Assignment 2

Λεοντής Παναγιώτης ΑΜ:2018030099

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

Αρχικά υλοποιήθηκαν οι συναρτήσεις για εγγραφή και ανάγνωση σε/από αρχείο. Στη writeFile() όπως και στη readFile() δίνεται ως όρισμα το path όπου βρίσκεται το αρχείο. Αφού ανοιχτεί, είτε διαβάζουμε είτε διαβάζουμε έναν χαρακτήρα την φορά και μέσω pointer περνάμε τις τιμές στο όρισμα της κάθε συνάρτησης. Στην fileRead() επιστρέφουμε και το πόσοι χαρακτήρες διαβάστηκαν για να χρησιμοποιηθεί η τιμή στην εκτέλεση του προγράμματος

TASK A

Στην keygen() δημιουργείται το αντίστοιχο cipher αναλόγως το bit_mode και τα υπόλοιπα ορίσματα που θα δοθούν στην EVP_BytesToKey() για να δημιουργηθεί το κλειδί σύμφωνα με το κωδικό που έχει δοθεί από το χρήστη. Στη main δεσμεύεται η κατάλληλη μνήμη για το κλειδί και καλείται η συνάρτηση.

TASK B

Στην encrypt() καλούνται με την σειρά οι αντίστοιχες συναρτήσεις (init_ex, update, final) για να γίνει το encryption του plaintext(). Ο cipher και πάλι δημιουργείται αναλόγως του bit_mode. Υπολογίζεται και το μέγεθος του κρυπτογραφημένου κειμένου και επιστρέφεται για να χρησιμοποιηθεί κατά την εγγραφή στο αρχείο. Στη main στο case 0 αρχικά ανοίγεται το αρχείο για να παρθεί το plaintext και έπειτα καλείται η encrypt(). Τέλος γράφεται η πληροφορία στο αρχείο που έχει δοθεί ως προορισμός.

TASK C

Στην decrypt() καλούνται με την σειρά οι αντίστοιχες συναρτήσεις (init_ex,update,final) για να γίνει το decryption του ciphertext. Ο cipher και πάλι δημιουργείται αναλόγως του bit_mode. Υπολογίζεται το μέγεθος του αποκρυπτογραφημένου κειμένου και επιστρέφεται για να χρησιμοποιηθεί κατά την εγγραφή στο αρχείο. . Στη main στο case 1 αρχικά ανοίγεται το αρχείο για να παρθεί το ciphertext και έπειτα καλείται η decrypt(). Τέλος γράφεται η πληροφορία στο αρχείο που έχει δοθεί ως προορισμός.

TASK D

Στην gen_cmac καλούνται με την σειρά οι αντίστοιχες συναρτήσεις (init,update,final) για να παραχθεί το CMAC. Ο cipher και πάλι δημιουργείται αναλόγως του bit_mode. Στη main στο case 2 αρχικά ανοίγεται το αρχείο για να παρθεί το plaintext και έπειτα καλείται η encrypt() για να γίνει κωδικοποίηση της πληροφορίας. Δεσμεύεται ο

κατάλληλος χώρος ώστε ο ciphertext να πάρει και τη πληροφορία και το CMAC που θα παραχθεί. Αφού αντιγραφούν όλοι οι χαρακτήρες γράφουμε το ciphertext στο αρχείο.

TASK F

Στη verify_cmac() ουσιαστικά γίνεται η σύγκριση των δυο CMAC που δίνονται ως ορίσματα και αν βρεθεί κάποια διαφορά επιστρέφεται αποτυχία. Στη main() στο case 3 αρχικά ανοίγουμε το αρχείο για να πάρουμε το ciphertext και δεσμεύεται η κατάλληλη μνήμη για το plaintext που θα πάρει μόνο τη πληροφορία χωρίς το cmac. Έπειτα καλείται η decrypt() για να αποκωδικοποιηθεί το αρχείο και η πληροφορία να περάσει στο plaintext. Στην συνέχεια γίνεται και η ανάκτηση του cmac και καλείται η verify_cmac() για να εντοπιστούν διαφορές.

Όλες οι εντολές που ζητήθηκαν εκτελέστηκαν κανονικά και τα αντίστοιχα αρχεία που προκύπτουν συμπεριλαμβάνονται. Στο TASK F4 κατά το verify παρατηρήθηκε ότι κανένα από τα δυο αρχεία δεν έκανε verify.

Αναφορά πηγών

https://www.openssl.org/