

Răspundeți la următoarele cerințe:

- Executați secvența de mai sus. Ce obțineți?
- Ce mod de operare este folosit? Ce observați?
- Ați recomanda folosirea modului de operare de la b)? De ce? De ce nu?
- Care este dimensiunea cheii? Dar a blocului?
- Modificați codul astfel încât să funcționeze dacă se înlocuiește valoarea `data` cu `data=b'test'`.
- Refaceți codul, schimbând modul de operare cu un alt mod de operare pe care îl considerați mai potrivit.

3. Atacul *Meet-in-the-Middle*



Înțelegeți cum funcționează *Data Encryption Standard (DES)* și atacul *Meet-in-the-Middle* citind [1], pg.129-133 și vizionând [3,4]. Înțelegeți de ce *Triple—DES* este folosit, în timp ce „*Double-DES*” nu aduce beneficii majore.



Se dă următoarea secvență de instrucțiuni, pentru care ? din `key1` și `key2` reprezintă o cifră hexazecimală necunoscută:

```
from Crypto.Cipher import DES

key1 = '\x?0\x00\x00\x00\x00\x00\x00\x00'
key2 = '\x?0\x00\x00\x00\x00\x00\x00\x00'

cipher1 = DES.new(key1, DES.MODE_ECB)
cipher2 = DES.new(key2, DES.MODE_ECB)

plaintext = "Provocare MitM!!"
ciphertext = cipher2.encrypt(cipher1.encrypt(plaintext))
```

În urma execuției, se obține:

```
ciphertext = "G\xfd\xdfpd\xa5\xc9'C\xe2\xf0\x84)\xef\xeb\xf9"
```

Implementați un atac de tip *Meet-in-the-Middle* pentru a determina cele 2 chei (i.e., cele două valori hexazecimale marcate cu ?). Câte chei ați testat în total? Câte criptări / decriptări ați făcut?

Referințe bibliografice

1. Kryszzczuk, K., & Richiardi, J. (2014). *Springer Encyclopedia of Cryptography and Security*. Accesibil la: https://www.researchgate.net/publication/230674947_Springer_Encyclopedia_of_Cryptography_and_Security Ultima accesare: septembrie 2021.
2. PyCryptodome. *AES*. <https://pycryptodome.readthedocs.io/en/latest/src/cipher/aes.html> Ultima accesare: noiembrie 2021.
3. D.Boneh. *Cryptography – The Data Encryption Standard*. Accesibil la: <https://youtu.be/l-uZvAlFEEU?list=PL2jykFOD1AWYosqucluZghEVjUkopdD1e> Ultima accesare: noiembrie 2021.
4. D.Boneh. *Cryptography – Exhaustive Search Attacks*. Accesibil la: https://youtu.be/V_HFxe73Kpg?list=PL2jykFOD1AWYosqucluZghEVjUkopdD1e Ultima accesare: noiembrie 2021.