Άσκηση 1

Κρυπτανάλυση

Εισαγωγή

Στην άσκηση αυτή θα πρέπει να ανακτήσετε κρυπτογραφημένα μηνύματα με τη βοήθεια προγραμμάτων που θα κατασκευάσετε εσείς. Τα μηνύματα, τα οποία μπορείτε να βρείτε στο Παράρτημα, είναι κρυπτογραφημένα με απλούς ή και με σύγχρονους αλγορίθμους και θα πρέπει να δοκιμάσετε όλες τις τεχνικές που έχετε γνωρίσει στο μάθημα και το εργαστήριο.

Υλοποίηση

Για την επίλυση των μηνυμάτων μπορείτε να γράψετε προγράμματα που θα σας βοηθήσουν. Έχετε τη δυνατότητα να χρησιμοποιήσετε οποιαδήποτε γλώσσα προγραμματισμού θέλετε για αυτό τον σκοπό. Θα πρέπει να είστε σε θέση, με τη βοήθεια των προγραμμάτων που εσείς θα κατασκευάσετε, να επιλύσετε παρόμοια προβλήματα που θα σας δοθούν στο εργαστήριο κατά την εξέταση της άσκησης.

Παράδοση

Θα πρέπει όμως να παραδώσετε τα εξής.

- Τις λύσεις των προβλημάτων.
- Τον κώδικα που έχετε γράψει και όλα τα αρχεία που πιθανόν να απαιτούνται για να χτιστεί ο κώδικας εκ νέου (π.χ., Makefile).
- Ένα έγγραφο στο οποίο τεκμηριώνετε όλα τα βήματά σας για την επίλυση του κάθε προβλήματος.

Στην άσκηση βαθμολογούνται οι λύσεις, ο κώδικά σας, και το έγγραφο τεκμηρίωσης. Θα πρέπει να τα παραδώσετε όλα αυτά μέσω το Blackboard.

Προθεσμία: 28 Φεβρουαρίου, 2023

Παράρτημα

Πρόβλημα 1, 2, 3, και 4
Αποκρυπτογραφήστε τα μηνύματα που είναι αποθηκευμένα στα αρχεία puzzle1, puzzle2, puzzle3 και puzzle4.

Πρόβλημα 5
Η Αλίκη, η οποία είναι φοιτήτρια του Παν. Κύπρου, άλλα δεν έχει παρακολουθήσει το ΕΠΛ326, πιστεύει ότι ο αλγόριθμος AES είναι ασφαλής, ανεξάρτητα με τις επιλογές χρήσης του. Επομένως έχει κρυπτογραφήσει ένα μήνυμα με AES και κλειδί των 128 bit. Η Αλίκη, όμως, έχει χρησιμοποιήσει στη διαδικασία της κρυπτογράφησης τη φοιτητική της ταυτότητα. Μειώνει αυτό την αξία του αλγορίθμου; Αποκρυπτογραφήστε το μήνυμα που βρίσκεται στο αρχείο puzzle5 και εξηγήστε αν η Αλίκη έχει κάνει κάποιο λάθος.