Tema 1 - Grupa I3B6
(25 de puncte)

October 19, 2020

Implementaţi o infrastructură de comunicaţie ce utilizează criptosistemul AES şi modurile de operare pentru cifrurile bloc pentru criptarea traficului intre două noduri A şi B cu următoarele caracteristici:

- se consideră un nod KM (key manager) care deţine 3 chei pe 128 biţi, K_1, K_2, K_3, unde:
  - cheia K_1 este utilizată pentru comunicarea intre A şi B in modul ECB;
  - cheia K_2 este utilizată pentru comunicarea intre A şi B in modul CFB;
  - cheia K_3 este utilizată pentru criptarea cheilor K_1, K_2 şi a vectorului de iniţializare (pentru modul de operare OFB); K_3 va fi utilizată pentru comunicarea intre KM şi A, respectiv KM şi B;
  - cheia K_3 este deţinută din start de toate cele trei noduri (A, B, KM);
  - cheile K_1, K_2 sunt deţinute iniţial doar de KM;
  - KM va genera şi un vector de iniţializare;
- Schimbul de chei:
  - pentru a iniţia o sesiune de comunicare securizată, nodurile A şi B transmit nodului KM un mesaj cu modul de operare dorit (ECB sau CFB);
  - dacă cele două moduri de operare propuse coincid, KM transmite cheia asociată şi, eventual, vectorul de iniţializare (pentru modul CFB), celor două noduri; altfel, KM alege la intâmplare unul dintre cele două moduri de operare, il transmite nodurilor A

şi B, impreună cu cheia corespunzătoare şi eventual vectorul de iniţializare; in ambele situaţii, fiecare element transmis de KM va fi criptat prin cheia K_3;

- nodurile A şi B răspund nodului KM printr-un mesaj de confirmare, criptat cu cheia primită, in modul de operare ales;
- KM decriptează cele două mesaje şi transmite un mesaj de inceput al comunicaţiei către cele două noduri A şi B;

- Comunicare securizată: comunicaţia intre cele două noduri A şi B se va realiza direct:
  - nodul A va cripta conţinutul unui fişier utilizând modul de operare ales, cu cheia şi vectorul de iniţializare corespunzător şi il va transmite nodului B; după transmiterea a câte 8 blocuri, nodul A va transmite un mesaj nodului KM şi va aştepta răspunsul acestuia;
  - nodul B decriptează blocurile primite şi le afişează; după procesarea a câte 8 blocuri, va transmite un mesaj nodului KM şi va aştepta răspunsul acestuia;
  - nodul KM, la primirea celor două mesaje (de la A, respectiv de la B), va transmite celor două noduri un mesaj de continuare a operaţiilor de criptare/decriptare;
  - la final, nodurile A şi B vor transmite mesaje de finalizare nodului KM.

Cerinţe:

- se acceptă utilizarea oricărui limbaj de programare şi a oricărei biblioteci criptografice pentru implementare;
- AES poate fi folosit ca algoritm de criptare pus la dispoziţie de orice bibliotecă criptografică;
- modul de operare al algoritmului (ECB, CFB) trebuie implementat explicit (impărţire blocuri, operaţii, criptare/decriptare fiecare bloc in parte); de asemenea se cere şi implementarea unei soluţii pentru cazul in care fişierul ce urmează a fi criptat nu are o dimensiune care să se impartă fix la dimensiunea unui bloc (o variantă de padding pentru ultimul bloc).

Predarea temei:

- Termen de predare prin email fix: 7 noiembrie, ora 24:00 (arhiva cu sursele + documentaţie / link către o astfel de arhivă);
- Sursele programului vor fi insoţite de un document ce va descrie modalitatea de rezolvare, modul de lansare in execuţie al aplicaţiei;
- Finalizarea evaluării temei va avea loc in laboratorul din data de 11 noiembrie, după o programare comunicată in prealabil.