Documentatie Tema 1

Limbaj folosit

Am utilizat in tema 1 **Python 3.6** si libraria Crypto.Cipher (py -3 –m pip install crypto)

Modalitate de rezolvare

Infrastructura de comunicatie consta in 3 scripturi (node_KM, node_A, node_B).

Scriptul node_KM se ocupa de gestionarea cheilor (corespunde nodului KM) si indeplineste cerintele temei (trimite mesajele cerute, corespunzator).

Scriptul node_A se ocupa de initierea sesiunii de comunicare securizata, face schimbul de mesaje necesare cu nodul KM, iar dupa ce a fost finalizata gestionarea cheilor, va citi textul dintr-un fisier (nu este limitata dimensiunea fisierului – fisierul pe care am testat are 17910 bytes) si va trimite nodului B textul criptat, iar in final trimite nodului KM numarul de blocuri criptate si transmise

Scriptul node_B se ocupa cu decriptarea blocurilor primite si trimite nodului KM numerele cerute.

In scriptul "criptosisteme" sunt implementate algoritmii de criptare si decriptare ECB, CBC si CFB (am folosit algoritmul ECB pentru criptarea mesajelor identice trimise de catre nodul KM (cheia k1 sau k2 si vectorul de initializare), si functiile ajutatoare pentru algoritmii precizati mai sus (padare, eliminarea padarii, xor intre 2 stringuri/bytestring, impartirea stringului in blocuri)

Modalitatea de lansare in executie

py -3.6 node_KM.py

py -3.6 node_A.py

py -3.6 node_B.py

Precizez ca este nevoie rularea in aceasta ordine a scripturilor.

Am precizat versiunea de python pentru ca pe aceasta am folosit-o, cel mai probabil functioneaza si cu alte versiuni de python 3(nu am testat si alte versiuni).