- SI Tema1 Raport Tehnic

- Nume: Dinu Marius Ciprian
- Grupa: 3A5
- Prof: Anca-Maria Nica

Mediu de lucru

Pentru implementarea solutiei s-a folosit c++ cu API-ul EVP din OpenSSL pentru o implementare a algoritmului de criptare AES 128. Cheia K3 e detinuta de toate nodurile. Cheile K1 si K2 se afla in Key Manager, impreuna cu IV-ul pentru modul OFB

Rezolvare

Implementarea explicita a AES-128-ecb, AES-128-ofb

AES de baza exista in API-ul EVP, in openssl/aes.h
Acesta a fost scalat pe ECB si OFB

Implementarea problemei:

Se creaza un nod KM si asteapta doua conexiuni : A si B
Se creaza un nod A si asteapta o conexiune
Se creaza un nod B si se conecteaza la A

A si B se conecteaza la KM

A va cere de la tastatura un input, fie 0 (pentru ECB) fie 1 (pentru OFB). Acesta reprezinta modul de rulare a algoritmului. El va fi trimis catre B si KM

Fiindca KM nu stie cine e A sau B, B va trimite si el catre KM modul primit de la A.
Pe baza modului, KM trimite inapoi fie cheia K1, fie K2 si IV
A si B se sincronizeaza pe baza mesajelor de la KM (fiecare contine cheia necesara si IV, unde e necesar (OFB))

A va cere un input reprezentand calea catre un fisier, pe care il va citi si cripta. Pe acesta il imparte si il trimite catre B block cu block.
B alcatuieste criptotextul si afiseaza pe ecran rezultatul decriptarii acestuia

III. Teste efectuale. Observatii

Testele aplicatiei au fost facute pe fisiere simplu text. Se poate presupune ca in cazul encoding-urilor mai avansate, cu implementarea curenta pot rezulta erori.