Documentatie Tema1-Securitatea Informatiei

Structura de comunicatie intre nodurile A, B si KM, este reprezentata de un model client-server, bazat pe thread-uri, unde KM este serverul si nodurile A si B sunt clientii.

Ordinea in care se conecteaza clientii este urmatoarea: prima data se va conecta clientul A, apoi clientul B. Nerespectarea acestei ordini poate afecta comunicarea si buna functionare a intregului program.

In „KM.cpp” am realizat o functie numita dupa numele fisierului. In acea functie, am creat cheile k1 ,k2 si vectorul de initializare(iv), in mod aleatoriu. Dupa ce am creat cheile k1 si k2 le-am criptat in modurile ECB si CFB si vectorul de initializare la fel.

Structura arhitecturii client-server este una clasica, am folosit pentru a-l crea diverse resurse pe care le aveam din anul precedent si folosind si alte resurse de pe internet.

In functia „raspunde” din KM este tot codul care este cerut de catre datele problemei. Initial KM primeste de la A si B modurile alese de catre ei. Daca cele doua moduri coincid atunci KM va crea cheile k1, k2 si iv si va trimimte un mesaj de inceput lui A si B, impreuna cu chia criptata, conform modului ales.Nodurile A si B vor decripta, fiecare intr-o functie separata,cheia primita de la KM in modul ales. KM va primi de la A si B un mesaj de confirmare ca au primit cele trimise si va decripta acel mesaj in modul corespunzator, urmand sa le trimita inapoi un mesaj de inceput de comunicare.

Daca modurile nu coincid, am folosit functia rand() pentru a genera un numar intre 0 si 1. Daca numarul este 1, va fi ales modul ECB, in caz contrar va fi ales modul CFB, restul procedurilor intre A si B ramand neschimbate.

Spre deosebire de textul exercitiului, nodurile A si B nu comunica direct, ci prin intermediul lui KM(lucru care am inteles ca ar fi permis).

Nodul A va incepe citirea din fisierul text.txt care contine textul ce trebuie criptat. Cat timp in fisier mai sunt blocuri de text ce pot fi citite, nodul A va transmite un mesaj corespunzator lui KM. Nodul A va cripta in modul ales dat de catre KM si va trimite blocul de text criptat catre acesta.

Imediat ce primeste textul criptat de la A, KM va juca un rol de intermediar intre cele doua noduri si va trimite lui B un mesaj, daca poate continua sau nu, impreuna cu textul pe care acesta trebuie sa il decripteze. Cat timp mesajul de la KM nu este negativ, nodul B va decripta si va afisa textul primit.

Cand din fisierul text.txt nu mai este ce citi, nodul A ii va trimite lui KM un mesaj cu textul „finish”, care va fi transmis si lui B, acest mesaj semnificand conditia de oprire a celor doua noduri.

Din nefericire, nu am reusit sa transmit vectorul de initializare criptat(l-am trimis in forma in care a fost creat, aleator) din cauza unor erori aparute la criptare/decriptare in nodurile A si B. Un alt lucru ar fi ca nu am reusit sa decriptez cate 8 blocuri in nodul B si nici sa trimit cate 8 blocuri din nodul A. De-asemenea nu am tratat cazul in care la final, ultimul bloc nu are o dimensiune fixa(nu am facut padding).

Cu toate cele spuse mai sus, programul rula si facea cele cerute de cerinta. Din dorinta de a incerca sa implementez si neajunsurile pe care le continea tema, am modificat unele bucati de cod in incercarea de a-l face mai bun. In final m-am ales cu o versiune care avea unele bug-uri si nu mai facea lucrurile in modul cerut. Nu am avut acces la o versiune anterioara corecta(nu am avut nici un back-up) si am incercat sa modific si mai mult ceea ce aveam deja pentru a functiona.

Programul in teorie functioneaza, am verificat rand cu rand, procedura cu procedura, fiecare send si receive, insa undeva in lucrurile acestea este o lipsa. Serverul intra intr-o stare de asteptare din care nu mai iese, blocand astfel si nodurile A si B din a mai face ceva(am verificat foarte atent toate receive-urile si send-urile si nu am vazut problema).

Am incercat sa vad cat mai mult comunicarea intre noduri, afisand pe ecran mesaje de primire/trimitere si ceea a fost primit/trimis.

Punctual, tema respecta majoritatea conditiilor, iar cerintele specificate in tema se regasesc si in cod, insa rezultatul final nu este cel dorit.