Ασφάλεια Συστημάτων και Υπηρεσιών | Άσκηση 1

Το παραδοτέο .zip αρχείο περιέχει τα ακόλουθα αρχεία:

- δύο .c αρχεία, με τους κώδικες των αλγορίθμων
- ένα makefile αρχείο,
- το παρόν .pdf αρχείο.
- ένα ενδεικτικό αρχείο plaintext.txt

RSA Algorithm

Στο αρχείο rsa_assign_1.c υλοποιείται ο κώδικας για τον **αλγόριθμο RSA**. Για το compilation, αρκεί ο χρήστης να εκτελέσει make rsa στο terminal, ή make all για να κάνει compile και τα δύο αρχεία. Για την εκτέλεση, στη συνέχεια, του προγράμματος, έχει τις παρακάτω επιλογές:

- ./rsa_assign_1 -g “length”
    - Με αυτή την επιλογή εκτελείται παραγωγή κλειδιών, χρησιμοποιώντας το δοσμένο από το χρήστη length. Τα κλειδιά αποθηκεύονται σε δύο αρχεία public_length.key και private_length.key.

- ./rsa_assign_1 -i plaintext.txt -o ciphertext.txt -k public_length.key -e
    - Εδώ ο αλγόριθμος ανακτά το public κλειδί από το αρχείο, εκτελεί RSA encryption στο input που λαμβάνεται από το plaintext.txt, και αποθηκεύει την κρυπτογραφημένη πληροφορία στο ciphertext.txt.

- ./rsa_assign_1 -i ciphertext.txt -o deciphertext.txt -k private_length.key -d
    - Εδώ ο αλγόριθμος ανακτά το private κλειδί από το αρχείο, εκτελεί RSA decryption στο κρυπτογραφημένο input που λαμβάνεται από το ciphertext.txt, και αποθηκεύει την αποκρυπτογραφημένη πληροφορία στο deciphertext.txt.

- ./rsa_assign_1 -a performance.txt
    - Εδώ ο αλγόριθμος εκτελεί τις τρεις λειτουργίες που περιγράφηκαν παραπάνω, τρεις φορές, με την παράμετρο length να λαμβάνει τις τιμές 1024, 2048 και 4096. Παράλληλα, υπολογίζεται ο συνολικός χρόνος encryption και decryption για κάθε length, και τα στοιχεία αυτά αποθηκεύονται σε ένα αρχείο performance.txt.

- ./rsa_assign_1 -h
    - Εκτύπωση στο terminal ενός help message για το χρήστη.

Το υλοποιημένο πρόγραμμα προορίζεται για encryption/decryption αριθμητικών τιμών.

Diffie-Hellman Key Exchange

Στο αρχείο dh_assign_1.c υλοποιείται ο κώδικας για τον **αλγόριθμο DH**. Για το compilation, αρκεί ο χρήστης να εκτελέσει make dh στο terminal, ή make all για να κάνει compile και τα δύο αρχεία. Για την εκτέλεση, στη συνέχεια, του προγράμματος έχει τις παρακάτω επιλογές:

- ./dh_assign_1 -o output.txt -p 23 -g 7 -a 15 -b 2
    - Ο αλγόριθμος θα λάβει ως είσοδο μια τιμή p και μια τιμή g και θα ελέγξει αν η πρώτη είναι prime number και αν η δεύτερη είναι primitive root της πρώτης. Θα λάβει ακόμα τα private κλειδιά a και b των Alice και Bob αντίστοιχα, και μέσω αυτών θα υπολογίσει τα public κλειδιά που ανταλλάσσουν τα δύο «πρόσωπα». Με τη χρήση αυτών των κλειδιών, και οι δύο μπορούν να ανακτήσουν ένα κοινό μυστικό. Τα public κλειδιά και το μυστικό που μοιράζονται, αποθηκεύονται στο αρχείο output.txt.

- ./dh_assign_1 -h
    - Εκτύπωση στο terminal ενός help message για το χρήστη

Οι συναρτήσεις για τον έλεγχο των primitive roots καθώς και η συνάρτηση για τον υπολογισμό του *a^b mod c*, στον κώδικα DH, πάρθηκαν από το Διαδίκτυο.

Σημείωση: οι αριθμητικές τιμές και τα ονόματα αρχείων που δίνονται παραπάνω είναι ενδεικτικά και ο χρήστης είναι ελεύθερος να εισάγει ό,τι στοιχεία επιθυμεί.