Securitatea informației: Tema #1

Până la 19 octombire 2021 ora 14:00

Asist. Dr. Anca-Maria Nica

Moduri de operare - criptosisteme bloc

Punctaj maxim: 25 puncte

Implementați o infrastructură de comunicație ce folosește criptosistemul AES pentru criptarea traficului dintre două noduri A și B cu următoarele caracteristici:

- se consideră un nod MC (manager de chei) care deține trei chei pe 128 de biți: k_1, k_2 și K
  - cheia k_1 este asociată cu modul de operare ECB;
  - cheia k_2 este asociată cu modul de operare XXX (se consideră că vectorul de inițializare are o valoare fixată, cunoscută in prealabil de cele două noduri A și B);
  - cheia K este utilizată pentru criptarea cheilor k_1 sau k_2. Cheia K este deținută din start de nodurile A, B și MC.
- Pentru a inița o sesiune de comunicare securizată, nodul A trimite un mesaj către nodul B în care comunică modul de operare (ECB sau XXX); de asemenea, nodul A transmite un mesaj nodului MC prin care cere cheia corespunzătoare (k_1 pentru modul de operare ECB, respectiv k_2 pentru modul de operare XXX).
- Nodul B, la primirea mesajului de la nodul A, cere nodului MC cheia corespunzătoare (k_1 pentru modul de operare ECB, respectiv k_2 pentru modul de operare XXX).
- nodul MC va cripta cheia cerută (k_1 sau k_2 în funcție de modul de operare ales) ca un singur bloc, utilizând criptosistemul AES cu cheia K și va trimite mesajul astfel obținut ca răspuns pentru nodurile A și B;
- cele două noduri A și B vor decripta mesajul primit de la MC și vor obține astfel cheia cerută;
- nodul B trimite, după primirea cheii, un mesaj nodului A prin care îl anunță că poate să înceapă comunicarea;
- nodul A criptează conținutul unui fișier text utilizând AES, cheia primită de la MC și modul de operare ales. A va transmite nodului B blocurile de criptotext obținute pe rând, iar nodul B va decripta blocurile primite și va afișa rezultatul obținut.

Observații:

- se acceptă utilizarea oricărui limbaj de programare și folosirea oricărei librarii criptografice pentru implementare;
- AES poate fi folosit ca algoritm de criptare pus la dispoziție de orice librarie criptografică.
- se cere ca modurile de operare (ECB și XXX) să fie implementate în cadrul temei, unde XXX poate fi unul din modurile $\{CBC, OFB, CFB\}$.
- nu se cere rezolvarea de eventuale probleme de sincronizare între noduri, interfață pentru noduri, sau un anumit protocol de comunicare.

Precizări importante

Tema este individuală. Orice tentativă de fraudă este penalizată prin acordarea punctajului 0 tuturor studenților implicați. Fiecare student(ă) va trimite prin e-mail la adresa teaching@ancamarianica.ro o arhivă cu numele: grupă_nume_prenume, având următoarele fișiere:

- fișierele sursă ce conțin implementarea cerinţelor exercițiului, inclusiv un fișier *makefile* pentru compilare, dacă este cazul;
- fișiere de intrare, respectiv de ieșire, dacă este cazul;
- un document ce va conține:
  - descrierea mediului de lucru utilizat (alte setări decât cele prezentate în acest document);
  - descrierea modului de rezolvare a cerinței exercițiului;
  - testele efectuate pe diverse fișiere de intrare și observațiile efectuate.

Termenul de predare a arhivei cu tema este cel precizat pe pagina de titlu.
Nu se admit întârzieri decât în cazuri bine justificate, anunțate în prealabil.