ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ
Τμήμα Πληροφορικής και Τηλεπικοινωνιών

Νικόλαος Ε. Κολοκοτρώνης
Αναπληρωτής Καθηγητής

Κρυπτοσυστήματα ιδιωτικού κλειδιού

ΚΡΥΠΤΟΓΡΑΦΙΑ: 2η εργασία

1. Υλοποιήστε τον αλγόριθμο κρυπτογράφησης/αποκρυπτογράφησης TEA σε γλώσσα ANSI C (ο κώδικας να είναι επαρκώς σχολιασμένος). Για την υλοποίησή σας:

α) Να κατασκευάσετε αρχεία κειμένου με διανύσματα ελέγχου, δηλ. ζεύγη I/O για τον έλεγχο της ορθότητας της υλοποίησης, όπου είναι $C = \mathrm{TEA}_K(M)$:

α.1. Το 1ο αρχείο θα περιέχει ζεύγη (M, C) για όλα τα M όταν $K = 0$.

α.2. Το 2ο αρχείο θα περιέχει ζεύγη (K, C) για όλα τα K όταν $M = 0$.

β) Να συμπληρώσετε στον ακόλουθο πίνακα τα υποκλειδιά που παράγονται από το κλειδί $K = \mathrm{a1e9}$ (στο δεκαεξαδικό σύστημα) σε κάθε γύρο

β.1. k^1 = _____ **β.2.** k^2 = _____

β.3. k^3 = _____ **β.4.** k^4 = _____

γ) Να δημιουργήσετε 1GiB τυχαίων δεδομένων (2^{26} μηνύματα) και να μετρήσετε την ταχύτητα της κρυπτογράφησης κι αποκρυπτογράφησης. Συμπληρώστε τα στοιχεία και δώστε screenshots:

γ.1. Κρυπτογράφηση: _____ sec

γ.2. Αποκρυπτογράφηση: _____ sec

2. Προκειμένου να προχωρήσετε σε κρυπτανάλυση του αλγορίθμου TEA, με τη χρήση της γραμμικής και διαφορικής κρυπτανάλυσης:

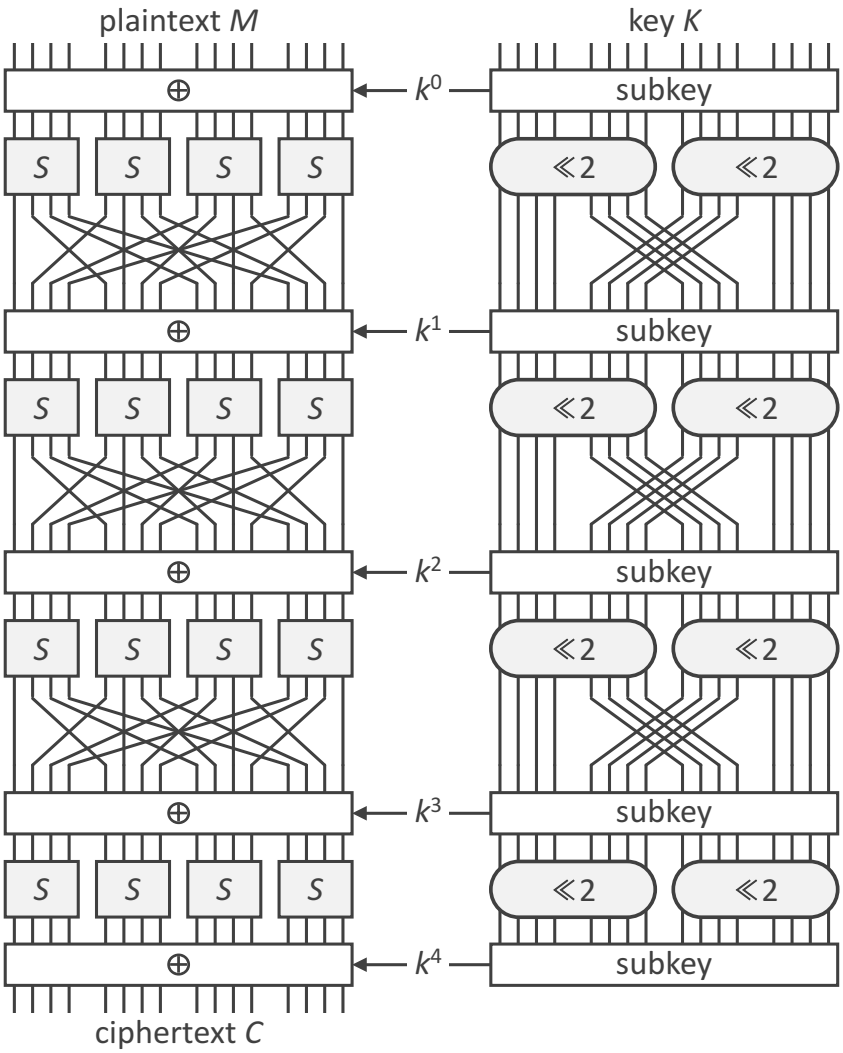
α) Βρείτε τον πίνακα γραμμικών προσεγγίσεων καθώς και τον πίνακα κατανομής διαφορών για το κουτί αντικατάστασης του αλγορίθμου.

β) Χρησιμοποιήστε την ανωτέρω πληροφορία ώστε να βρείτε τα 10 καλύτερα γραμμικά και διαφορικά χαρακτηριστικά του αλγορίθμου για 3 γύρους.

3. Υλοποιήστε μια από τις μεθόδους γραμμικής ή διαφορικής κρυπτανάλυσης και να εφαρμόσετε τα χαρακτηριστικά που βρήκατε. Θεωρήστε ότι τα κείμενα που έχετε αναχαιτίσει είναι κρυπτογραφημένα με το κλειδί $K = \mathrm{a1e9}$ (άγνωστο όμως σε εσάς). Τι ποσοστό επιτυχίας είχατε και πόσα ζεύγη (M, C) χρειαστήκατε;

Παράρτημα. Ο κρυπταλγόριθμος TEA

Ο συμμετρικός κρυπταλγόριθμος TEA (toy encryption algorithm) που απεικονίζεται στο Σχήμα 1 είναι ένας τμηματικός αλγόριθμος 4 γύρων, του οποίου η σχεδίαση βασίζεται σε *δίκτυα αντικατάστασης–αντιμετάθεσης* (SPNs).



Σχήμα 1. Ο κρυπταλγόριθμος TEA

Ο κρυπταλγόριθμος δέχεται ως είσοδο 16 bit κλειδί και επεξεργάζεται τμήματα απλού κειμένου μήκους 16 bit. Το 4x4 κουτί αντικατάστασης *S* δίνεται στον ακόλουθο πίνακα

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
***S*(*x*)**	6	4	c	5	0	7	2	e	1	f	3	d	8	a	9	b

Ο αλγόριθμος επέκτασης του κλειδιού *K* είναι απλός. Σε κάθε γύρο πραγματοποιούνται αριστερές (κυκλικές) ολισθήσεις 2 θέσεων και στη συνέχεια αντιμετάθεση (με εξαίρεση τον τελευταίο γύρο) για την παραγωγή του *i*–στου υποκλειδιού.