ECB/CFB Encryption

Vina Andreea Madalina 3A3

19 octombrie 2021

1 Limbajul folosit

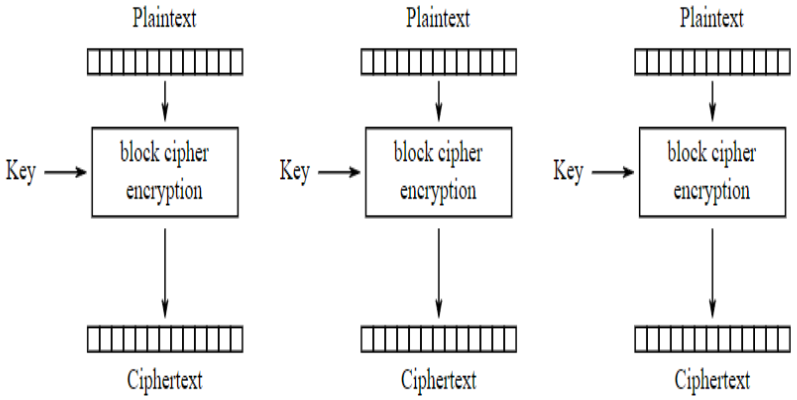
Limbajul folosit în cadrul acestei teme este Python pentru ușurința scrierii codului dar și a folosirii librăriilor criptografice.
Scrierea codului a fost realizată în VS Studio Code.

2 Modul de rezolvare al cerințelor

- Studierea celor doua diagrame pentru modurile de criptare alese : ECB și CBC.
- Crearea a doua fișiere : ECB.py si CFB.py care au două funcții : funcția de criptarea a unui text primit ca parametru împreună cu cheia cu care se dorește să se realizeze criptarea și funcția de decriptare care primește ca parametru textul criptat împreună cu cheia de decriptare utilizată și in cadrul criptării.
- Crearea unui manager de chei care retinea K, k1, k2.
- Crearea a două noduri A și B unde : A cere de la tastatură introducerea unui mod de criptate : ECB/CFB și transmite mai departe către nodul B acest mod. Atât A cat și B cer cheile de criptare in funcție de modul ales de la managerul de chei, le decriptează și încep criptarea (A) respectiv decriptarea (B).

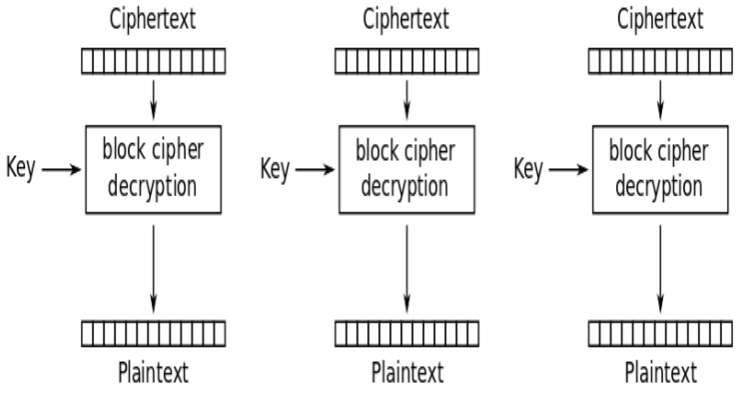
3 ECB

Modul de criptare ECB este unul destul de simplist și din același motiv nu foarte sigur.
El împarte textul primit in blocuri de 16 biți, criptează folosind cheia aleasă anterior și lipește rezultatul, obținându-se astfel textul criptat.//



Electronic Codebook (ECB) mode encryption

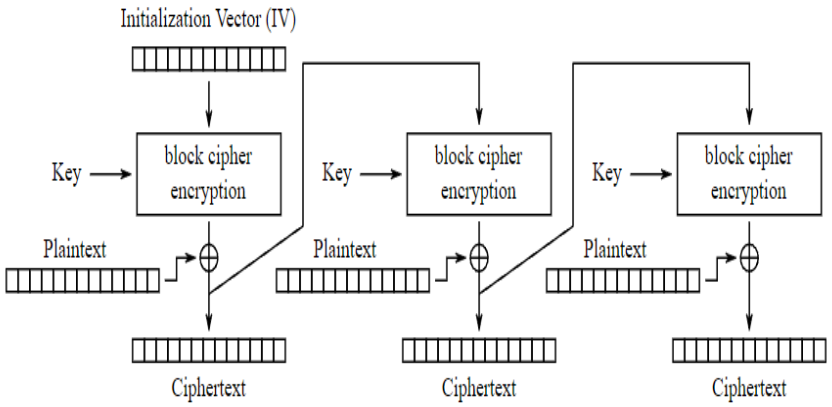
Decriptarea se realizeaza în mod asemănător conform schemei de mai jos :



Electronic Codebook (ECB) mode decryption

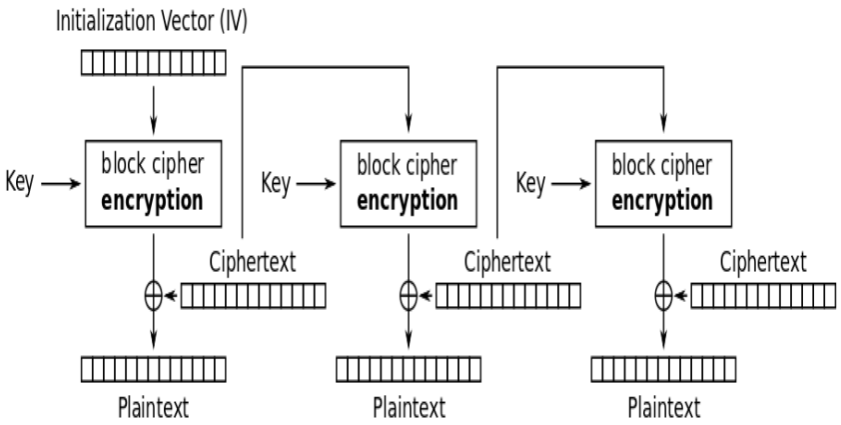
4 CFB

Modul de criptare CFB primește textul original împreună cu cheia de criptare, iar în cazul primului bloc de 16 biți criptarea se realizeaza cu ajutorul vectorului de inițializare obținându-se ceea ce este reprezentat în schemă ca "block cipher encryption". Între acesta și Plain text se realizează operația de XOR, iar rezultatul va ține loc de vectorul de inițializare pentru urmatoarele blocuri de 16 biți.



Cipher Feedback (CFB) mode encryption

Decriptarea se relizează în mod asemănător :



Cipher Feedback (CFB) mode decryption

5 Teste realizate

S-au realizat teste atât de dimensiuni mici : un cuvânt/o propoziție, teste de dimensiuni medii : fraze pe mai multe linii, cât și teste de dimensiuni mari : scriptul din fimul de animație Shrek, toate cu rezultate bune.