Tema laborator - Tema 1- 25 puncte

Implementati o infrastructura de comunicatie ce foloseste criptosistemul AES pentru criptarea traficului intre doua noduri A si B cu urmatoarele caracteristici:

1. *Se considera un nod KM (key manager) care detine doua chei pe 128 de biţi K si K'. Cheia K este asociata cu un mod de operare CBC sau OFB. Cheia K' este utilizata pentru criptarea cheii K. Se considera ca vectorul de initializare are o valoare fixata cunoscuta din start atat de A cat si de B. De asemenea cheia K' este detinuta din start si de A si de B.*

2. *Pentru a initia o sesiune de comunicare securizata nodul A trimite un mesaj catre B in care comunica modul de operare (CBC sau OFB), cerand in acelasi timp nodului KM cheia de criptare. Acesta genereaza cheia K in mod random, cu ajutorul unei librarii criptografice, si apoi o cripteaza ca un singur bloc cu AES folosind cheia K', dupa care o trimite nodului A. Dupa ce A primeste cheia criptata de la KM, acesta o trimite mai departe nodului B. A si B vor decripta cheia K pentru a incepe comunicarea. De asemenea nodul B va trimite catre A un mesaj de incepere a comunicarii.*

3. *Dupa primirea mesajului de confirmare de la B (referitor la inceperea comunicarii), A incepe sa trimita catre B continutul unui fisier criptat pe blocuri folosind modul selectat. Nodul B va decripta blocurile primite si va afisa rezultatul obtinut.*

Observatie

Se accepta orice limbaj si folosirea oricarei librarii pentru implementare. AES poate fi folosit ca algoritm de criptare pus la dispozitie de orice librarie criptografica. Modul de operare (CBC si OFB) se cere sa fie implementat in cadrul temei. Nu se cere rezolvarea de eventuale probleme de sincronizare intre noduri, interfata pentru noduri, sau un anumit protocol de comunicare.

Termen de predare strict prin e-mail la adresa liliana.cojocaru@info.uaic.ro pana pe data de 8 noiembrie (preferabil link spre un repository cu sursele). Finalizarea evaluarii temei va avea loc in laboratorul din data de 11 noiembrie.