Mîndruleanu Matei Daniel - tema 3 SSI

Exercitiul 1:

1)

```
import base64

cripted_code = "o9/khC3Pf3/9CyNCbdzHPy5oorccEawZSFt3mgCicRnihDSM8Obhlp3vviAVuBbiO
tCSz6husBWqhfF0Q/8EZ+6iI9KygD3hAfFgnzyv9w=="
hex_key = "ecb181a479a6121add5b42264db9b44b4b48d7d93c62c56a3c3e1aba64c7517a90ed44
f8919484b6ed8acc4670db62c249b9f5bada4ed474c9e4d111308b614788cd4fbdc1e949c1629e12f
a5fdbd9"

bytees = base64.b64decode(cripted_code)
key = bytes.fromhex(hex_key)

print(bytes(a^b for a,b in zip(bytees, key)))
```

```
Output:
b'One Time Pad este un sistem de criptare perfect sigur daca este folosit corect.
'
```

Transformam mesajul criptat si cheia in bytes, dupa care le xoram intre ele pentru a afla mesajul decriptat.

2)

```
cripted_code = "o9/khC3Pf3/9CyNCbdzHPy5oorccEawZSFt3mgCicRnihDSM8Obhlp3vviAVuBbiO
tCSz6husBWqhfF0Q/8EZ+6iI9KygD3hAfFgnzyv9w=="
decripted_code = b"Orice text clar poate obtinut dintr-
un text criptat cu OTP dar cu o alta cheie."

bytees = base64.b64decode(cripted_code)

print(base64.b64encode(bytes(a^b for a,b in zip(bytees, decripted_code))))
```

```
Output:
b'7K2N50jvCxqFfwMhAb21H14Hw8N5McN7PDIZ73SCFXCM8EahhYjB4viXygB2yn+STrHm78sbkFr+1dE
QIo0kBJuCTPLT7EmAIZII+lXK2Q=='
```

Transormam in binar doar mesajul criptat si xoram cu mesajul decriptat, dupa care afisam cheia in baza 64.

3)

Criptarea a 2 sau mai multor mesaje cu aceeasi cheie nu este secure deoarece daca criptam 2 mesaje cu aceeasi cheie, apoi xoram mesajele criptate obtinute intre ele, se pot extrage informatii din ambele mesaje folosind criptanaliza.

Exercitiul 2:

1)

Substitutia mono-alfabetica este un sistem de criptare care foloseste metoda substitutiei. Se alege un alfabet aleatoriu, punand toare literele din alfabetul englez in alta ordine decat cea obisnuita. Fiecare litera din mesajul ce urmeaza sa fie criptat va fi transformata in litera cu acelasi index cu aceasta (in alfabetul englez) in alfabetul ales. Mesajul se poate decripta stiind alfabetul utilizand aceeasi metoda, doar ca invers. Fara a sti alfabetul, se aplica un algoritm bazat pe frecventa aparitiilor, ceea ce il face vulnerabil la atacurile cu asemenea algoritmi. <Intr-un mesaj criptat destul de mare se ordoneaza literele in ordinea frecventei aparitiilor, urmand ca acestea sa fie inlocuite la decriptare cu literele cu acelasi index din lista literelor alfabetului englez, tot ordonate dupa frecventa>

Exemplu:

Avem alfabetul AZERTYUIOPQSDFGHJKLMWXCVBN

Litera ‘B’, dupa criptare, va fi ‘Z’

Exemplu:

Avem alfabetul AZERTYUIOPQSDFGHJKLMWXCVBN

Mesajul initial: ‘Ana has apples.’

Mesajul criptat: ‘Afa ial ahhstl.’

Mesajul dupa decriptarea stiind alfabetul: ‘Ana has apples.’

Mesajul dupa decriptarea cu frecventa: ‘TAT ITS TOONES.’ Deci putem vedea ca decriptarea cu frecventa nu este deloc accurate cand vine vorba de texte mici.

2)

Criptarea cu transpozitii este un sistem de criptare care foloseste metoda transpozitiei. Se alege o transpozitie si se alege un mod de citire si de scriere.

Exemplu: ‘mamaliga branza’ grupez mesajul in grupe de cate 3 caractere si aleg transpozitia 123 = 213. Scriem pe linii.

mam = amm /

ali = lai /

ga_ = ag_ /

bra = rba /

nza = zna

Citim pe coloane -> ‘alarzmagbnmi aa’

Decriptare:

Impartim mesajul criptat astfel cat sa ramanem cu 3 grupe si le scriem pe coloane, dupa care aplicam transpozitia inversa 213 = 123:

A m m = mam

L a i = ali

A g _ = ga_

R b a = bra

Z n a = nza

Citim pe linii: ‘mamaliga branza’

In cazul in care nu avem caractere multiplu de 3, la criptare umplem ultima grupa cu caracterul vid si le introducem in mesajul criptat, la decriptare trebuie sa stim pozitia caracterului/caracterelor vid/vide.

Ca Securitate, metoda nu este foarte sigura deoarece are aproape la fle de multe caractere ca mesajul intiail (cu eroare de maxim 2) si poate fi vulnerabil la atacurile algoritmilor de frecventa, ca mono-alfabeticul.

Putem decripta, ne stiind cheia, ghicind permutarea sau ghicind un cuvand si deducand permutarea, sau cu algoritmul de anagrame daca textul este foarte mic, sau folosing algoritmii de frecventa, care, dupa cum am demonstrate mai sus nu sunt deloc eficienti la texte mici.

Exercitiul 3:

ALICE AND FOF ARE THE WORLDS MOST BAMOUS CRYPTOGRAPHIC COUPLE. SINCE THEIR INVENTION IN 1978, THEY HAVE AT ONCE FEEN CALLED INSEPARAFLE, AND HAVE FEEN THE SUFJECT OB NUMEROUS DIVORCES, TRAVELS, AND TORMENTS. IN THE ENSUING YEARS, OTHER CHARACTERS HAVE JOINED THEIR CRYPTOGRAPHIC BAMILY. THERES EVE, THE PASSIVE AND SUFMISSIVE EAVESDROPPER, MALLORY THE MALICIOUS ATTACKER, AND TRENT, TRUSTED FY ALL, JUST TO NAME A BEW. WHILE ALICE, FOF, AND THEIR EXTENDED BAMILY WERE ORIGINALLY USED TO EXPLAIN HOW PUFLIC KEY CRYPTOGRAPHY WORKS, THEY HAVE SINCE FECOME WIDELY USED ACROSS OTHER SCIENCE AND ENGINEERING DOMAINS. THEIR INBLUENCE CONTINUES TO GROW OUTSIDE OB ACADEMIA AS WELL: ALICE AND FOF ARE NOW A PART OB GEEK LORE, AND SUFJECT TO NARRATIVES AND VISUAL DEPICTIONS THAT COMFINE PEDAGOGY WITH IN-JOKES, OBTEN REBLECTING OB THE SEXIST AND HETERONORMATIVE ENVIRONMENTS IN WHICH THEY WERE FORN AND CONTINUE TO FE USED. MORE THAN JUST THE WORLDS MOST BAMOUS CRYPTOGRAPHIC COUPLE, ALICE AND FOF HAVE FECOME AN ARCHETYPE OB DIGITAL EXCHANGE, AND A LENS THROUGH WHICH TO VIEW FROADER DIGITAL CULTURE. Q.DUPONT AND A.CATTAPAN CRYPTOCOUPLE.

Textul este decriptat aproape corect, mesajul fiind lizibil. Textul este destul de lung cat sa se poata folosi un algoritm de frecventa.