

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 incryptie.

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

În primul rând, o instanță a Serverului trebuie să fie pornită. Executabilul de Server se regăsește în folderul "bin". Nu este necesară pasarea vreunui argument la linia de comandă.

Executabilul de Client se regăsește în folderul "bin". Trebuie pasat un argument la linia de comandă, specificând modul de operare folosit("ecb"/"ECB" ori "cfb"/"CFB"). Dacă argumentul este invalid, Clientul va folosi CFB.

Serverul va aștepta conexiuni. După conectarea unui Client, toți ceilalți Clienti sunt notificați. Apoi, se așteaptă un mesaj din partea noului Client, în cadrul căruia menționează dacă dorește să folosească modul de operare ECB, ori CFB, pentru criptarea AES. După recepționarea mesajului, se creează o cheie nouă și un vector de inițializare(random, folosind primita RAND_bytes() din headerul "openssl/rand.h" a bibliotecii openssl. Acestea sunt trimise, pe rand, către client. Din acel punct, Clientul respectiv este plasat în pool-ul de Clienti conectați.

Când un Client trimite un mesaj, acesta este decriptat de către server și recriptat, conform cheilor și vectorilor de inițializare asociați fiecărui altui Client, ca apoi criptotextele să fie trimise către ceilalți Clienti.

În momentul în care un Client se deconectează, Serverul detectează acest eveniment și notifică toți ceilalți Clienti.

6 Modalități de Criptare

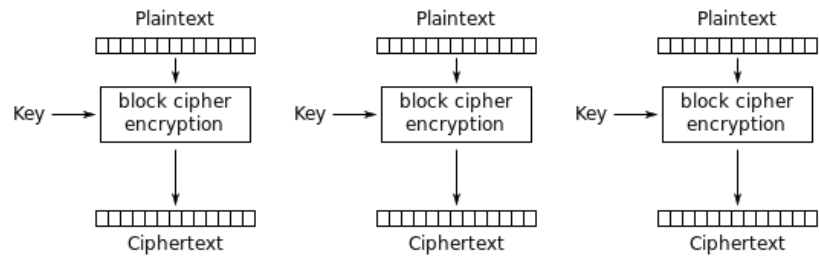
După realizarea conexiunii Serverului cu un Client, mesajul în care Clientul specifică modalitatea de criptare dorită este criptat folosind modul de operare CFB, având la dispoziție cheia și vectorul de inițializare din fișierele "key.pem" și "iv.pem". Răspunsul Serverului(continând o nouă cheie și un nou vector de inițializare, care urmează să fie folosite în comunicarea cu Clientul) va fi, de asemenea, încriptat folosind cheia și vectorul de inițializare inițial.

Fiecărui Client îi este asociată o cheie și un vector de inițializare, care sunt generate random la momentul conectării sale. Până la terminarea conexiunii, Serverul va comunica cu acel Client folosind respectiva cheie și respectivul vector de inițializare.

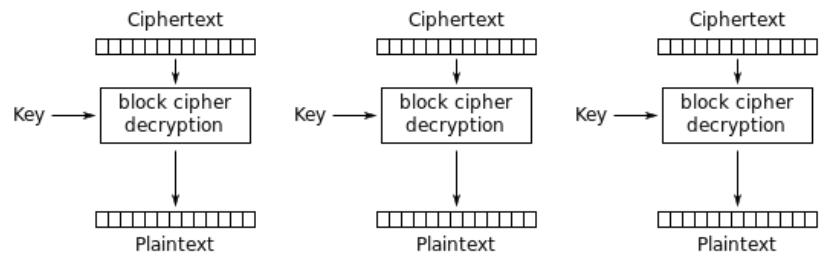
7 Implementări Moduri de Operare

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

7.1 ECB

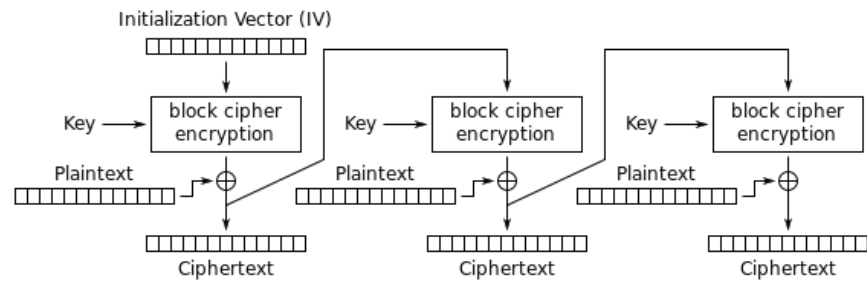


Electronic Codebook (ECB) mode encryption

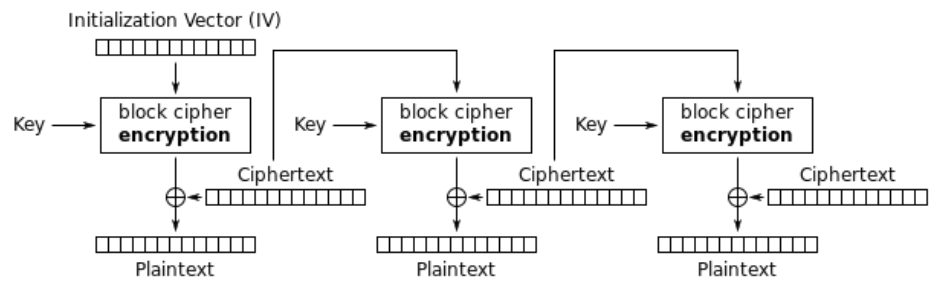


Electronic Codebook (ECB) mode decryption

7.2 CFB



Cipher Feedback (CFB) mode encryption



Cipher Feedback (CFB) mode decryption