



Κρυπτογραφία

ΕΞΕΤΑΣΤΙΚΗ ΦΕΒΡΟΥΑΡΙΟΥ 2025-26

Θέμα 1ο (2.0 μονάδες)

(α) Δώστε έναν επίσημο ορισμό του κρυπταλγορίθμου $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$, ορίζοντας τις σχετικές συναρτήσεις κι εξηγώντας τον τρόπο λειτουργίας τους, για τον

- γραμμικό κρυπταλγόριθμο, και
- κρυπταλγόριθμο Vigenère.

(β) Να αποκρυπτογραφήσετε το κρυπτοκείμενο $C = \Delta\Delta\Delta\ B\Theta\Phi\ \Delta\Omega\Phi$ που έχει παραχθεί με τον γραμμικό κρυπταλγόριθμο με κλειδί $K = (5, 7) \in \mathbb{Z}_{24}^2$. (Θεωρήστε $A \leftrightarrow 0, B \leftrightarrow 1, \dots, \Omega \leftrightarrow 23$)

Θέμα 2ο (3.0 μονάδες)

(α) Τι ορίζουμε ως γραμμική πολυπλοκότητα LC_x δυαδικής ακολουθίας x ; Να τεκμηριώστε γιατί αποτελεί σημαντικό κρυπτογραφικό κριτήριο.

(β) Να περιγράψετε τον τρόπο λειτουργίας του αλγορίθμου Berlekamp-Massey και να τον εφαρμόσετε στις κλειδοροές $x = 1100101$ και $y = 0000001$.

(γ) Να απεικονίσετε σε διάγραμμα τα προφίλ γραμμικής πολυπλοκότητας LCP_x και LCP_y και να τα συγκρίνετε μεταξύ τους. Ποια ακολουθία θα θεωρούσατε πιο κρυπτογραφικά ισχυρή και γιατί;

Θέμα 3ο (3.0 μονάδες)

(α) Να περιγράψετε τη μέθοδο γραμμικής κρυπτανάλυσης όπως εφαρμόστηκε στον αλγόριθμο DES.

(β) Τι ονομάζεται γραμμικό χαρακτηριστικό, πως υπολογίζεται, και από ποιους παράγοντες εξαρτάται η πιθανότητα ισχύος;

(γ) Να βρείτε τις βέλτιστες γραμμικές προσεγγίσεις για το κουτί αντικατάστασης $y = S(x)$ που δίνεται πιο πάνω.

x	0	1	2	3	4	5	6	7
y	7	6	5	4	3	2	1	0

Θέμα 4ο (2.0 μονάδες)

(α) Να περιγράψετε τον τρόπο με τον οποίο πραγματοποιείται η κρυπτογράφηση και η ψηφιακή υπογραφή μέσω αλγορίθμων δημοσίου κλειδιού.

(β) Να δώσετε σύντομη περιγραφή δυο τουλάχιστον επιθέσεων στα ανωτέρω σχήματα.