Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων
Πολυτεχνική Σχολή, Πανεπιστήμιο Αιγαίου

Κρυπτογραφία – Προγραμματιστική Άσκηση

Διδάσκουσα: Ελισάβετ Κωνσταντίνου, Επικ. Καθηγήτρια

Η υλοποίηση θα γίνει με χρήση της βιβλιοθήκης GNUMP. Αναλυτικότερα, σας ζητείται να υλοποιήσετε τα εξής:

Ζήτημα 1 (3 μονάδες). Υλοποιήστε τον αλγόριθμο κρυπτογράφησης RSA. Αναλυτικότερα:

1. Υλοποιήστε έναν αλγόριθμο που θα μετατρέπει ένα μήνυμα σε έναν ακέραιο και το αντίστροφο. Υποθέστε ότι τα μηνύματα αποτελούνται μόνο από χαρακτήρες του αγγλικού αλφαβήτου.
2. Δημιουργήστε δύο πρώτους αριθμούς p και q μεγέθους 512 bits. Υπολογίστε στη συνέχεια το N, ένα δημόσιο κλειδί e και το αντίστοιχό του ιδιωτικό d. Με τις παραμέτρους που έχετε δημιουργήσει, κρυπτογραφήστε και αποκρυπτογραφήστε ένα μήνυμα της επιλογής σας για να ελέγξετε την ορθότητα της υλοποίησής σας.

Ζήτημα 2 (3 μονάδες). Υλοποιήστε τον αλγόριθμο κρυπτογράφησης ElGamal. Αναλυτικότερα:

1. Δημιουργήστε έναν πρώτο αριθμό p μεγέθους 200 bits και υπολογίστε έναν γεννήτορα του σώματος Z_p^* (εδώ δεν είναι απαραίτητο να υλοποιήσετε έναν αλγόριθμο παραγοντοποίησης).
2. Δημιουργήστε ένα δημόσιο κλειδί και το αντίστοιχό του ιδιωτικό κλειδί. Με τις παραμέτρους που έχετε δημιουργήσει, κρυπτογραφήστε και αποκρυπτογραφήστε ένα μήνυμα της επιλογής σας για να ελέγξετε την ορθότητα της υλοποίησής σας.

Ζήτημα 3 (3 μονάδες). Υλοποιήστε τον αλγόριθμο κρυπτογράφησης Rabin. Αναλυτικότερα:

1. Δημιουργήστε δύο πρώτους αριθμούς p και q μεγέθους 200 bits που να είναι ισότιμοι με 3 mod 4.
2. Με τις παραμέτρους που έχετε δημιουργήσει, κρυπτογραφήστε και αποκρυπτογραφήστε ένα μήνυμα της επιλογής σας για να ελέγξετε την ορθότητα της υλοποίησής σας. Χρησιμοποιήστε την παρατήρηση 8.12 του βιβλίου (θα χρειαστεί να υλοποιήσετε και τον αλγόριθμο 2.107) καθώς και έναν τρόπο για να ξεχωρίζετε το σωστό από τα τέσσερα μηνύματα που προκύπτουν από την αποκρυπτογράφηση.

Ζήτημα 4 (1 μονάδα). Υλοποιήστε μια συνάρτηση που να κρυπτογραφεί ένα αρχείο κειμένου. Μπορείτε να χρησιμοποιήσετε όποιον αλγόριθμο επιθυμείτε από τα ζητήματα 1, 2 και 3.

Παράδοση: Η εργασία θα παραδοθεί την Παρασκευή 27 Απριλίου μέσω eclass. Παραδοτέα είναι: (α) ο πηγαίος κώδικας και (β) μια σύντομη τεχνική αναφορά όπου θα εξηγούνται οι επιλογές που κάνατε στην υλοποίηση σας καθώς και οι απαντήσεις που απαιτούνται στα ζητήματα 1, 2, 3 και 4.

Καλή Επιτυχία!