdot r_2 + r_3 \quad 0 \leq r_3 < r_2$$

$$r_2 = q_3 \cdot r_3 + r_4 \quad 0 \leq r_4 < r_3$$

...

...

...

$$r_{m-2} = q_{m-1} \cdot r_{m-1} + r_m \quad 0 \leq r_m < r_{m-1}$$

$$r_{m-1} = q_m \cdot r_m$$

έχουμε ότι ο μέγιστος κοινός διαιρέτης των b , n είναι το τελευταίο μη μηδενικό υπόλοιπο r_m . Στην περίπτωση που αυτό είναι ίσο με 1, τότε και μόνο τότε ο φυσικός b θα έχει πολλαπλασιαστικό αντίστροφο $(\text{mod } n)$ ο οποίος θα είναι και μοναδικός.

Η επόμενη διαδικασία που υπολογίζει αυτόν τον πολλαπλασιαστικό αντίστροφο αποτελεί τον γενικευμένο αλγόριθμο του Ευκλείδη:

Ορίζουμε μια ακολουθία αριθμών $\{t_v\}$, βασιζόμενοι στα πηλίκα των διαιρέσεων που προηγήθηκαν:

$$t_0 = 0$$

$$t_1 = 1$$

$$t_2 = t_0 - q_1 \cdot t_1$$

$$t_j = t_{j-2} - q_{j-1} \cdot t_{j-1} \quad (j = 3, \dots, m)$$

για τους αριθμούς αυτούς πάντα ισχύει:

$$t_j r_1 \equiv r_j \pmod{n}$$



και προχωρώντας επαγωγικά μπορούμε να επαληθεύσουμε τον ισχυρισμό για όλους τους όρους της ακολουθίας $\{t_n\}$, συνεπώς και για τον τελευταίο θα έχουμε:

$$t_m b \equiv 1 \pmod{n}$$

Έτσι ο t_m ο τελευταίος δηλαδή όρος της ακολουθίας που κατασκευάσαμε, είναι ακριβώς ο ζητούμενος πολλαπλασιαστικός αντίστροφος του $b \pmod{n}$.

Κινέζικο Θεώρημα Υπολοίπων.

Έστω m_1, m_2, \dots, m_k φυσικοί αριθμοί πρώτοι μεταξύ τους ανά δύο δηλαδή $(m_i, m_j) = 1$, για κάθε $i \neq j$ τότε το σύστημα ισοτιμιών

$$x \equiv b_1 \pmod{m_1}$$

$$x \equiv b_2 \pmod{m_2}$$

...

$$x \equiv b_k \pmod{m_k}$$

δέχεται μοναδική λύση $\pmod{m_1 \cdot m_2 \cdots m_n}$ δηλαδή ως προς την ισοτιμία με μέτρο $M = m_1 \cdot m_2 \cdots m_n$.

Ο ακέραιος αριθμός x όπως φαίνεται και από την απόδειξη του θεωρήματος (Αριθμοθεωρία Γαλάνης Σελίδα 154, Θεώρημα 4.2.1) δίνεται από την σχέση:

$$x = b_1 \cdot M_1 \cdot M_1^{-1} + b_2 \cdot M_2 \cdot M_2^{-1} + \dots + b_k \cdot M_k \cdot M_k^{-1}$$

όπου $M_i = M/m_i$ για $i = 1, 2, \dots, k$.

Για την άσκησή μας τώρα ψάχνουμε να βρούμε όλους τους ακεραίους οι οποίοι αφήνουν υπόλοιπο 1 όταν διαιρεθούν με το 9, αφήνουν υπόλοιπο 2 όταν διαιρεθούν με το 8 και αφήνουν υπόλοιπο 3 όταν διαιρεθούν με το 7. Δηλαδή ουσιαστικά έχουμε να λύσουμε το παρακάτω σύστημα:

$$x \equiv 1 \pmod{9}$$

$$x \equiv 2 \pmod{8}$$

$$x \equiv 3 \pmod{7}$$



Εφόσον τα μέτρα των ισοτιμιών $m_1 = 9$, $m_2 = 8$ και $m_3 = 7$, είναι ανά δύο μεταξύ τους πρώτοι αριθμοί, από το Κινέζικο θεώρημα υπολοίπων προκύπτει ότι το παραπάνω σύστημα ισοτιμιών δέχεται μοναδική λύση ως προς την ισοτιμία με μέτρο $M = m_1 \cdot m_2 \cdot m_3 = 9 \cdot 8 \cdot 7 = 504$. Έχουμε

$$b_1 = 1$$

$$b_2 = 2$$

$$b_3 = 3$$

$$M_1 = \frac{504}{9} = 56$$

$$M_2 = \frac{504}{8} = 63$$

$$M_3 = \frac{504}{7} = 72$$

Για να υπολογίσουμε τους πολλαπλασιαστικούς αντίστροφους M_i^{-1} των $M_i \pmod{m_i}$ θα κάνουμε χρήση του γενικευμένου αλγόριθμου του Ευκλείδη.

Αρχικά υπολογίζουμε τον πολλαπλασιαστικό αντίστροφο του $56 \pmod{9}$ όμως

$$56 \equiv 2 \pmod{9}$$

που σημαίνει ότι οι ακέραιοι 56 και 2 όταν διαιρεθούν με τον ακέραιο 9, αφήνουν το ίδιο υπόλοιπο δηλαδή υπόλοιπο 2.

Εφαρμόζουμε αρχικά τον κλασικό αλγόριθμο του Ευκλείδη για τον υπολογισμό του μέγιστου κοινού διαιρέτη των 2 και 9.

Οι διαδοχικές διαιρέσεις δίνουν:

$$9 = 4 \cdot 2 + 1, \quad 2 = 2 \cdot 1$$

$$q_1 = 4, q_2 = 2$$

Όπως αναμένονταν $(2, 9) = 1$ μιας και οι δύο είναι πρώτοι αριθμοί, άρα υπάρχει ο αντίστροφος του $2 \pmod{9}$. Ο προσδιορισμός του γίνεται μέσω της ακολουθίας $\{t_v\}$, η οποία ορίζεται βάσει των πηλίκων που προέκυψαν στις προηγούμενες διαιρέσεις ως εξής:



$$t_0 = 0$$

$$t_1 = 1$$

$$t_2 = t_0 - q_1 \cdot t_1 = -4 = 5 \pmod{9}.$$

Συνεχίζουμε με τον πολλαπλασιαστικό αντίστροφο του $63 \pmod{8}$ όμως

$$63 \equiv 7 \pmod{8}$$

που σημαίνει ότι ο ακέραιος 63 είναι ισότιμος ή ισοδύναμος με τον 7 modulo 8, δηλαδή οι ακέραιοι 63 και 7 αφήνουν το ίδιο υπόλοιπο όταν διαιρεθούν διά 8.

Εφαρμόζουμε αρχικά τον κλασικό αλγόριθμο του Ευκλείδη για τον υπολογισμό του μέγιστου κοινού διαιρέτη των 7 και 8.

Οι διαδοχικές διαιρέσεις δίνουν:

$$8 = 1 \cdot 7 + 1, \quad 7 = 7 \cdot 1$$

$$q_1 = 1, q_2 = 7$$

Όπως αναμένονταν $(7, 8) = 1$ μιας και οι δύο είναι μεταξύ τους πρώτοι αριθμοί, άρα υπάρχει ο αντίστροφος του $7 \pmod{8}$. Ο προσδιορισμός του γίνεται μέσω της ακολουθίας $\{t_v\}$, η οποία ορίζεται βάσει των πηλίκων που προέκυψαν στις προηγούμενες διαιρέσεις ως εξής:

$$t_0 = 0$$

$$t_1 = 1$$

$$t_2 = t_0 - q_1 \cdot t_1 = -1 = 7 \pmod{8}.$$

Και τέλος έχουμε τον πολλαπλασιαστικό αντίστροφο του $72 \pmod{7}$ όμως

$$72 \equiv 2 \pmod{7}$$

μιας και οι ακέραιοι 72 και 2 αφήνουν το ίδιο υπόλοιπο όταν διαιρεθούν δια 7.

Εφαρμόζουμε αρχικά τον κλασικό αλγόριθμο του Ευκλείδη για τον υπολογισμό του μέγιστου κοινού διαιρέτη των 2 και 7.

Οι διαδοχικές διαιρέσεις δίνουν:



$$7 = 3 \cdot 2 + 1, 2 = 2 \cdot 1$$

$$q_1 = 3, \quad q_2 = 2$$

Όπως αναμένονταν $(2, 7) = 1$ μιας και οι δύο είναι πρώτοι αριθμοί, άρα υπάρχει ο αντίστροφος του 2 (mod 9). Ο προσδιορισμός του γίνεται μέσω της ακολουθίας $\{t_v\}$, η οποία ορίζεται βάσει των πηλίκων που προέκυψαν στις προηγούμενες διαιρέσεις ως εξής:

$$t_0 = 0$$

$$t_1 = 1$$

$$t_2 = t_0 - q_1 \cdot t_1 = -3 = 4 \pmod{7}.$$

Άρα η ζητούμενη λύση του συστήματος ισοτιμιών είναι:

$$x = b_1 \cdot M_1 \cdot M_1^{-1} + b_2 \cdot M_2 \cdot M_2^{-1} + b_3 \cdot M_3 \cdot M_3^{-1}$$

$$x = 1 \cdot 56 \cdot 5 + 2 \cdot 63 \cdot 7 + 3 \cdot 72 \cdot 4$$

$$x = 280 + 882 + 564$$

$$x = 2026 \pmod{504}$$

$$x = 10 \pmod{504}$$

Δηλαδή με απλά λόγια όλοι οι ακέραιοι οι οποίοι όταν διαιρούνται με τον ακέραιο 504 αφήνουν υπόλοιπο τον ακέραιο 10.
Επαλήθευση για τον ακέραιο 10

$$10 = 1 \cdot 9 + 1 \quad \Rightarrow \quad 10 = 1 \pmod{9}$$

$$10 = 1 \cdot 8 + 2 \quad \Rightarrow \quad 10 = 2 \pmod{8}$$

$$10 = 1 \cdot 7 + 3 \quad \Rightarrow \quad 10 = 3 \pmod{7}$$

η για τον ακέραιο 514

$$514 = 57 \cdot 9 + 1 \quad \Rightarrow \quad 514 = 1 \pmod{9}$$

$$514 = 64 \cdot 8 + 2 \quad \Rightarrow \quad 514 = 2 \pmod{8}$$

$$514 = 73 \cdot 7 + 3 \quad \Rightarrow \quad 514 = 3 \pmod{7}$$



παρόμοια και για τους υπόλοιπους ακέραιους 1522, 1522, 2026 κ.ο.κ.

(Θέμα 3) Έστω το κουτί αντικατάστασης

Είσοδος i	S(i)	Είσοδος i	S(i)
000	101	100	111
001	100	101	000
010	011	110	100
011	010	111	010

(α) να δείξετε ότι το κουτί S δεν είναι αντιστρέψιμο (β) να δείξετε ότι δεν ισχύει η ιδιότητα $S(x_1 \oplus x_2) = S(x_1) \oplus S(x_2)$ (γ) υπολογίστε τη διάχυση των bits εισόδου για το κάθε bit ξεχωριστά (διευκρίνιση: η μέγιστη διάχυση ενός bit εισόδου είναι 3 εφόσον έχει τη δυνατότητα να επηρεάσει και τα 3 bits εξόδου).

Τα κουτιά αντικατάστασης είναι το μόνο μη γραμμικό βήμα σε έναν κρυπταλγόριθμο. Ένα κουτί αντικατάστασης αντιστοιχίζει m bits εισόδου σε n bits εξόδου. Για το κουτί αντικατάστασης του θέματος έχουμε $m=3$ και $n=3$. Επειδή αυτό το κουτί είναι σχετικά μικρό η υλοποίησή του πραγματοποιείται στις περισσότερες γλώσσες προγραμματισμού με έναν μονοδιάστατο πίνακα, όπου ο δείκτης του πίνακα είναι η είσοδος, ενώ το περιεχόμενο ορίζει την έξοδο. Ο πίνακας που μας δίνεται σε αυτό το θέμα παριστάνει ένα κουτί αντικατάστασης που αντιστοιχίζει δυαδικές λέξεις των 3 bits σε δυαδικές λέξεις των 3 bits.

α) Για να είναι το κουτί αντιστρέψιμο θα πρέπει, αφού έχουμε τον ίδιο αριθμό bits, το πεδίο τιμών της εισόδου να ταυτίζεται με αυτό της εξόδου. Αυτό όμως δεν συμβαίνει.

Για την είσοδο έχουμε τις τιμές:

000, 001, 010, 011, 100, 101, 110, και 111

ενώ για την έξοδο έχουμε τις τιμές:

000, 010 (δύο φορές), 011, 100 (δύο φορές), 101, και 111

δηλαδή λείπουν οι τιμές 001 και 110.

Στην περίπτωση δηλαδή που αντιστρέψουμε την έξοδο και την κάνουμε είσοδο, τότε δεν μπορούμε πάντα να πάρουμε στην έξοδο την αρχική είσοδο.



Για παράδειγμα αν η είσοδος του κουτιού είναι 001 τότε η έξοδος είναι 100. Αν γίνει είσοδος του κουτιού η τιμή 100 τότε έχουμε σαν έξοδο την τιμή 111 και όχι την αρχική 001.

β) Για την δεύτερη ιδιότητα διαλέγουμε

$$x_1 = 001$$

$$x_2 = 010$$

οπότε

$$S(x_1) = 100$$

$$S(x_2) = 011$$

$$S(x_1) \oplus S(x_2) = 111$$

$$x_1 \oplus x_2 = 011$$

$$S(x_1 \oplus x_2) = 010$$

Άρα έχουμε

$$S(x_1) \oplus S(x_2) \text{ διάφορο του } S(x_1 \oplus x_2).$$

γ) Για να υπολογίσουμε την διάχυση του τρίτου bit εισόδου έχουμε τέσσερις περιπτώσεις:

1η περίπτωση είσοδος 000 ή είσοδος 001. Δηλαδή αλλαγή μόνο του τρίτου bit εισόδου με τα πρώτα δύο να είναι 00. Έχουμε στην έξοδο τα αποτελέσματα 101 και 100 αντίστοιχα. Δηλαδή διάχυση $\delta=1$ αφού τα πρώτα δύο bits είναι ίδια 10 και αλλάζει μόνο το τρίτο.

2η περίπτωση είσοδος 010 ή είσοδος 011. Δηλαδή αλλαγή μόνο του τρίτου bit εισόδου με τα πρώτα δύο να είναι 01. Έχουμε στην έξοδο τα αποτελέσματα 011 και 010 αντίστοιχα. Δηλαδή διάχυση $\delta=1$ αφού τα πρώτα δύο bits είναι ίδια 01 και αλλάζει μόνο το τρίτο.

3η περίπτωση είσοδος 100 ή είσοδος 101. Δηλαδή αλλαγή μόνο του τρίτου bit εισόδου με τα πρώτα δύο να είναι 10. Έχουμε στην έξοδο τα αποτελέσματα 111 και 000 αντίστοιχα. Δηλαδή διάχυση $\delta=3$ αφού αλλάζουν όλα τα bits.

4η περίπτωση είσοδος 110 ή είσοδος 111. Δηλαδή αλλαγή μόνο του τρίτου bit εισόδου με τα πρώτα δύο να είναι 11. Έχουμε στην έξοδο τα αποτελέσματα 100 και 010 αντίστοιχα. Δηλαδή διάχυση $\delta=2$ αφού το τελευταίο bit είναι ίδιο το 0 και αλλάζουν τα πρώτα δύο.

Για να υπολογίσουμε την διάχυση του πρώτου bit εισόδου έχουμε τέσσερις περιπτώσεις:

1η περίπτωση είσοδος 000 ή είσοδος 100. Δηλαδή αλλαγή μόνο του πρώτου bit εισόδου με τα δύο τελευταία να είναι 00. Έχουμε στην έξοδο τα αποτελέσματα 101 και 111 αντίστοιχα. Δηλαδή διάχυση $\delta=1$ αφού το πρώτο και το τρίτο bit είναι ίδια 11 και αλλάζει μόνο το δεύτερο.

2η περίπτωση είσοδος 001 ή είσοδος 101. Δηλαδή αλλαγή μόνο του πρώτου bit εισόδου με τα δύο τελευταία να είναι 01. Έχουμε στην



έξοδο τα αποτελέσματα 100 και 000 αντίστοιχα. Δηλαδή διάχυση $\delta=1$ αφού τα δύο τελευταία bits είναι ίδια 00 και αλλάζει μόνο το πρώτο.

3η περίπτωση είσοδος 010 ή είσοδος 110. Δηλαδή αλλαγή μόνο του πρώτου bit εισόδου με τα δύο τελευταία να είναι 10. Έχουμε στην έξοδο τα αποτελέσματα 011 και 100 αντίστοιχα. Δηλαδή διάχυση $\delta=3$ αφού αλλάζουν όλα τα bits.

4η περίπτωση είσοδος 011 ή είσοδος 111. Δηλαδή αλλαγή μόνο του πρώτου bit εισόδου με τα δύο τελευταία να είναι 11. Έχουμε στην έξοδο τα αποτελέσματα 010 και 010 αντίστοιχα. Δηλαδή διάχυση $\delta=0$ δεν αλλάζει κανένα bit.

Για να υπολογίσουμε τέλος την διάχυση του δεύτερου bit έχουμε και πάλι τέσσερις περιπτώσεις:

1η περίπτωση είσοδος 000 ή είσοδος 010. Δηλαδή αλλαγή μόνο του δεύτερου bit εισόδου με τα δύο άλλα bits να είναι 0 και 0. Έχουμε στην έξοδο τα αποτελέσματα 101 και 011 αντίστοιχα. Δηλαδή διάχυση $\delta=2$ αφού το τρίτο bit είναι ίδιο δηλαδή 1 και αλλάζουν τα άλλα δύο.

2η περίπτωση είσοδος 001 ή είσοδος 011. Δηλαδή αλλαγή μόνο του δεύτερου bit εισόδου με τα δύο άλλα bits να είναι 0 και 1. Έχουμε στην έξοδο τα αποτελέσματα 100 και 010 αντίστοιχα. Δηλαδή διάχυση $\delta=2$ αφού το τρίτο bit είναι ίδια δηλαδή 0 και αλλάζουν τα άλλα δύο.

3η περίπτωση είσοδος 100 ή είσοδος 110. Δηλαδή αλλαγή μόνο του δεύτερου bit εισόδου με τα δύο άλλα bits να είναι 1 και 0. Έχουμε στην έξοδο τα αποτελέσματα 111 και 100 αντίστοιχα. Δηλαδή διάχυση $\delta=2$ αφού το πρώτο bit είναι ίδιο δηλαδή 1 και αλλάζουν τα άλλα δύο.

4η περίπτωση είσοδος 101 ή είσοδος 111. Δηλαδή αλλαγή μόνο του δεύτερου bit εισόδου με τα δύο άλλα bits να είναι 1 και 1. Έχουμε στην έξοδο τα αποτελέσματα 000 και 010 αντίστοιχα. Δηλαδή διάχυση $\delta=1$ αφού το πρώτο και το τρίτο bit είναι ίδια δηλαδή 0 και 0 και αλλάζει μόνο το δεύτερο.

(Θέμα 4) Κρυπτανάλυστε τις παρακάτω ακολουθίες, προσδιορίζοντας γραμμικούς καταχωρητές ανάδρασης οι οποίοι να μπορούν να παράγουν τις ακολουθίες αυτές. Στη συνέχεια χρησιμοποιήστε τους γραμμικούς καταχωρητές που προσδιορίσατε για να προβλέψετε το επόμενο bit της ακολουθίας.

1010110010, 10011101001101, 0001010111, 100000001

Για την επίλυση αυτού του θέματος θα χρησιμοποιήσουμε τον αλγόριθμο των Berlekamp και Massey όπως τον έχουμε ήδη παρουσιάσει στο πρώτο θέμα. Τα αποτελέσματα των βημάτων του αλγόριθμου καθορισμού του χαρακτηριστικού πολυωνύμου για την πρώτη ακολουθία 1010110010 συνοψίζονται στον παρακάτω πίνακα 4.

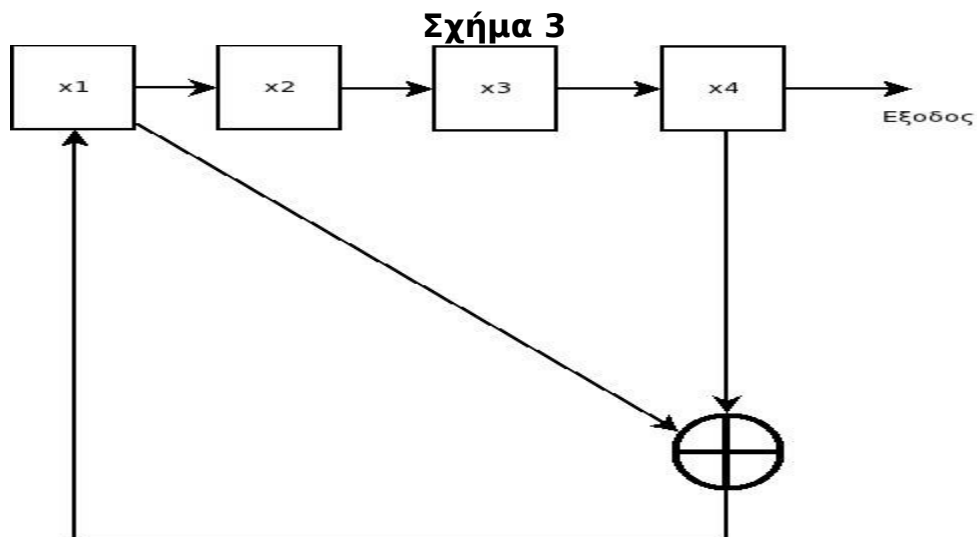


Πίνακας 4

a_N	d	$f(x)$	$f(x)$	L	m	$b(x)$	N
-	-	-	1	0	-1	1	0
1	1	1	$1+x$	1	0	1	1
0	1	$1+x$	1	1	0	1	2
1	1	1	$1+x^2$	2	2	1	3
0	0	1	$1+x^2$	2	2	1	4
1	0	1	$1+x^2$	2	2	1	5
1	1	$1+x^2$	$1+x^2+x^3$	4	5	$1+x^2$	6
0	1	$1+x^2+x^3$	$1+x+x^2$	4	5	$1+x^2$	7
0	1	$1+x+x^2$	$1+x+x^4$	4	5	$1+x^2$	8
1	0	$1+x+x^2$	$1+x+x^4$	4	5	$1+x^2$	9
0	0	$1+x+x^2$	$1+x+x^4$	4	5	$1+x^2$	10

Δηλαδή ο καταχωρητής έχει μήκος $L = 4$ και το χαρακτηριστικό πολυώνυμο είναι $f(x) = 1 + x + x^4$.

Ο καταχωρητής φαίνεται στο σχήμα 3



Το επόμενο bit της ακολουθίας 1010110010 είναι το 0 και ο υπολογισμός γίνεται στον πίνακα 5 που ακολουθεί.



Πίνακας 5

x_1	x_2	x_3	x_4
0	1	0	1
1	0	1	0
1	1	0	1
0	1	1	0
0	0	1	1
1	0	0	1
0	1	0	0
0	0	1	0
0	0	0	1
1	0	0	0
1	1	0	0

Η τελευταία στήλη του πίνακα 5 αποτελεί την έξοδο του γραμμικού καταχωρητή και το τελευταίο στοιχείο αυτής της στήλης είναι η πρόβλεψη για το επόμενο bit της ακολουθίας.

Στους επόμενους πίνακες 6 και 7 έχουμε την λύση για την ακολουθία 1011101001101.

Πίνακας 6

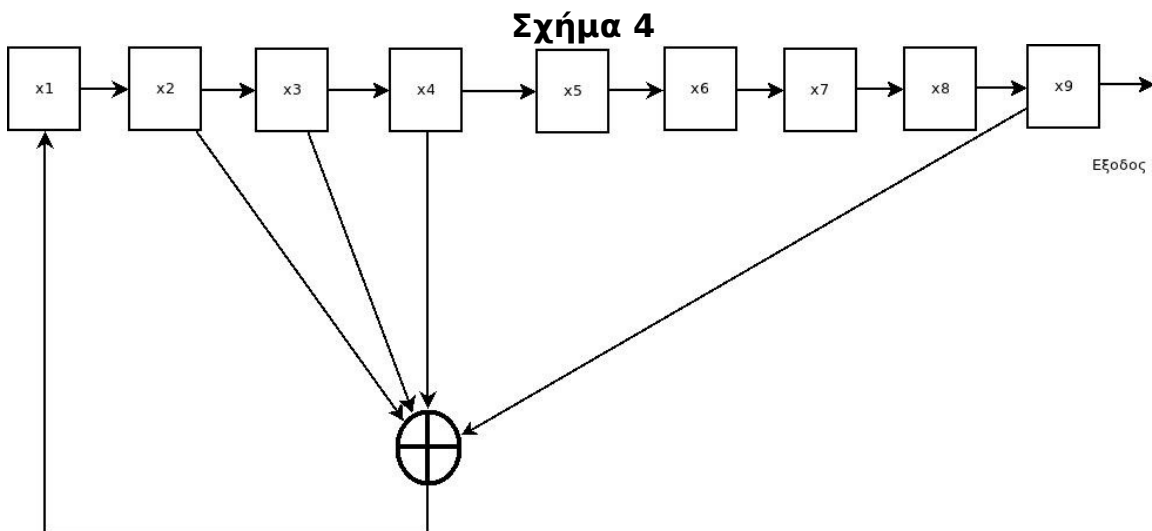
a_N	d	$f(x)$	$f(x)$	L	m	$b(x)$	N
-	-	-	1	0	-1	1	0
1	1	1	$1+x$	1	0	1	1
0	1	$1+x$	1	1	1	$1+x$	2
0	0	$1+x$	1	1	1	$1+x$	3
1	1	1	$1+x^2+x^3$	3	3	1	4
1	1	$1+x^2+x^3$	$1+x+x^2+x^3$	3	3	1	5
1	1	$1+x^2+x^3$	$1+x+x^3$	3	3	1	6
0	0	$1+x+x^2+x^3$	$1+x+x^3$	3	3	1	7
1	0	$1+x+x^2+x^3$	$1+x+x^3$	3	3	1	8
0	0	$1+x+x^2+x^3$	$1+x+x^3$	3	3	1	9
0	0	$1+x+x^2+x^3$	$1+x+x^3$	3	3	1	10
1	0	$1+x+x^2+x^3$	$1+x+x^3$	3	3	1	11



1	0	$1+x+x^2+x^3$	$1+x+x^3$	3	3	1	12
0	1	$1+x+x^3$	$1+x+x^3+x^9$	10	12	$1+x+x^3$	13
1	1	$1+x+x^3+x^9$	$1+x^2+x^3+x^4+x^9$	10	12	$1+x+x^3$	14

Δηλαδή ο καταχωρητής έχει μήκος $L = 10$ και το χαρακτηριστικό πολυώνυμο είναι $f(x) = 1 + x^2 + x^3 + x^4 + x^9$

Ο καταχωρητής φαίνεται στο σχήμα 4



Το επόμενο bit της ακολουθίας 10011101001101 είναι το 1 και ο υπολογισμός γίνεται στον πίνακα 7 που ακολουθεί.

Πίνακας 7

x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}
0	0	1	0	1	1	1	0	0	1
1	0	0	1	0	1	1	1	0	0
1	1	0	0	1	0	1	1	1	0
0	1	1	0	0	1	0	1	1	1
1	0	1	1	0	0	1	0	1	1
1	1	0	1	1	0	0	1	0	1
0	1	1	0	1	1	0	0	1	0
1	0	1	1	0	1	1	0	0	1
0	1	0	1	1	0	1	1	0	0
0	0	1	0	1	1	0	1	1	0



0	0	0	1	0	1	1	0	1	1
0	0	0	0	1	0	1	1	0	1
0	0	0	0	0	1	0	1	1	0
1	0	0	0	0	0	1	0	1	1
1	0	0	0	0	0	0	1	0	1

Η τελευταία στήλη του πίνακα 7 αποτελεί την έξοδο του γραμμικού καταχωρητή και το τελευταίο στοιχείο αυτής της στήλης είναι η πρόβλεψη για το επόμενο bit της ακολουθίας.

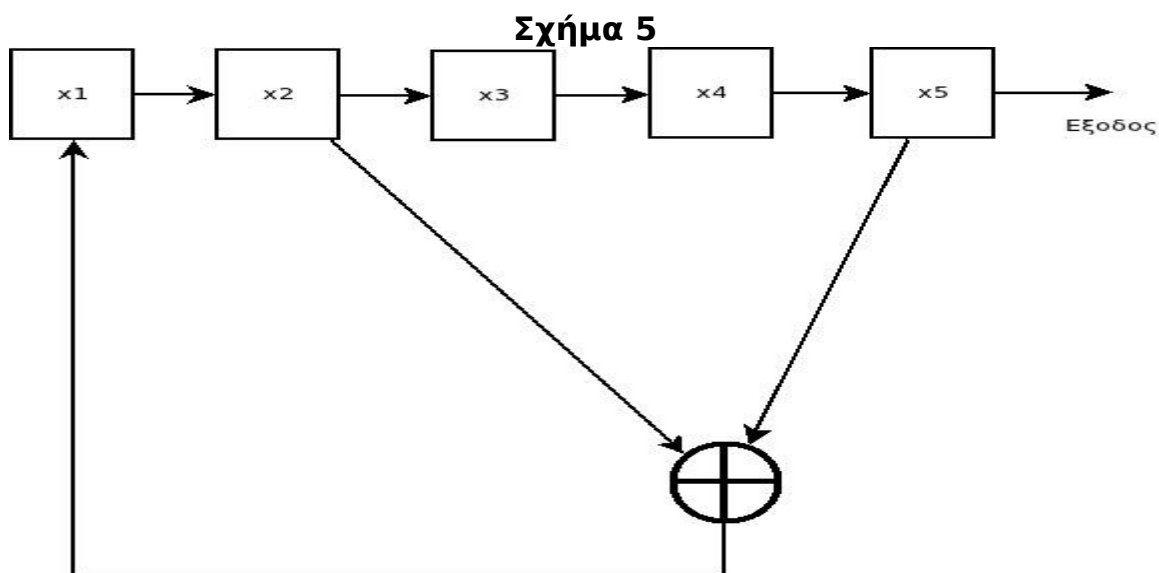
Στους επόμενους πίνακες 8 και 9 έχουμε την λύση για την ακολουθία 0001010111.

Πίνακας 8

a_N	d	$f(x)$	$f(x)$	L	m	$b(x)$	N
-	-	-	1	0	-1	1	0
0	0	-	1	0	-1	1	1
0	0	-	1	0	-1	1	2
0	0	-	1	0	-1	1	3
1	1	1	$1+x^4$	4	3	1	4
0	0	1	$1+x^4$	4	3	1	5
1	1	$1+x^4$	$1+x^2+x^4$	4	3	1	6
0	0	$1+x^4$	$1+x^2+x^4$	4	3	1	7
1	1	$1+x^2+x^4$	$1+x^2$	4	3	1	8
1	1	$1+x^2$	$1+x^2+x^5$	5	8	$1+x^2$	9
1	0	$1+x^2$	$1+x^2+x^5$	5	8	$1+x^2$	10

Δηλαδή ο καταχωρητής έχει μήκος $L = 5$ και το χαρακτηριστικό πολυώνυμο είναι $f(x) = 1 + x^2 + x^5$.

Ο καταχωρητής φαίνεται στο σχήμα 5



Το επόμενο bit της ακολουθίας 0001010111 είναι το 0 και ο υπολογισμός γίνεται στον πίνακα 9 που ακολουθεί.

Πίνακας 9

x_1	x_2	x_3	x_4	x_5
0	1	0	0	0
1	0	1	0	0
0	1	0	1	0
1	0	1	0	1
1	1	0	1	0
1	1	1	0	1
0	1	1	1	0
1	0	1	1	1
1	1	0	1	1
0	1	1	0	1
0	0	1	1	0

Η τελευταία στήλη του πίνακα 9 αποτελεί την έξοδο του γραμμικού καταχωρητή και το τελευταίο στοιχείο αυτής της στήλης είναι η πρόβλεψη για το επόμενο bit της ακολουθίας.

Στους επόμενους πίνακες 10 και 11 έχουμε την λύση για την ακολουθία 1000000001.



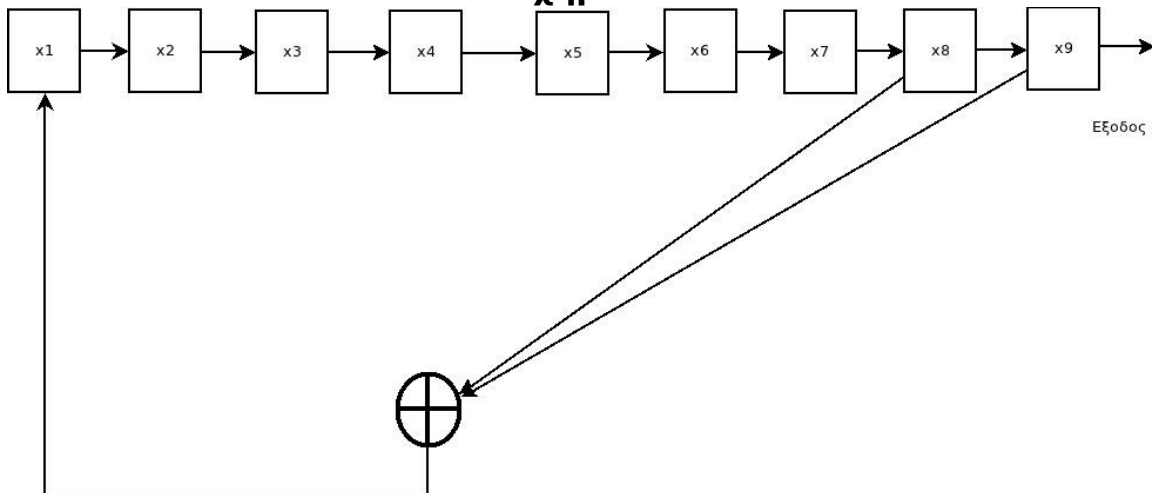
Πίνακας 10

a_N	d	$f(x)$	$f(x)$	L	m	$b(x)$	N
-	-	-	1	0	-1	1	0
1	1	1	$1+x$	1	0	1	1
0	1	$1+x$	1	1	1	$1+x$	2
0	1	$1+x$	1	1	1	$1+x$	3
0	1	$1+x$	1	1	1	$1+x$	4
0	1	$1+x$	1	1	1	$1+x$	5
0	1	$1+x$	1	1	1	$1+x$	6
0	1	$1+x$	1	1	1	$1+x$	7
0	1	$1+x$	1	1	1	$1+x$	8
0	1	$1+x$	1	1	1	$1+x$	9
1	1	1	$1+x^8+x^9$	9	9	1	10

Δηλαδή ο καταχωρητής έχει μήκος $L = 9$ και το χαρακτηριστικό πολυώνυμο είναι $f(x) = 1 + x^8 + x^9$.

Ο καταχωρητής φαίνεται στο σχήμα 6

Σχήμα 6



Το επόμενο bit της ακολουθίας 1000000001 είναι το 0 και ο υπολογισμός γίνεται στον πίνακα 11 που ακολουθεί.

Πίνακας 11

x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9
-------	-------	-------	-------	-------	-------	-------	-------	-------



0	0	0	0	0	0	0	0	1
1	0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0
0	0	0	1	0	0	0	0	0
0	0	0	0	1	0	0	0	0
0	0	0	0	0	1	0	0	0
0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	0	1	0
1	0	0	0	0	0	0	0	1
1	1	0	0	0	0	0	0	0

Η τελευταία στήλη του πίνακα 11 αποτελεί την έξοδο του γραμμικού καταχωρητή και το τελευταίο στοιχείο αυτής της στήλης είναι η πρόβλεψη για το επόμενο bit της ακολουθίας.

(Θέμα 5) Γνωρίζετε το μήνυμα (plaintext) BEAN καθώς και το κωδικοποιημένο μήνυμα (ciphertext) ΟΥΚΗ για ένα κρυπτοσύστημα Hill βαθμού 2. Να προσδιορίσετε το αντίστροφο κλειδί (πίνακα) A^{-1} ώστε να μπορέσετε να αποκωδικοποιήσετε τα κωδικοποιημένα μηνύματα που λαμβάνετε. Διευκρινίζεται ότι το αλφάβητο διαθέτει 29 χαρακτήρες (τα γράμματα του Αγγλικού αλφαβήτου καθώς και τους χαρακτήρες ., ? και το διάστημα «_»).

$\{ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z . ? _ \} = \{ 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 \}$

Ο κρυπταλγόριθμος του Hill είναι μια πολυδιάστατη (πολυαφλαβητική) γενίκευση του γραμμικού κρυπταλγόριθμου. Έχει την δυνατότητα να κρύψει τις συχνότητες εμφάνισης των συμβόλων του απλού κειμένου, όμως δεν μπορεί να αντισταθεί σε μια επίθεση γνωστού απλού κειμένου (known plaintext). Στο συγκεκριμένο θέμα γνωρίζουμε το απλό κείμενο με μήκος $m=4$ και το αντίστοιχο κρυπτοκείμενο με ίδιο μήκος $m=4$ και θα ανακαλύψουμε το κλειδί.

Παρακάτω φαίνεται ο πίνακας 12 που αντιστοιχεί τους χαρακτήρες σε αριθμούς.

**Πίνακας 12**

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z	.	,	?	_
14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

Το απλό κείμενο και το κρυπτοκείμενο εκφράζονται ως δύο πίνακες 2x2 για τους οποίους ισχύει:

$$\begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix} = K \cdot \begin{bmatrix} p_1 & p_2 \\ p_3 & p_4 \end{bmatrix} \pmod{29}$$

όλες οι πράξεις είναι (mod 29) αφού το αλφάβητο που χρησιμοποιούμε έχει 29 χαρακτήρες.

Αναγκαία συνθήκη για να ανακαλυφθεί το κλειδί είναι ένας από τους δύο αυτούς πίνακες να έχει αντίστροφο. Επειδή μας ζητείται να προσδιορίσουμε το αντίστροφο κλειδί (πίνακα) K^{-1} , θα πρέπει να ελέγξουμε αρχικά αν ο πίνακας του κρυπτοκειμένου έχει αντίστροφο. Η τιμές όπως προκύπτουν από τον προηγούμενο πίνακα αντιστοίχισης είναι:

$$\begin{array}{llll} c_1 = 14, & c_2 = 24, & c_3 = 10, & c_4 = 7 \\ p_1 = 1, & p_2 = 4, & p_3 = 0, & p_4 = 13 \end{array}$$

Ο πίνακας του κρυπτοκειμένου έχει αντίστροφο αφού η ορίζουσα αυτού του πίνακα

$$\det C = 14 \cdot 24 - 24 \cdot 10 = 96$$

είναι διάφορη του μηδενός.

Ο προσδιορισμός του αντίστροφου κλειδιού ακολουθεί την παρακάτω διαδικασία.

Αρχική προϋπόθεση είναι το μήκος του αλφαβήτου να είναι πρώτος αριθμός που ισχύει αφού ο 29 είναι πρώτος αριθμός.

Έστω

$$\vec{p}_1, \vec{p}_2, \dots, \vec{p}_m$$

διανύσματα του απλού κειμένου (m το πλήθος) του αγνώστου κρυπτοσυστήματος Hill διάστασης m με άγνωστο κλειδί K.



Αντίστοιχα

$$\vec{c}_1, \vec{c}_2, \dots, \vec{c}_m$$

τα διανύσματα του κρυπτογραφημένου κειμένου. Διαμορφώνουμε τους πίνακες P και C

$$P = \begin{bmatrix} \vec{p}_1 & \vec{p}_2 & \dots & \vec{p}_m \end{bmatrix}$$
$$C = \begin{bmatrix} \vec{c}_1 & \vec{c}_2 & \dots & \vec{c}_m \end{bmatrix}$$
$$\begin{bmatrix} C^T & P^T \end{bmatrix}$$

Επεξεργαζόμαστε τον τελευταίο πίνακα ώστε να έρθει σε μορφή reduced-row echelon, δηλαδή να εμφανίσει αριστερά τον μοναδιαίο διάστασης 2. Αφού συμβεί αυτό τότε το δεξί σκέλος του παραγόμενου πίνακα είναι ο ανάστροφος (transpose) του αντίστροφου κλειδιού K^{-1} . Δηλαδή:

$$\begin{bmatrix} C^T | P^T \end{bmatrix} = \begin{bmatrix} 14 & 24 & 1 & 4 \\ 10 & 7 & 0 & 13 \end{bmatrix} \quad \text{σχέση 1}$$

σε αυτό το σημείο θα χρειαστεί να υπολογίσουμε τον αντίστροφο mod29 του 14 δηλαδή τον $14^{-1} \text{ mod } 29$. Θα χρησιμοποιήσουμε τον γενικευμένο αλγόριθμο του ευκλείδη.

Ο μέγιστος κοινός διαιρέτης των 14 και 29 είναι ο 1 δηλαδή είναι πρώτοι μεταξύ τους αριθμοί. $\text{ΜΚΔ}(14, 29) = 1$

Από τις διαδοχικές διαιρέσεις έχουμε

$$29 = 14 \cdot 2 + 1 \quad \text{άρα } q_1 = 2$$

$$14 = 14 \cdot 1 + 0 \quad \text{άρα } q_2 = 14$$

$$t_0 = 0$$

$$t_1 = 1$$

$$t_2 = t_0 - q_1 \cdot t_1 = -2 = 27 \pmod{29}$$

Δηλαδή ο αντίστροφος του 14 (mod29) είναι ο 27. Επαλήθευση:

$$24 \cdot 27 = 378 \equiv 1 \pmod{29}$$



οπότε πολλαπλασιάζουμε την πρώτη γραμμή του πίνακα της σχέσης 1 επί 27 με σκοπό να κάνουμε το πρώτο στοιχείο μονάδα (mod29)

$$[C^T | P^T] = \begin{bmatrix} 378 & 648 & 27 & 108 \\ 10 & 7 & 0 & 13 \end{bmatrix}$$

$$[C^T | P^T] = \begin{bmatrix} 1 & 10 & 27 & 21 \\ 10 & 7 & 0 & 13 \end{bmatrix}$$

Πολλαπλασιάζουμε την πρώτη γραμμή με -10 και προσθετούμε στη δεύτερη (ώστε να εμφανιστεί το 0 στη θέση <2,1>):

$$[C^T | P^T] = \begin{bmatrix} 1 & 10 & 27 & 21 \\ 0 & -93 & -270 & -197 \end{bmatrix}$$

$$[C^T | P^T] = \begin{bmatrix} 1 & 10 & 27 & 21 \\ 0 & -6 & -9 & -23 \end{bmatrix}$$

$$[C^T | P^T] = \begin{bmatrix} 1 & 10 & 27 & 21 \\ 0 & 23 & 20 & 6 \end{bmatrix}$$

σε αυτό το σημείο θα χρειαστεί να υπολογίσουμε τον αντίστροφο mod29 του 23 δηλαδή τον $23^{-1} \text{ mod } 29$. Θα χρησιμοποιήσουμε πάλι τον γενικευμένο αλγόριθμο του Ευκλείδη.

Ο μέγιστος κοινός διαιρέτης των 23 και 29 είναι ο 1 δηλαδή είναι πρώτοι μεταξύ τους αριθμοί. $\text{ΜΚΔ}(23, 29)=1$

Από τις διαδοχικές διαιρέσεις έχουμε

$$29 = 23 \cdot 1 + 6 \quad \text{άρα } q_1 = 1$$

$$23 = 9 \cdot 3 + 5 \quad \text{άρα } q_2 = 3$$

$$6 = 5 \cdot 1 + 1 \quad \text{άρα } q_3 = 1$$

$$5 = 1 \cdot 5 + 0 \quad \text{άρα } q_4 = 5$$

$$t_0 = 0$$

$$t_1 = 1$$

$$t_2 = t_0 - q_1 \cdot t_1 = -1$$

$$t_3 = t_1 - q_2 \cdot t_2 = 4$$



$$t_4 = t_2 - q_3 \cdot t_3 = -5 = 24 \pmod{29}$$

Δηλαδή ο αντίστροφος του 23 (mod29) είναι ο 24. Επαλήθευση:

$$23 \cdot 24 = 552 \equiv 1 \pmod{29}$$

Πολλαπλασιάζουμε τη δεύτερη γραμμή με το 24 (αντίστροφος mod 29 του 23) ώστε να μας δώσει ίσο - υπόλοιπο πίνακα με 1 στη θέση <2,2>.

$$[C^T | P^T] = \begin{bmatrix} 1 & 10 & 27 & 21 \\ 0 & 552 & 480 & 144 \end{bmatrix}$$

$$[C^T | P^T] = \begin{bmatrix} 1 & 10 & 27 & 21 \\ 0 & 1 & 16 & 28 \end{bmatrix}$$

Πολλαπλασιάζουμε τη δεύτερη γραμμή με -10 και προσθέτουμε στην πρώτη.

$$[C^T | P^T] = \begin{bmatrix} 1 & 0 & -133 & -259 \\ 0 & 1 & 16 & 28 \end{bmatrix}$$

$$[C^T | P^T] = \begin{bmatrix} 1 & 0 & -17 & -27 \\ 0 & 1 & 16 & 28 \end{bmatrix}$$

$$[C^T | P^T] = \begin{bmatrix} 1 & 0 & 12 & 2 \\ 0 & 1 & 16 & 28 \end{bmatrix}$$

Ο ζητούμενος πίνακας είναι:

$$K^{-1} = \begin{bmatrix} 12 & 16 \\ 2 & 28 \end{bmatrix}$$

Μπορούμε τώρα να αποκρυπτογραφήσουμε τα κωδικοποιημένα μηνύματα που λαμβάνουμε. Για παράδειγμα εάν $c_1 = 14$ και $c_2 = 24$ έχουμε

$$\begin{bmatrix} p_1 \\ p_2 \end{bmatrix} = \begin{bmatrix} 12 & 16 \\ 2 & 28 \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$$

$$p_1 = 12 \cdot 14 + 16 \cdot 24 = 552 \equiv 1 \pmod{29}$$



$$p_2 = 2 \cdot 14 + 28 \cdot 24 = 700 \equiv 4 \pmod{29}$$

δηλαδή για τους χαρακτήρες $c_1 = O$ και $c_2 = Y$ έχουμε τους χαρακτήρες $p_1 = B$ και $p_2 = E$.

Με τον ίδιο προκύπτουν και οι χαρακτήρες A και N .

Για $c_3 = 10$ και $c_4 = 7$ έχουμε:

$$\begin{bmatrix} p_1 \\ p_2 \end{bmatrix} = \begin{bmatrix} 12 & 16 \\ 2 & 28 \end{bmatrix} \cdot \begin{bmatrix} 10 \\ 7 \end{bmatrix}$$

$$p_1 = 12 \cdot 10 + 16 \cdot 7 = 232 \equiv 0 \pmod{29}$$

$$p_2 = 2 \cdot 10 + 28 \cdot 7 = 216 \equiv 13 \pmod{29}$$

δηλαδή για τους χαρακτήρες $c_3 = K$ και $c_4 = H$ έχουμε τους χαρακτήρες $p_3 = A$ και $p_4 = N$.

(Θέμα 6) Να αποκωδικοποιήσετε το ακόλουθο μήνυμα (ciphertext) το οποίο έχει προκύψει από πολυαλφαβητική αντικατάσταση (Vigenere).

cctgvkgensvluumdi hckzamdgawmzv gxtgqjgvalij tzdwk gpkz wvgwj lwt
svpzsvfkvtwbwpu ijl kceodifvvaltwxv

Οι κρυπτογραφικές πράξεις χωρίζονται σε δύο κύριες κατηγορίες στην αναδιάταξη (transposition) και στην αντικατάσταση (substitution). Η αντικατάσταση με την σειρά της χωρίζεται σε δυο κατηγορίες με κριτήριο το πλήθος των αλφαβήτων στα οποία επιδρά μια κρυπτογραφική πράξη: στη μονοαλφαβητική αντικατάσταση και στην πολυαλφαβητική αντικατάσταση. Στην συγκεκριμένη άσκηση μελετάμε την πολυαλφαβητική αντικατάσταση του Vigenere.

Το πρώτο βήμα στην προσπάθεια ανακάλυψης του κλειδιού ενός κρυπταλγόριθμου Vigenere είναι να βρεθεί το μέγεθος του κλειδού.

Ο έλεγχος Kasiski εκμεταλλεύεται το γεγονός ότι συχνά επαναλαμβανόμενα μοτίβα του απλού κειμένου θα τύχουν κρυπτογράφησης με τμήματα του κλειδιού παραπάνω από μια φορά. Στην περίπτωση που συμβεί αυτό το επαναλαμβανόμενο μοτίβο θα είναι φανερό και στο κρυπτοκείμενο. Στον παρακάτω πίνακα 13



φαίνονται όλοι οι χαρακτήρες του κρυπτοκειμένου και οι αριθμοί που δείχνουν τις θέσεις των χαρακτήρων στο κρυπτοκείμενο.

Πίνακας 13

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
c	c	t	g	v	k	g	e	n	s	v	l	u	u	m	d	i	h
19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
c	k	z	a	m	d	g	a	w	m	z	v	g	x	t	g	q	j
37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54
g	v	a	l	i	j	t	z	d	w	k	g	p	k	z	w	v	g
55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72
w	j	l	w	t	s	v	p	z	s	v	f	k	v	t	w	b	w
73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
p	u	i	j	l	k	c	e	o	d	i	f	v	v	a	l	t	w
91	92																
x	v																

Όπως φαίνεται από τον πίνακα 13 το μοτίβο ναl εμφανίζεται για πρώτη φορά στην θέση 38 και για δεύτερη φορά στην θέση 86. Η απόσταση μεταξύ αυτών των δύο θέσεων είναι $86 - 38 = 48$.

Οι διαιρέτες του 48 είναι οι ακέραιοι 2, 3, 4, 6, 8, 12, και 24.

Επίσης παρατηρούμε ότι δεν εμφανίζεται κάποιο άλλο μοτίβο περισσότερων γραμμάτων. Θα πρέπει το μήκος του κλειδιού να είναι ένας από τους προηγούμενους ακέραιους. Κάνουμε την υπόθεση ότι το μήκος του κλειδιού δεν μπορεί να είναι 2, 3 ή και 4. Αυτή την υπόθεση την στηρίζουμε στο γεγονός ότι δεν υπάρχουν αρκετά μοτίβα γραμμάτων που να εμφανίζονται. Ένα μικρού μήκους κλειδί θα είχε σαν αποτέλεσμα περισσότερα μοτίβα να εμφανίζονται περισσότερες φορές όπως επίσης να εμφανίζονται μοτίβα μεγαλύτερου μεγέθους.

Ο έλεγχος Kasiski άρα μας δίνει ένα σύνολο από υποψήφια μήκη για το κλειδί. Εδώ τα υποψήφια μήκη είναι 6, 8, 12 και 24. Στη συνέχεια ο έλεγχος kasiski δεν μπορεί να απομονώσει το σωστό κλειδί. Έχοντας βρει υποψήφια μήκη για το κλειδί θα πρέπει να αποκλείσουμε το λάθος και να καταλήξουμε στο σωστό. Ο υπολογισμός του δείκτη σύμπτωσης είναι ένα δυνατό εργαλείο που αποκαλύπτει αν ένα κρυπτοκείμενο περιλαμβάνει ένα ή παραπάνω αλφάβητα.

Θα χρησιμοποιήσουμε τον πίνακα 14 για να υπολογίσουμε τα τετράγωνα των πιθανοτήτων εμφάνισης των γραμμάτων του γαλλικού αλφαβήτου σε ένα κανονικό γαλλικό κείμενο. Το τετράγωνο της πιθανότητας σημαίνει την πιθανότητα να επιλέξουμε δύο οποιαδήποτε



γράμματα απο ένα απλό κείμενο και αυτά να είναι ίδια. Ο πίνακας προέρχεται από το παρακάτω link

http://en.wikipedia.org/wiki/Letter_frequency

Σε κάποιους χαρακτήρες προσθέσαμε την συχνότητα των χαρακτήρων που περιλαμβάνουν τόνους μιας και γνωρίζαμε (διευκρίνιση) ότι το απλό κείμενο είναι γαλλικό χωρίς τόννους.

Πίνακας 14

Γράμμα γαλλικής αλφαβήτου	πιθανότητα	Κανονικοποιημένα δεδομένα	Τετράγωνο πιθανότητας
a	0.08122	8	0.006597
b	0.00901	1	0.000081
c	0.03345	3	0.001119
d	0.03669	4	0.001346
e	0.17125	17	0.029327
f	0.01066	1	0.000114
g	0.00866	1	0.000075
h	0.00737	1	0.000054
i	0.07579	8	0.005744
j	0.00545	1	0.000030
k	0.00049	0	0.000000
l	0.05456	5	0.002977
m	0.02968	3	0.000881
n	0.07095	7	0.005034
o	0.05378	5	0.002892
p	0.03021	3	0.000913
q	0.01362	1	0.000186
r	0.06553	7	0.004294
s	0.07948	8	0.006317
t	0.07244	7	0.005248
u	0.06369	6	0.004056
v	0.01628	2	0.000265
w	0.00114	0	0.000001



x	0.00387	0	0.000015
y	0.00308	0	0.000009
z	0.00136	0	0.000002
Αθροίσματα	0.99971		0.077577

Υποθέτουμε ότι το πιθανό μήκος του κλειδιού είναι ίσο με 6. Αυτό σημαίνει ότι το κρυπτοκείμενο δημιουργήθηκε από 6 αλφάβητα, που μπορούν να ξεχωρίσουν σε ομάδες κρυπτοκειμένων:

ομάδα 1: $\{c_1, c_7, c_{13}, \dots\}$
ομάδα 2: $\{c_2, c_8, c_{14}, \dots\}$
ομάδα 3: $\{c_3, c_9, c_{15}, \dots\}$
ομάδα 4: $\{c_4, c_{10}, c_{16}, \dots\}$
ομάδα 5: $\{c_5, c_{11}, c_{17}, \dots\}$
ομάδα 6: $\{c_6, c_{12}, c_{18}, \dots\}$

Εάν το μήκος του κλειδιού είναι σωστό τότε η κάθε ομάδα περιέχει μόνο στοιχεία από ένα αλφάβητο. Στην περίπτωση όμως που το κλειδί είναι διαφορετικό του 6, κάθε ομάδα θα περιέχει στοιχεία από δύο και πάνω αλφάβητα. Στη χειρότερη περίπτωση θα περιέχει στοιχεία από όλα τα αλφάβητα. Ο δείκτης σύμπτωσης εφαρμόζεται σε οποιαδήποτε μια από τις παραπάνω ομάδες και είναι ένας τρόπος μέτρησης της απόκλισης της κατανομής των συχνοτήτων των γραμμάτων μεταξύ του κρυπτοκειμένου και της αντίστοιχης φυσικής γλώσσας (εδώ γαλλικά) που απαρτίζει το απλό κείμενο. Εάν η ομάδα περιέχει μόνο ένα αλφάβητο η κατανομή των συχνοτήτων θα είναι “κοντά” σε αυτήν του απλού κειμένου, δηλαδή στην δική μας περίπτωση κοντά στην τιμή 0.077577. Εάν όμως υπάρχουν παραπάνω από ένα αλφάβητα στο κρυπτοκείμενο και άρα το μήκος του κλειδιού δεν είναι το σωστό, οι κατανομές μεταξύ του απλού κειμένου και του κρυπτοκειμένου θα “απέχουν” με την κατανομή του κρυπτοκειμένου να παρουσιάζει μικρότερες διακυμάνσεις από μια “επίπεδη” κατανομή.

Έστω F_i ο αριθμός των εμφανίσεων του γράμματος i στο κρυπτοκείμενο. Η πιθανότητα να επιλέξουμε δύο φορές το γράμμα i θα είναι το πλήθος των δυνατών δυάδων (i, i) προς το συνολικό πλήθος των δυάδων. Το συνολικό πλήθος των δυνατών δυάδων (i, i) θα είναι $F_i(F_i - 1)/2$, ενώ εάν το κρυπτοκείμενο έχει μέγεθος n το συνολικό πλήθος των δυάδων θα είναι αντίστοιχα $n(n - 1)/2$. Έτσι η ποσότητα αντιπροσωπεύει την πιθανότητα να επιλέξουμε δύο φορές το ίδιο γράμμα i . Για την συνέχεια υπολογίζουμε τον δείκτη σύμπτωσης για την 3η ομάδα του κρυπτοκειμένου με την βοήθεια του πίνακα 15. Ο δείκτης σύμπτωσης IC (Index Coincidence) δίνεται από την σχέση:



$$IC = \sum_{i=a}^z \left(\frac{F_i(F_i - 1)}{n(n-1)} \right)$$

Πίνακας 15

	F_i	$F_i - 1$	$F_i(F_i - 1)$	$F_i(F_i - 1)/n(n-1)$
a	2	1	2	0.0095
b	0	-1	0	0
c	0	-1	0	0
d	1	0	0	0
e	0	-1	0	0
f	0	-1	0	0
g	0	-1	0	0
h	0	-1	0	0
i	1	0	0	0
j	0	-1	0	0
k	0	-1	0	0
l	1	0	0	0
m	1	0	0	0
n	0	-1	0	0
o	0	-1	0	0
p	0	-1	0	0
q	0	-1	0	0
r	0	-1	0	0
s	0	-1	0	0
t	3	2	6	0.0286
u	1	0	0	0
v	0	-1	0	0
w	1	0	0	0
x	0	-1	0	0
y	0	-1	0	0
z	3	2	6	0.0286
	15	14	15x14	0.0667



	n	n-1	n(n-1)	IC
--	---	-----	--------	----

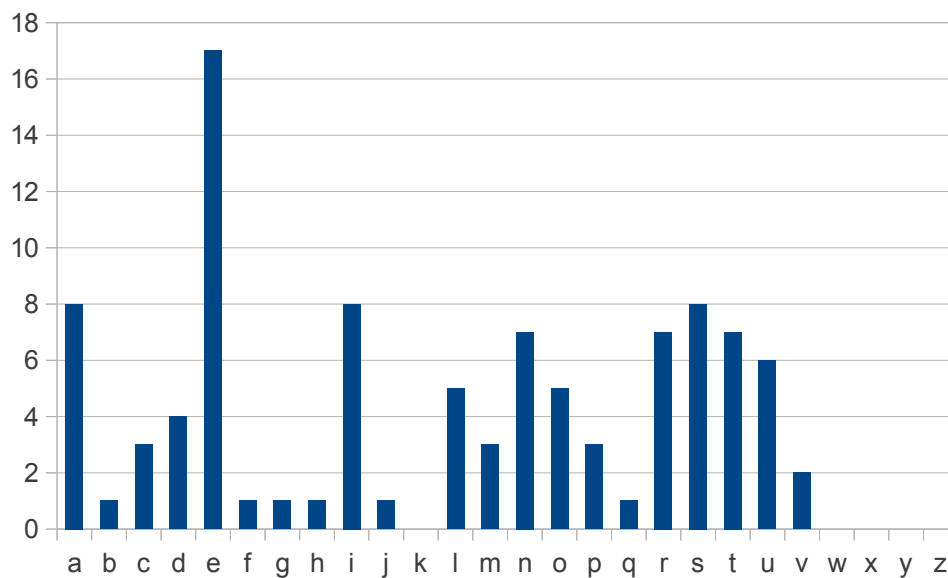
Χωρίζοντας το κρυπτοκείμενο σε ομάδες των 8 χαρακτήρων υπολογίζουμε τον δείκτη σύμπτωσης για την 1η από αυτές τις ομάδες, αντίστοιχα όπως πριν και βρίσκουμε $IC = 0.0454$

Εάν συνεχίσουμε την ίδια διαδικασία και χωρίσουμε το κρυπτοκείμενο σε ομάδες των 12 ή και των 24 χαρακτήρων δεν μπορούμε να έχουμε ασφαλή συμπεράσματα διότι ο αριθμός των χαρακτήρων του κρυπτοκειμένου είναι μικρός.

Έτσι οδηγούμαστε στο συμπέρασμα, λαμβάνοντας υπ' όψη και την υπόδειξη, ότι το μήκος του κλειδιού είναι 6.

Με βάση τις συχνότητες εμφάνισης των γραμμάτων της γαλλικής γλώσσας του πίνακα 14 κατασκευάζουμε το ιστόγραμμα όπως φαίνεται στο επόμενο σχήμα 3.

Σχήμα 3



Παρατηρώντας το ραβδόγραμμα και τον πίνακα 14 βγάζουμε τα παρακάτω συμπεράσματα. Το ραβδόγραμμα που αναφέρεται στους χαρακτήρες της γαλλικής γλώσσας έχει τρία ακρότατα. Δύο μέγιστα και ένα ελάχιστο. Οι χαρακτήρες a και e έχουν την μέγιστη συχνότητα εμφάνισης (17.125 και 8.122) ενώ ο χαρακτήρας k έχει την ελάχιστη συχνότητα (0.049). Η απόσταση από τον χαρακτήρα a στον χαρακτήρα e είναι τρεις χαρακτήρες, από τον χαρακτήρα e στον χαρακτήρα k είναι πέντε χαρακτήρες και από τον χαρακτήρα k στον χαρακτήρα a είναι δεκαπέντε χαρακτήρες.

Στη συνέχεια χωρίζουμε το κρυπτοκείμενο σε 6 ομάδες χαρακτήρων και καταμετρούμε την συχνότητα εμφάνισης κάθε χαρακτήρα. Οι



μετρήσεις φαίνονται στον πίνακα 15. Κάθε δεύτερη στήλη έχει τα δεδομένα κανονικοποιημένα έτσι ώστε όλες οι τιμές να είναι στην περιοχή από 0 έως 17.

Κατασκευάζουμε το ραβδόγραμμα συχνοτήτων κάθε ομάδας και συγκρίνουμε κάθε ραβδόγραμμα με το σχήμα 3. Μετακινούμε δεξιά και κυκλικά τα ακρότατα του σχήματος 3 που αντιστοιχούν στα γράμματα α, ε και κ με σκοπό να συμπέσουν με τυχόν ακρότατα του κάθε ραβδογράμματος. Το γράμμα του ραβδογράμματος της ομάδας που συμπίπτει με την ράβδο του γράμματος α του σχήματος 3 είναι ο χαρακτήρας του κλειδιού που ψάχνουμε.

Πίνακας 15

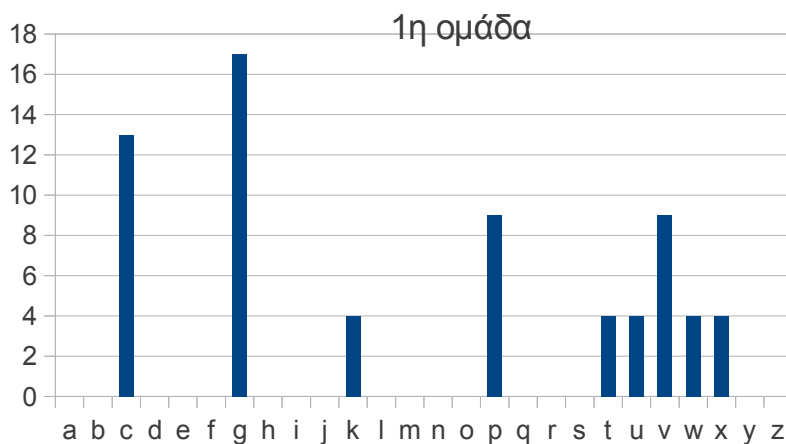
Γαλλικά		1η ομάδα		2η ομάδα		3η ομάδα		4η ομάδα		5η ομάδα		6η ομάδα	
a	8	0	0	1	4	2	11	1	4	0	0	0	0
b	1	0	0	0	0	0	0	0	0	1	4	0	0
c	3	3	13	1	4	0	0	0	0	0	0	0	0
d	4	0	0	0	0	1	6	2	9	0	0	1	9
e	17	0	0	2	9	0	0	0	0	0	0	0	0
f	1	0	0	0	0	0	0	0	0	0	0	2	17
g	1	4	17	0	0	0	0	2	9	0	0	2	17
h	1	0	0	0	0	0	0	0	0	0	0	1	9
i	8	0	0	0	0	1	6	0	0	3	13	0	0
j	1	0	0	1	4	0	0	1	4	0	0	2	17
k	0	1	4	2	9	0	0	0	0	1	4	2	17
l	5	0	0	0	0	1	6	2	9	1	4	1	9
m	3	0	0	0	0	1	6	1	4	1	4	0	0
n	7	0	0	0	0	1	6	0	0	0	0	0	0
o	5	0	0	0	0	1	6	0	0	0	0	0	0
p	3	2	9	1	4	0	0	0	0	0	0	0	0
q	1	0	0	0	0	0	0	0	0	1	4	0	0
r	7	0	0	0	0	0	0	0	0	0	0	0	0
s	8	0	0	0	0	0	0	2	9	0	0	1	9
t	7	1	4	0	0	3	17	0	0	2	9	0	0
u	6	1	4	2	9	0	0	0	0	0	0	0	0
v	2	2	9	4	17	0	0	0	0	4	17	1	9



w	0	1	4	0	0	1	6	4	17	0	0	2	17
x	0	1	4	1	4	0	0	0	0	0	0	0	0
y	0	0	0	0	0	0	0	0	0	0	0	0	0
z	0	0	0	1	4	3	17	0	0	1	4	0	0

Το ραβδόγραμμα της 1ης ομάδας φαίνεται στο επόμενο σχήμα 4.

Σχήμα 4



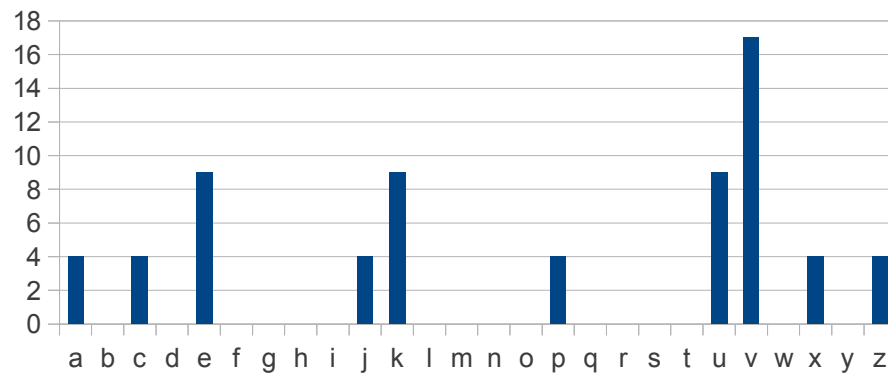
Παρατηρούμε μέγιστο στον χαρακτήρα c μετά από τρεις χαρακτήρες μέγιστο στον χαρακτήρα g μετά από πέντε χαρακτήρες ελάχιστο στον χαρακτήρα m και μετά από δεκαπέντε χαρακτήρες μέγιστο πάλι στον χαρακτήρα c. Άρα βγάζουμε το συμπέρασμα ότι ο χαρακτήρας του κλειδιού είναι ο c.

Παρόμοια έχουμε το ραβδόγραμμα της 2ης, 3ης, 4ης 5ης και 6ης ομάδας στα σχήματα 5, 6, 7, 8 και 9 που φαίνονται παρακάτω:



Σχήμα 5

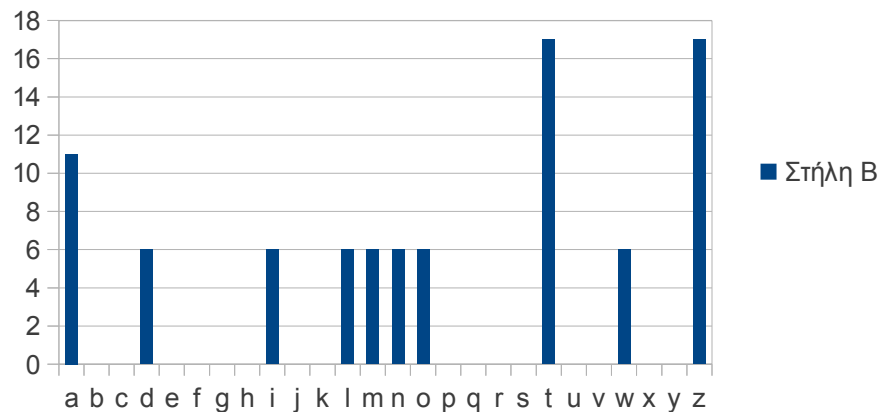
2η ομάδα



Σε αυτή την ομάδα δεν έχουμε ασφαλή συμπεράσματα σχετικά με τον χαρακτήρα του κλειδιού. Θα συμπληρώσουμε τον χαρακτήρα αφού υπολογίσουμε τους υπόλοιπους και χρησιμοποιώντας το δεδομένο ότι η λέξη κλειδί είναι κανονική αγγλική λέξη. Δηλαδή η κυκλική μετατόπιση προς τα δεξιά δεν ταύτισε τα ακρότατα του σχήματος 3 με αυτά του σχήματος 5.

Σχήμα 6

3η ομάδα

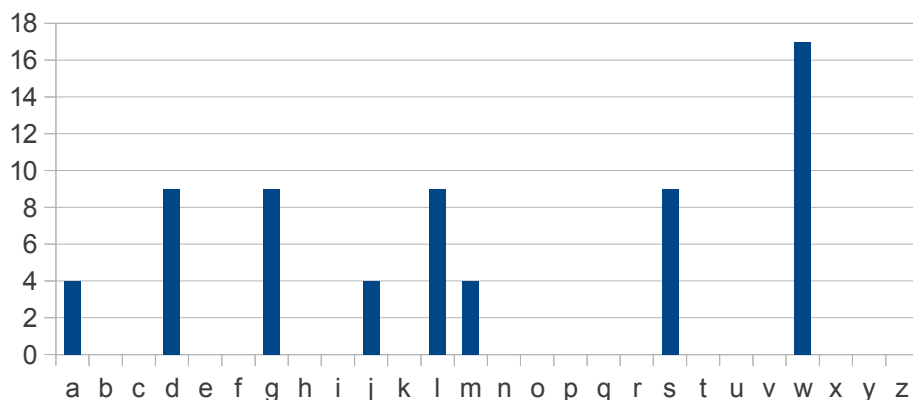


Έχουμε μέγιστο στον χαρακτήρα i μετά από τρεις χαρακτήρες έχουμε μέγιστο στον χαρακτήρα m, μετά από πέντε χαρακτήρες έχουμε ελάχιστο στον χαρακτήρα s και μετά από δεκαπέντε χαρακτήρες έχουμε πάλι μέγιστο στον χαρακτήρα i. Άρα ο χαρακτήρας του κλειδιού είναι ο i.



Σχήμα 7

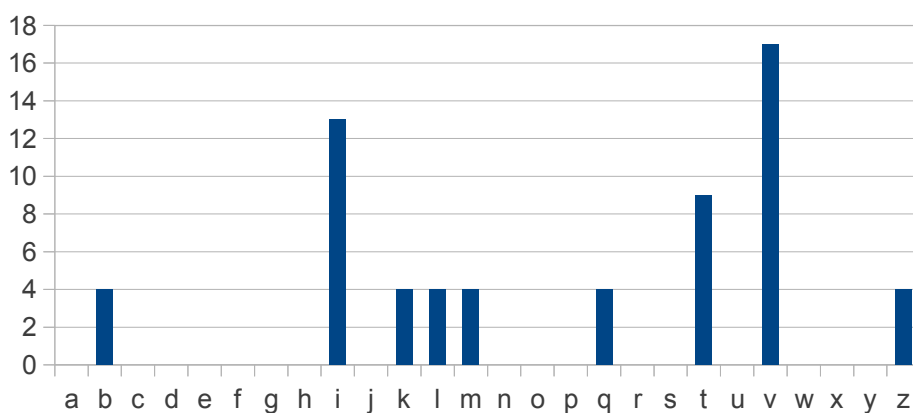
4η ομάδα



Εδώ έχουμε μέγιστο στον χαρακτήρα s, μετά από τρεις χαρακτήρες έχουμε μέγιστο στον χαρακτήρα w, μετά από πέντε χαρακτήρες έχουμε ελάχιστο στον χαρακτήρα c και μετά από δεκαπέντε χαρακτήρες έχουμε πάλι μέγιστο στον χαρακτήρα s. Άρα ο χαρακτήρας του κλειδιού είναι ο χαρακτήρας s.

Σχήμα 8

5η ομάδα

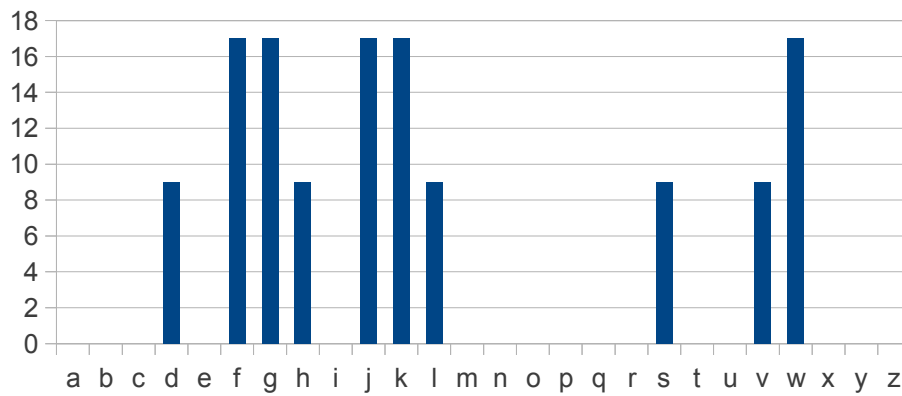


Εδώ έχουμε μέγιστο στον χαρακτήρα i μετά από τρεις χαρακτήρες έχουμε μέγιστο στον χαρακτήρα m, μετά από πέντε χαρακτήρες έχουμε ελάχιστο στον χαρακτήρα s και μετά από δεκαπέντε χαρακτήρες έχουμε πάλι μέγιστο στον χαρακτήρα i, άρα ο χαρακτήρας του κλειδιού είναι ο i.



Σχήμα 9

6η ομάδα



Εδώ έχουμε μέγιστο στον χαρακτήρα s μετά από τρεις χαρακτήρες έχουμε μέγιστο στον χαρακτήρα w, μετά από πέντε χαρακτήρες έχουμε ελάχιστο στον χαρακτήρα c και μετά από δεκαπέντε χαρακτήρες έχουμε πάλι μέγιστο στον χαρακτήρα s, άρα ο χαρακτήρας του κλειδιού είναι ο s.

Τελικά η λέξη κλειδί αποτελείται από τους χαρακτήρες:

c, _, i, s, i, s

Άρα πρόκειται για την λέξη “crisis”.

Μπορούμε τώρα να ξεκινήσουμε την αποκωδικοποίηση του κρυπτοκειμένου χρησιμοποιώντας την λέξη κλειδί “crisis”. Ο πίνακας 16 παριστάνει την οικογένεια αλφαβήτων Vigenere και ο πίνακας 17 δείχνει την αποκωδικοποίηση του κρυπτοκειμένου χαρακτήρα χαρακτήρα. Από όλα τα αλφάβητα του πίνακα 16 χρησιμοποιούμε μόνο τα αλφάβητα που αντιστοιχούν στα διαφορετικά γράμματα της λέξης του κλειδιού δηλαδή “c”, “r”, “i”, “s”.

Πίνακας 16

	plaintext																									
	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
b	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
c	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
d	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
e	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
f	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e



k e y	g	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
	h	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
	i	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
	j	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
	k	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
	l	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
	m	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
	n	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
	o	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
	p	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
	q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
	r	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
	s	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
	t	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
	u	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
	v	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
	w	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
	x	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
	y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
	z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

Η αποκρυπτογράφηση του πρώτου χαρακτήρα c γίνεται με την βοήθεια του αλφαβήτου "c" που είναι γραμμοσκιασμένο. Και όπως φαίνεται από τον πίνακα 16 είναι ο χαρακτήρας "a".

Η αποκρυπτογράφηση του δεύτερου χαρακτήρα "c" γίνεται με την βοήθεια του αλφαβήτου "r" που είναι γραμμοσκιασμένο και είναι όπως φαίνεται από τον πίνακα 16 ο χαρακτήρας "l".

Η αποκρυπτογράφηση του τρίτου χαρακτήρα "t" γίνεται με την βοήθεια του αλφαβήτου "i" που είναι γραμμοσκιασμένο και είναι όπως φαίνεται από τον πίνακα 16 ο χαρακτήρας "l".

Η αποκρυπτογράφηση του τέταρτου χαρακτήρα "g" γίνεται με την βοήθεια του αλφαβήτου "s" που είναι γραμμοσκιασμένο και είναι όπως φαίνεται από τον πίνακα 16 ο χαρακτήρας "o".

Συνεχίζουμε με τον ίδιο τρόπο και έτσι δημιουργούμε τον παρακάτω πίνακα 17.



Πίνακας 17

c	r	i	s	i	s	c	r	i	s	i	s	c	r	i	s	i	s
c	c	t	g	v	k	g	e	n	s	v	l	u	u	m	d	i	h
a	l	l	o	n	s	e	n	f	a	n	t	s	d	e	l	a	p
c	r	i	s	i	s	c	r	i	s	i	s	c	r	i	s	i	s
c	k	z	a	m	d	g	a	w	m	z	v	g	x	t	g	q	j
a	t	r	i	e	l	e	j	o	u	r	d	e	g	l	o	i	r
c	r	i	s	i	s	c	r	i	s	i	s	c	r	i	s	i	s
g	v	a	l	i	j	t	z	d	w	k	g	p	k	z	w	v	g
e	e	s	t	a	r	r	i	v	e	c	o	n	t	r	e	n	o
c	r	i	s	i	s	c	r	i	s	i	s	c	r	i	s	i	s
w	j	l	w	t	s	v	p	z	s	v	f	k	v	t	w	b	w
u	s	d	e	l	a	t	y	r	a	n	n	i	e	l	e	t	e
c	r	i	s	i	s	c	r	i	s	i	s	c	r	i	s	i	s
p	u	i	j	l	k	c	e	o	d	i	f	v	v	a	l	t	w
n	d	a	r	d	s	a	n	g	l	a	n	t	e	s	t	l	e
c	r																
x	v																
v	e																

Το τελικό κείμενο είναι:

allons enfants de la patrie
le jour de gloire est arrive
contre nous de la tyrannie
l etendard sanglant est leve

και είναι από την Μασσαλιώτιδα ο Εθνικός ύμνος της Γαλλίας και στα ελληνικά:



Σηκωθείτε παιδιά της Πατρίδας
Η μέρα της δόξας έφθασε
Ενάντια της τυραννίας μας
Το ματωμένο λάβαρο υψώθηκε

Κριτήρια αξιολόγησης:

Θέμα	Μέγιστος Βαθμός
Θ.1	18
Θ.2	14
Θ.3	17
Θ.4	18
Θ.5	18
Θ.6	15
Σύνολο	100

Ο συνολικός βαθμός θα διαιρεθεί δια 10, ώστε να προκύψει ο τελικός βαθμός της εργασίας. Ημερομηνία Παράδοσης: **15-05-2011**

Καλή Επιτυχία!