Tema 1 - Grupa I3B3
(25 de puncte)

October 15, 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 KM;
  - cheia K_2 este utilizată pentru comunicarea intre B şi KM;
  - cheia K_3 este utilizată pentru criptarea cheilor K_1, K_2 şi a vectorilor de iniţializare;
  - 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 doi vectori de iniţializare;
- Schimbul de chei:
  - pentru a iniţia o sesiune de comunicare securizată, nodul A transmite un mesaj nodului KM cu modul de operare dorit (CBC, CFB);
  - nodul KM ii răspunde lui A cu două mesaje criptate fiecare cu cheia K_3, primul mesaj conţinând cheia corespunzătoare (K_1), al doilea mesaj conţinând un vector de iniţializare;
  - nodul KM ii transmite lui B celălalt mod de operare (A şi B vor utiliza moduri diferite de operare);
  - nodul B transmite un mesaj de confirmare;

  - nodul KM transmite nodului B cheia K_2 şi un vector de iniţializare, prin două mesaje diferite, criptate cu cheia K_3;
  - nodurile A şi B răspund nodului KM printr-un mesaj de confirmare, criptat cu cheia primită (K_1, respectiv K_2);
  - 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 prin intermediul nodului KM:

  - nodul A va cripta conţinutul unui fişier utilizând modul de operare ales, cu cheia şi vectorul de iniţializare corespunzător şi va transmite nodului KM intâi numărul de blocuri criptotext, iar apoi fiecare bloc criptotext separat (KM va primi $n + 1$ mesaje, unde n este numărul de blocuri din fişier, primul conţinând numărul n criptat in acelaşi mod ca şi blocurile de text);
  - nodul KM decriptează blocurile primite de la A, le criptează cu cheia pentru B şi le transmite, in ordine, nodului B;
  - nodul B decriptează blocurile primite, afişează rezultatul şi transmite mesaj de confirmare nodului KM;
  - la primirea mesajului de la B, nodul KM transmite mesaj de confirmare nodului A.

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 (CBC, CFB, OFB) 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: 1 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 5 noiembrie, după o programare comunicată in prealabil.