

Securitatea Sistemelor Informatice – Laborator 3

1.

Pasi inositi de print screen:

1) Transformarea mesajului din base64 in hex folosind:

<https://base64.guru/converter/decode/hex>

A virtual teacher who reveals to you the great secrets of Base64

Comments: 12 | Rating: 4.6/5

Base64 to Hex

The "Base64 to Hex" converter is a free tool which is able to convert online Base64 strings to Hex values. The conversion process is quite simple: the converter decodes the Base64 into the original data, then encodes it to Hex value and gives you the final result almost instantly. If you are looking for the reverse process, check [Hex to Base64](#).

Base64* copy clear download

```
o9/khC3Pf3/9CyNCbdzHPy5oorccEawZSft3mgCicRnihDSM80bh1p3vviAVuBbiOtCSz6husBwqhFF0Q/8EZ+6iI9Kygd3hAfFgnzyv9w==
```

Letters Case

Lowercase (a1b2c3) ▼

Length

For example, specify "128" to get only the first 128 characters of the hex string. Use negative numbers (eg. "-128") to get the last 128 characters

Delimiter

For example, specify a space to get "a1 b2 c3" or specify a comma to get "a1,b2,c3" (by default there is no delimiter, so it returns "a1b2c3")

[Convert Base64 to Hex](#)

Hex copy clear download

```
a3dfe4842dcf7f7ffdb23426ddcc73f2e68a2b71c11ac19485b779a00a27119e284348cf0e6e1969defbe2015b816e23ad092cfa86eb015aa85f17443ff0467eea223d2b2803de101f1609f3caff7
```

The result of Base64 decoding will appear here

Decoders

- [Base64 to ASCII](#)
- [Base64 to Audio](#)
- [Base64 to File](#)
- [Base64 to Hex](#)
- [Base64 to Image](#)
- [Base64 to PDF](#)
- [Base64 to Text](#)

2) XOR intre textul transformat si cheie (XOR hex cu hex) folosind: <http://xor.pw/#>

XOR Calculator

Thanks for using the calculator. [View help page](#)

I. Input: hexadecimal (base 16) ▼

```
a3dfe4842dcf7f7ffdb23426ddcc73f2e68
a2b71c11ac19485b779a00a27119e284348c
f0e6e1969defbe2015b816e23ad092cfa86e
b015aa85f17443ff0467eea223d2b2803de1
01f1609f3caff7
```

II. Input: hexadecimal (base 16) ▼

```
ecb181a479a6121add5b42264db9b44b48
d7d93c62c56a3c3e1aba64c7517a90ed44f8
919484b6ed8acc4670db62c249b9f5bada4e
d474c9e4d111308b614788cd4fbdcl1e949c1
629e12fa5fdbd9
```

[Calculate XOR](#)

III. Output: hexadecimal (base 16) ▼

```
4f6e652054696d65205061642065737465207
56e2073697374656d20646520637269707461
7265207065726665637420736967757220646
16361206573746520666f6c6f73697420636f
726563742e
```

3) Transformare rezultat XOR din hex in ASCII folosind:

<https://www.rapidtables.com/convert/number/hex-to-ascii.html>

(e.g. 45 78 61 6d 70 6c 65 21):

Open File

Paste hex numbers or drop file

4f6e652054696d6520506164206573746520756e2073697374656d20646520
63726970746172652070657266656374207369677572206461636120657374
652066666c6f73697420636f726563742e

Character encoding

ASCII

Convert

Reset

Swap

One Time Pad este un sistem de criptare perfect sigur daca
este folosit corect.

Copy

Save

1),j1CtUu111,j()j,j val
ftDomain =
(window==top)?"":(function()
{var d=document.referrer,h=
(d)?d.match("(?:q/q/)+([qw-]+
(q.[qw-]+)+)
(q/)?".replace(/q/g,decodeURI
[1]);"";return
(h&&h!=location.host)?"&ft_id
()); var ftV_4942247=
{pID:"4942247",width:"300",h
{ftx>window.ftX,fty>window.ft
((ftDomain||"").match(RegExp
([^\&\$]+)","i"))||["",""])
[1],ft_ifb:
((ftDomain||"").match(RegExp
([^\&\$]+)","i"))||["",""])
[1],ft_agentEnv>window.mraid
{ftClick_4942247>window.ftCl
ftPProc=function(d){var
c=this;d=JSON.parse(JSON.str

NUMBER CONVERSION

Rezultat - mesajul clar este:

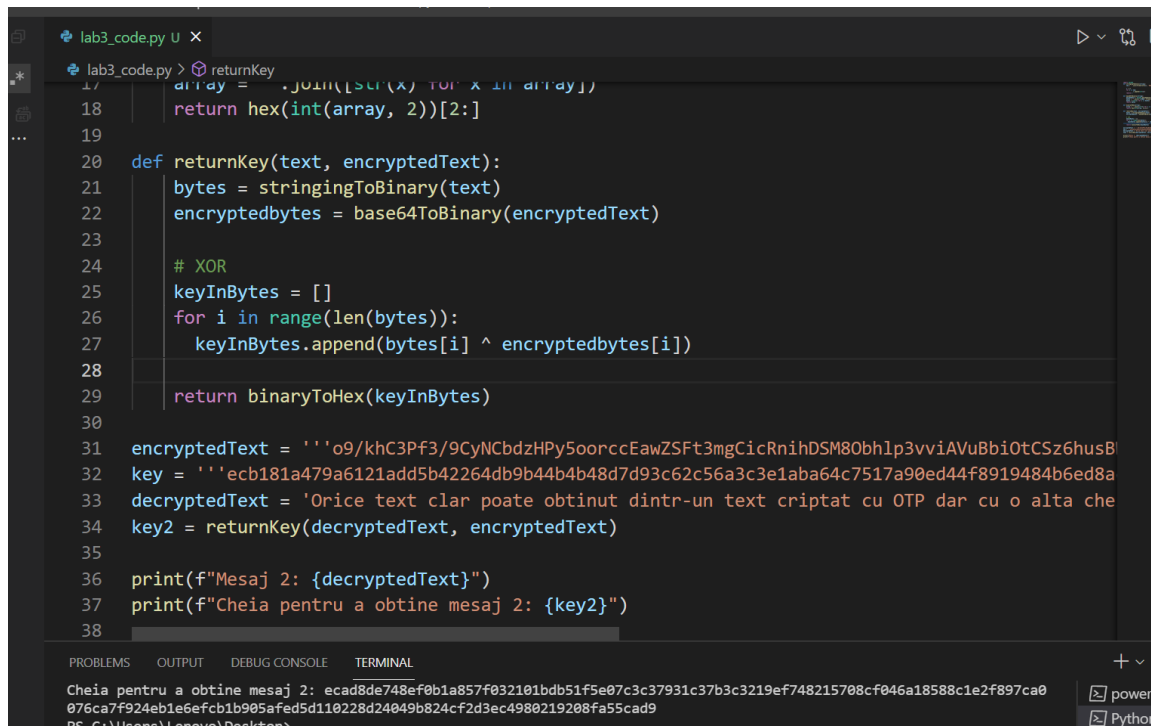
One Time Pad este un sistem de criptare perfect sigur daca este folosit corect.

Cheia noua am generat-o folosind codul:

```
lab3_code.py X
lab3_code.py > returnKey
1 import base64
2 def stringToBinary(string):
3     new = ''.join(format(ord(i), '08b') for i in string)
4
5     l = []
6     for x in new:
7         l.append(int(x))
8     return l
9
10 def base64ToBinary(string):
11     decodedText = base64.decodebytes(string)
12     bytes = "".join(["{:08b}".format(x) for x in decodedText])
13     bytes = [int(x) for x in bytes]
14     return bytes
15
16 def binaryToHex(array):
17     array = ''.join([str(x) for x in array])
18     return hex(int(array, 2))[2:]
19
20 def returnKey(text, encryptedText):
21     bytes = stringToBinary(text)
22     encryptedBytes = base64ToBinary(encryptedText)
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL

Cheia pentru a obtine mesaj 2: ecad8de748ef0b1a857f032101bdb51f5e07c3c37931c37b3c3219ef748215708cf046a18588c1e2f897ca0076ca7f924eb1e6efcb1b905afed5d110228d24049b824cf2d3ec4980219208fa55cad9



```

lab3_code.py U x
lab3_code.py > returnKey
17 array = .join([str(x) for x in array])
18 return hex(int(array, 2))[2:]
19
20 def returnKey(text, encryptedText):
21     bytes = stringToBinary(text)
22     encryptedbytes = base64ToBinary(encryptedText)
23
24     # XOR
25     keyInBytes = []
26     for i in range(len(bytes)):
27         keyInBytes.append(bytes[i] ^ encryptedbytes[i])
28
29     return binaryToHex(keyInBytes)
30
31 encryptedText = 'o9/khC3Pf3/9CyNCbdzHPy5oorccEawZSFt3mgCicRnihDSM80bhl3vviAVuBbiOtCSz6husB'
32 key = 'ecb181a479a6121add5b42264db9b44b4b48d7d93c62c56a3c3e1aba64c7517a90ed44f8919484b6ed8a'
33 decryptedText = 'Orice text clar poate obtinut dintr-un text criptat cu OTP dar cu o alta che'
34 key2 = returnKey(decryptedText, encryptedText)
35
36 print(f'Mesaj 2: {decryptedText}')
37 print(f'Cheia pentru a obtine mesaj 2: {key2}')
38
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
Cheia pentru a obtine mesaj 2: ecad8de748ef0b1a857f032101bdb51f5e07c3c37931c37b3c3219ef748215708cf046a18588c1e2f897ca0076ca7f924eb1e6efcb1b905afed5d110228d24049b824cf2d3ec4980219208fa55cad9
PS C:\Users\Lenovo\Desktop>

```

Rezultat:

ecad8de748ef0b1a857f032101bdb51f5e07c3c37931c37b3c3219ef748215708cf046a18588c1e2f897ca0076ca7f924eb1e6efcb1b905afed5d110228d24049b824cf2d3ec4980219208fa55cad9

Ce impact are refolosirea cheii?

Daca cineva are acces la un mesaj, atunci poate afla cheia, si reselectiv toate mesajele criptate cu aceeasi cheia:

2.

- Metoda substitutiei:

Caesar Cipher

Foloseste un alfabet circular de caractere, pe care merge cu un offset pentru a stabili relatii intr-un caracter original si cel criptat. Folosirea unei aranjari normale a alfabetului, ('A'..'Z', 'a'..'z') duce la spargerea destul de simpla a sistemului prin luarea valorilor pe rand si incercarea lor. Sistemul poate fi facut mai sigur prin rearanjarea alfabetului (65! de posibilitati de aranjare a alfabetului in ordine circulara).

Ca metoda de criptanaliza, ar fi ghicirea aranjarii alfabetului prin potrivirea cifrului cu un alfabet si un offset astfel incat sa se obtina cuvinte cu sens, utilizate des. Daca se va obtine un

Dima Oana-Teodora 341

aranjament care face sens, se incerca acea configuratie peste tot mesajul, si daca isi pastreaza sensul, inseamna ca este foarte arpoape de adevar.

Exemplu de functionare folosind site-ul : <https://www.dcode.fr/caesar-cipher>

mesaj = Ana are mere

cifru = dqd duh puh

The screenshot displays the dCode website's Caesar Cipher tools. On the left, a 'Results' panel shows the decoded message 'dqd duh puh' and a poster for 'EUFORIA Episod special' on HBO GO. The main area is divided into two sections: 'CAESAR CIPHER DECODER' and 'CAESAR ENCODER'. The decoder section has a text input field containing 'gFcgH EdhvdU', a shift value of 3, and a 'DECRYPT CAESAR CODE' button. The encoder section has a text input field containing 'ana are mere', the same shift value of 3, and an 'ENCRYPT BY CAESAR CODE' button. A sidebar on the right lists various cipher-related topics and links to similar pages like ROT Cipher, Shift Cipher, and Vigenere Cipher.

- Metoda transpozitiei:

Foloseste o permutare aleatorie de lungime k, si reordoneaza cate k caractere dupa ordinea permutarii.

Exemplu de functionare:

mesaj = permutarea

k = 5

key = (5, 3, 1, 2, 4)

permutarea

cifru = urpem artae

Metoda de spargere: gasirea combinatiilor de litere care au sens, calcularea permutarii prin care se obtin acele cuvinte, aplicarea ei pe intregul mesaj criptat si testare.

3. Analiza de frecventa

Rezolvarea exercitiului folosind codul de mai jos:

```

View Go Run Terminal Help lab3_ex3code.py - Desktop - Visual Studio Code

lab3_ex3code.py U lab3_ex3code.py U X
lab3_ex3code.py > ...
39     'U': 'V',
40     'V': 'Y',
41     'W': 'N',
42     'X': 'J',
43     'Y': 'F',
44     'Z': 'Z',
45 }
46
47 text = ''
48 for character in cipher:
49     if character in letters:
50         text += letters[character]
51     else:
52         text += character
53 print(text)
54
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
cipher = encrypt(msg, k)
File "c:\Users\Lenovo\Desktop\lab3_ex2code.py", line 15, in encrypt
TypeError: unsupported operand type(s) for +: 'NoneType' and 'int'
PS C:\Users\Lenovo\Desktop> & "D:/Python 3.9.6/python.exe" c:/Users/Lenovo/Desktop/lab3_ex2code.py
Mesaj original: Constantin
Mesaj criptat: Iutyztzot
Mesaj decritpat: Constantin
PS C:\Users\Lenovo\Desktop> & "D:/Python 3.9.6/python.exe" c:/Users/Lenovo/Desktop/lab3_ex3code.py
ALICE AND BOB ARE THE WORLDS MOST FAMOUS CRYPTOGRAPHIC COUPLE. SINCE
THEIR INVENTION IN 1978, THEY HAVE AT ONCE BEEN CALLED INSEPARABLE, AND
HAVE BEEN THE SUBJECT OF NUMEROUS DIVORCES, TRAVELS, AND TORMENTS. IN THE
0.6.64-bit 0.0.0 tabnine 1n 44. Col 14 Spaces:

```

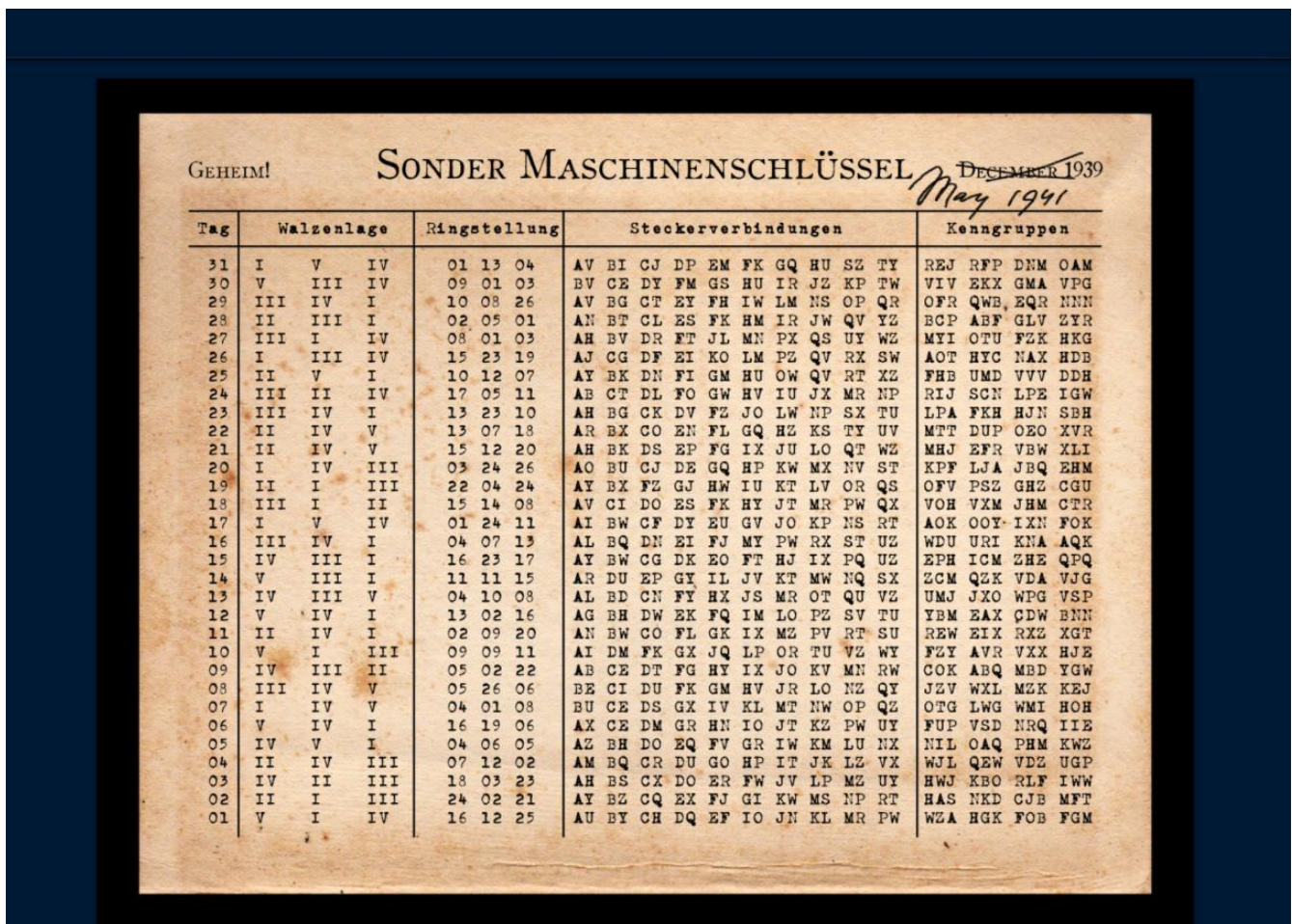
Rezultat:

ALICE AND BOB ARE THE WORLDS MOST FAMOUS CRYPTOGRAPHIC COUPLE. SINCE THEIR INVENTION IN 1978, THEY HAVE AT ONCE BEEN CALLED INSEPARABLE, AND HAVE BEEN THE SUBJECT OF NUMEROUS DIVORCES, TRAVELS, AND TORMENTS. IN THE ENSUING YEARS, OTHER CHARACTERS HAVE JOINED THEIR CRYPTOGRAPHIC FAMILY. THERES EVE, THE PASSIVE AND SUBMISSIVE EAVESDROPPER, MALLORY THE MALICIOUS ATTACKER, AND TRENT, TRUSTED BY ALL, JUST TO NAME A FEW. WHILE ALICE, BOB, AND THEIR EXTENDED FAMILY WERE ORIGINALLY USED TO EXPLAIN HOW PUBLIC KEY

CRYPTOGRAPHY WORKS, THEY HAVE SINCE BECOME WIDELY USED ACROSS OTHER SCIENCE AND ENGINEERING DOMAINS. THEIR INFLUENCE CONTINUES TO GROW OUTSIDE OF ACADEMIA AS WELL: ALICE AND BOB ARE NOW A PART OF GEEK LORE, AND SUBJECT TO NARRATIVES AND VISUAL DEPICTIONS THAT COMBINE PEDAGOGY WITH IN-JOKES, OFTEN REFLECTING OF THE SEXIST AND HETERONORMATIVE ENVIRONMENTS IN WHICH THEY WERE BORN AND CONTINUE TO BE USED. MORE THAN JUST THE WORLDS MOST FAMOUS CRYPTOGRAPHIC COUPLE, ALICE AND BOB HAVE BECOME AN ARCHETYPE OF DIGITAL EXCHANGE, AND A LENS THROUGH WHICH TO VIEW BROADER DIGITAL CULTURE. Q.DUPONT AND A.CATTAPAN CRYPTOCOUPLE

4.

Simulator folosit: <https://cryptii.com/>



Am ales ziua 25 :

2, 5, 1 – 10, 12, 7 – ay bk dn fi gm hu ow qv rt xz – DDH

Encoding

VIEW Text

OANA TEODORA DIMA

ENCODE DECODE

Enigma machine

MODEL
Enigma M3

REFLECTOR
UKW B

ROTOR 1	POSITION	RING
II	10 J	4 D
ROTOR 2	POSITION	RING
V	12 L	4 D
ROTOR 3	POSITION	RING
I	7 G	8 H

PLUGBOARD
ay bk dn fi gm hu ow qv rt xz

FOREIGN CHARS
Include Ignore

→ Encoded 17 chars

VIEW Text

avjue kvggd iqfgl

OANA DIMA -> avjue kvggd iqfgl

Decoding

VIEW Text

avjue kvggd iqfgl

ENCODE DECODE

Enigma machine

MODEL
Enigma M3

REFLECTOR
UKW B

ROTOR 1	POSITION	RING
II	10 J	4 D
ROTOR 2	POSITION	RING
V	12 L	4 D
ROTOR 3	POSITION	RING
I	7 G	8 H

PLUGBOARD
ay bk dn fi gm hu ow qv rt xz

FOREIGN CHARS
Include Ignore

→ Decoded 17 chars

VIEW Text

oanat eodor adima