Barsan-Romano Alexandru

3A1

Tema 1

Descrierea mediului de lucru utilizat

Tema este facuta in limbajul Python. Sunt 4 fisiere: cbc.py, ecb.py (care contin cate o clasa cu ajutorul carora am facut criptarea si decriptarea unui text avand o cheie) si fisierele server.py si client.py, prin care se asigura comunicarea prin socket.

Descrierea modului de rezolvare a cerintei

Tema are o arhitectura server-client cu socket. Serverul detine 3 chei: o cheie pe care o are si clientul, pentru a cripta celelalte chei si 2 chei specifice modului de lucru (CBC sau ECB).

Dupa ce se stabileste o conexiune TCP, clientul trimite modul de lucru catre server. In functie de acesta, serverul cripteaza cheia specifica cu cheia generala, si o trimite clientului. Cheia criptata primita de la server este decriptata de client si trimite serverului un mesaj prin care spune ca poate incepe comunicarea criptata intre cele 2 noduri. Dupa ce serverul primeste acest mesaj, serverul trimite un mesaj criptat cu cheia specifica (pe care acum o are si clientul). Clientul o decripteaza si afiseaza mesajul in plain text. In cazul modului CBC, serverul transmite si un vector de initializare cu ajutorul caruia clientul face decriptarea.

Teste efectuate

In fisierele ecb.py si cbc.py se gaseste cate o functie test() prin care am testat diferse fisiere cu chei de lungime variata, verificand daca dupa efectuarea criptarii si decriptarii, textul ramane acelasi. Rezultatele sunt pozitive