Assignment 1

Λεοντής Παναγιώτης AM:2018030099

Εντολή για να τρέξει το πρόγραμμα: make
./encrypt

Αποτέλεσμα τρέχοντας της εντολή gcc --version : gcc (Ubuntu 9.3.0-17ubuntu1~20.04)

"**demoprogram.c**"

Περιέχεται η main. Για κάθε αλγόριθμο ζητείται από το χρήστη να πληκτρολογήσει το plaintext για encryption. Επιπλέον ορίζονται και οι κατάλληλες μεταβλητές οι οποίες δίνονται σαν όρισμα στις αντίστοιχες συναρτήσεις. Για παράδειγμα ο pointer otp_plaintext δέχεται το encrypted array που επιστρέφει η otp_encrypt() και έπειτα δίνεται ως όρισμα στην otp_decrypt() για την αποκωδικοποίηση.

"simple_crypto.h"

Δηλώνονται οι μέθοδοι που θα χρησιμοποιηθούν και τα απαραίτητα σχόλια για να γίνει κατανοητός ο σκοπός λειτουργίας τους.

" simple_crypto.c"

Υλοποιούνται οι μέθοδοι που ορίζονται στο αρχείο "simple_crypto.h".

Για τον αλγόριθμο OTP γίνεται επεξεργασία του string που δίνει ο user και κρατούνται μόνο τους χαρακτήρες 'a'-'z', 'A'-'Z' και '0'-'9'. Παράγεται το τυχαίο κλειδί, γίνεται το encryption με XOR και εκτυπώνονται κατάλληλα τα αποτελέσματα. Το key αποθηκεύεται σε global pointer για να χρησιμοποιηθεί στην αποκωδικοποίηση και το encrypted array επιστρέφεται για να δοθεί ως όρισμα στην otp_decrypt(). Στην αποκωδικοποίηση κάνοντας XOR μεταξύ encrypted array και κλειδιού παράγεται το decrypted array το οποίο και εκτυπώνεται.

Για τον αλγόριθμο Ceasar's ελέγχεται για κάθε χαρακτήρα του plaintext εάν ανήκει σε ένα από τα 'a'-'z', 'A'-'Z' και '0'-'9' και αν ναι τότε προστίθεται το key σαν offset για να γίνει το encryption. Έγινε κατάλληλος χειρισμός για την περίπτωση όπου το αποτέλεσμα βγει εκτός ορίων ώστε να παίρνει τιμές κυκλικά(πχ 'z'+'3'='c'). Τέλος εκτυπώνεται το encrypted message στη κονσόλα και επιστρέφεται για να γίνει χρήση στο ceasars_decrypt(). Εκεί γίνεται η αποκωδικοποίηση αντίστροφα από την κωδικοποίηση και εκτυπώνεται το αποτέλεσμα.

Για τον αλγόριθμο Vigenere's αρχικά γίνεται επεξεργασία του plaintext σε περίπτωση που περιέχει μικρό γράμμα 'a'-'z' και μετατρέπεται σε κεφαλαίο 'A'-'Z'. Τα γράμματα A-Z θεωρούνται ως [0, 1, …, 25] και γίνεται το encryption προσθέτοντας τον χαρακτήρα του plaintext και τον αντίστοιχο του key και έπειτα mod26. Με offset 'A' παράγεται ο αντίστοιχος encrypted χαρακτήρας. Εκτυπώνεται το encrypted array και επιστρέφεται για να μπει ως όρισμα στο vigeneres_decrypt(). Εκεί με αντίστροφη διαδικασία, παράγεται το decrypted array και εκτυπώνεται.

Εκτός από τις παραπάνω μεθόδους για encrypt και decrypt για κάθε ένα από τους 3 αλγορίθμους υλοποιήθηκαν και οι εξής μέθοδοι:

- *createOtpKey()* καλείται κατά το encrypt με αλγόριθμο OTP για να παράγει το τυχαίο κλειδί. Με βάση το μήκος αυτού του array που προορίζεται για encryption παράγεται το κλειδί χρησιμοποιώντας το /dev/urandom
- *checkIfPrintable()* επειδή μπορεί να προκύψουν χαρακτήρες ASCII που δεν μπορούν να εκτυπωθούν στην κονσόλα, δίνουμε ως όρισμα ένα array και είτε εκτυπώνεται ο χαρακτήρας είτε εκτυπώνεται σε HEX μορφή. Χρησιμοποιείται όταν γίνει το encryption και το decryption σε OTP όπου μπορεί να προκύψουν non-printable ASCII characters
- *modifyVigeneresKey()* Κατά το encryption με αλγόριθμο Vigenere's εάν το κλειδί έχει μικρότερο μήκος από το plaintext πρέπει να συμπληρωθεί ώστε να φτάσει στο ίδιο μήκος. Εκεί όπου τελειώνει το κλειδί, συμπληρώνεται ξαναγράφοντάς το.