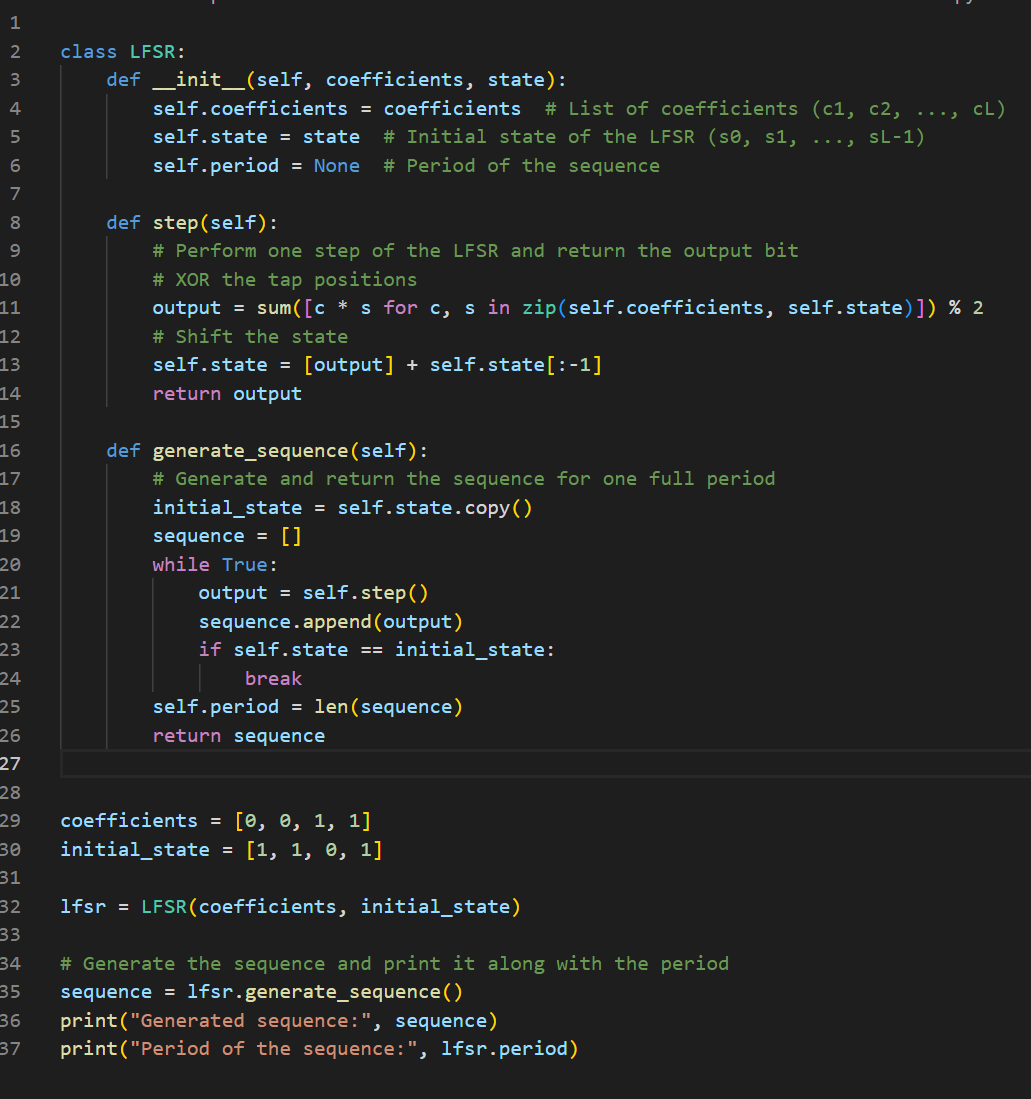
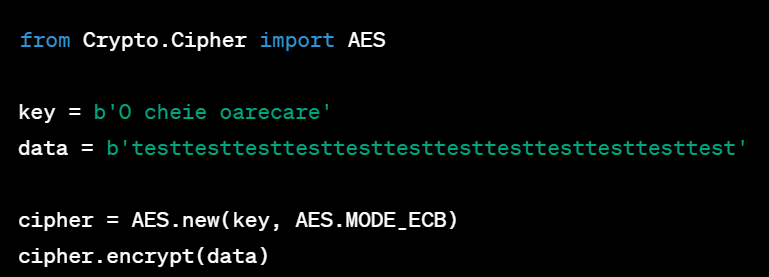
**Laboratorul 6**

1. ****Linear Feedback Shift Registers (LFSRs)

2. Advanced Encryption Standard (AES)



a) Am obținut următorul șir de caractere hexazecimale reprezentând datele criptate:

b'\x88\x10\x86\xe2\xf3\xaai)\x9fz\xcb\xf0h4\xa4\xec\x88\x10\x86\xe2\xf3\xaai)\x9fz\xcb\xf0h4\xa4\xec\x88\x10\x86\xe2\xf3\xaai)\x9fz\xcb\xf0h4\xa4\xec'

Modul de operare folosit este ECB (Electronic Codebook). Observ ca acest mod de operare nu este cel mai sigur pentru criptarea datelor deoarece blocuri identice de text clar vor produce blocuri identice de text criptat. Acest lucru poate permite unui atacator să identifice modele în datele criptate.



Nu aș recomanda folosirea modului ECB din cauza problemelor de securitate menționate anterior. Este vulnerabil la analiza de pattern-uri și nu adaugă aleatoriu la datele criptate, ceea ce este esențial pentru securitatea criptării.



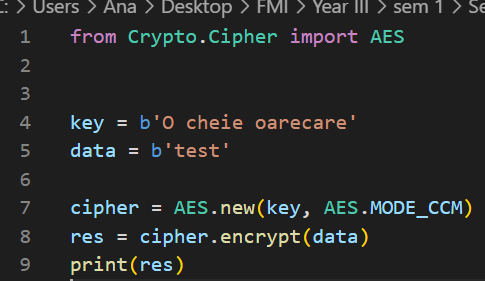
Dimenisunea cheii este 16, la fel si a blocului, specific modului ECB. Cheia de criptare va fi mereu multiplu de 16.



Pentru a face codul să funcționeze cu data=b'test', trebuie să adăugăm padding la date, deoarece AES necesită ca datele de intrare să fie un multiplu al dimensiunii blocului (16 octeți).



Am modificat modul de operare cu CCM, care functioneaza pe date de lungime variabila.



3. Atacul Meet-in-the-Middle

