Securitatea Informatiei

Tema 1

Nistor Marian-Sergiu, 3B6

November 7, 2020

1 Introducere

Aplicatia implica o retea, bazata pe arhitectura TCP Server-Client, in care comunicarea se realizeaza criptat.

2 Premise

Atat Serverul, cat si Clientul, pot fi executate pe orice mediu Linux, inclusiv WSL(Windows Subsystem for Linux).
Este necesar ca pe sistemul respectiv sa fie instalat libopenssl, spre a avea acces la primitivele de incriptie.

3 Compilare

Serverul si Clientul au, fiecare, un "Makefile", care poate fi executat la linia de comanda, astfel:

```
./Makefile
```

In urma executiei Makefile-ului, sunt generate executabilele, plasate in folderul "bin".

4 Resurse

Atat in cazul Serverului, cat si al Clientului, cheia si vectorul de initializare folosite pentru comunicarea initiala cu Serverul, se regasesc in folderul "resources", in fisierele "key.pem" si, respectiv, "iv.pem".

5 Mod de Utilizare

In primul rand, o instanta a Serverului trebuie sa fie pornita. Executabilul de Server se regaseste in folderul "bin". Nu este necesara pasarea vreunui argument la linia de comanda.
Serverul va astepta conexiuni. Dupa conectarea unui Client, toti ceilalti Clienti sunt notificati. Apoi, se asteapta un mesaj din partea noului Client, in cadrul caruia mentioneaza daca doreste sa foloseasca modul de operare ECB, ori CFB, pentru incriptia AES. Dupa receptionarea mesajului, se creaza o cheie noua si un vector de initializare(random, folosind primita RAND_bytes() din headerul "openssl/rand.h" a bibliotecii openssl. Acestea sunt trimise, pe rand, catre client. Din acel punct, Clientul respectiv este plasat in pool-ul de Clienti conectati.
Cand un Client trimite un mesaj, acesta este decriptat de catre server si recriptat, conform cheilor si vectorilor de initializare asociate fiecarui altui Client, ca apoi criptotextele sa fie trimise catre ceilalti Clienti.
In momentul in care un Client se deconecteaza, Serverul detecteaza acest eveniment si notifica toti ceilalti Clienti.

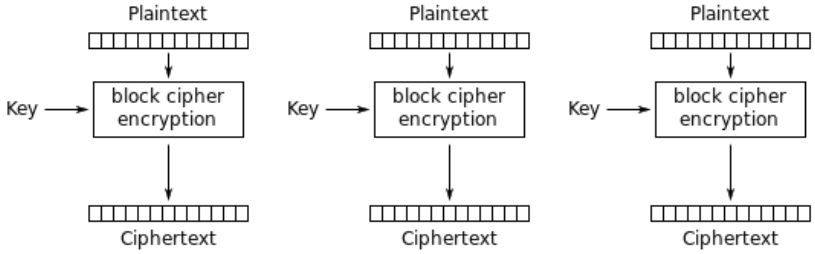
6 Modalitati de Incriptie

Dupa realizarea conexiunii Serverului cu un Client, mesajul in care Clientul specifica modalitatea de incriptie dorita este criptat folosind modul de operare CFB, avand la dispozitie cheia si vectorul de initializare din fisierele "key.pem" si "iv.pem". Raspunsul Serverului(continand o noua cheie si un nou vector de initializare, care urmeaza sa fie folosite in comunicarea cu Clientul) va fi, de asemenea, incriptionat folosind cheia si vectorul de initializare initial.
Fiecarui Client ii este asociata o cheie si un vector de initializare, care sunt generate random la momentul conectarii sale. Pana la terminarea conexiunii, Serverul va comunica cu acel Client folosind respectiva cheie si respectivul vector de initializare.

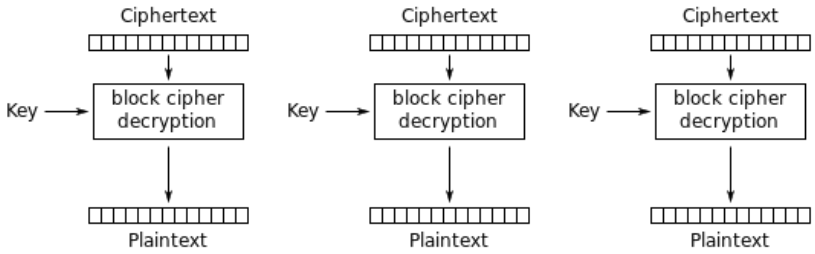
7 Implementari Moduri de Operare

Pentru a implementa modurile de operare ECB si CFB, s-au folosit primitivele "aes_encrypt" si "aes_decrypt" din headerul "openssl/aes.h" a bibliotecii openssl.

7.1 ECB

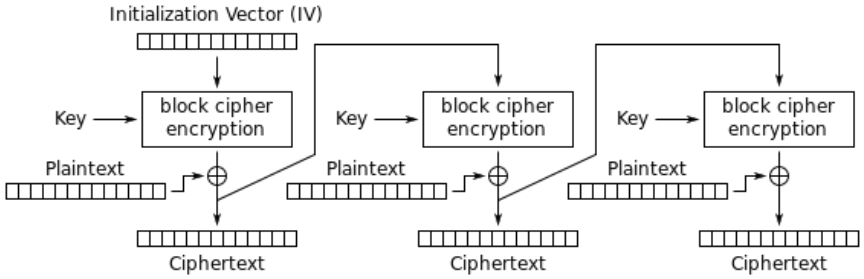


Electronic Codebook (ECB) mode encryption

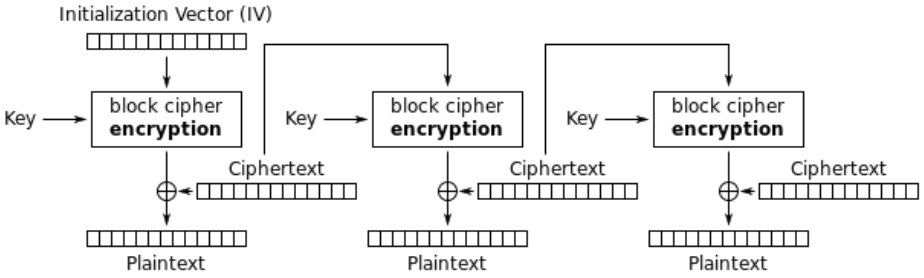


Electronic Codebook (ECB) mode decryption

7.2 CFB



Cipher Feedback (CFB) mode encryption



Cipher Feedback (CFB) mode decryption