**Tema 1**

**Descrierea mediului de lucru**

Limbajul folosit este Java, iar Ide-ul folosit este Intelij, prin urmare nu este nevoie de un makefile.

**Descrierea modului de rezolvare a cerintelor exercitiului**

Cheile sunt initializate folosind stringuri cu ajutorul metodei **setKeys** din clasa **ManagerNode**. **Modul** de criptare este ales **random** de program in main. Criptarea cheilor este facuta de clasa ManagerNode in metoda **encryptKey** folosind un obiect de tipul javax.crypto.Cipher. Decriptarea se face de catre fiecare obiect individual A si B prin metoda **decrypt**, folosind acelasi tip de obiect.

Metoda **readInput** din clasa Node citeste din fisierul input.txt si ***imparte mesajul in blocuri*** pe care le trimite ca parametru metodelor **sendECB** si **sendCFB** din aceeasi clasa. Aceste metode cripteaza mesajul si il trimit ca parametru metodelor **decECB** respective **decCFB** ale nodului B(al doilea obiect-B- de tip Node incorporat ca atribut in obiectul A).

**Expandarea cheilor** este facuta de metodele **expKeyEnc** si **expKeyDec** care folosesc metodele **rotateWord** si **getInverse** (inversul modular in GF(2^8)) si fac **substitutia**(Rjindael`s sBox). Constantele rcon si matricea de inlocuire pentru getInverse sunt hardcodate.

In metoda **sendECB** are loc criptarea. Mai intai se apeleaza metoda expKey apoi se face **substitutia** **sBox** (pasul **SubTypes**), apoi **permutarea** **liniilor**, apoi permutarea coloanelor(pasul **MixColumns**). La permutarea coloanelor se foloseste o matrice 4X4, diferita pentru decriptare, hardcodata. La finalul fiecare runde se adauga **cheia de runda** din **expKey** iar pasul MixColumns este sarit pentru ultima runda.

**Diferenta dintre metodele sendECB si sendCFB** care sunt similare este ca prima metoda **cripteaza** **mesajul** iar a doua metoda **cripteaza** **vectorul de initializare iV** in acelasi mod apoi la final face **xor cu mesajul,** la urmatorul bloc de mesaj vectorul de initializare fiind modificat(pentru a face posibila inlantuirea).

**Teste efectuate**

Programul compileaza fara erori si cripteaza/decripteaza corect cheile (afisate din main in bytes) dar nu si mesajul (afisat caracter dupa caracter).