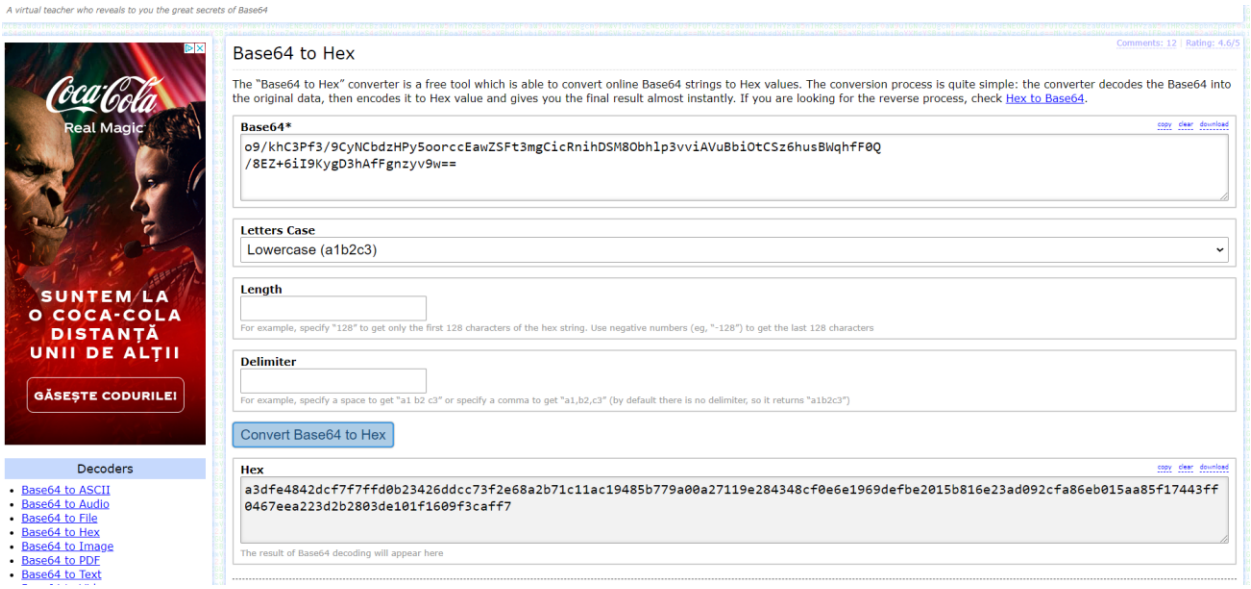
Dima Oana-Teodora 341

Securitatea Sistemelor Informatice – Laborator 3

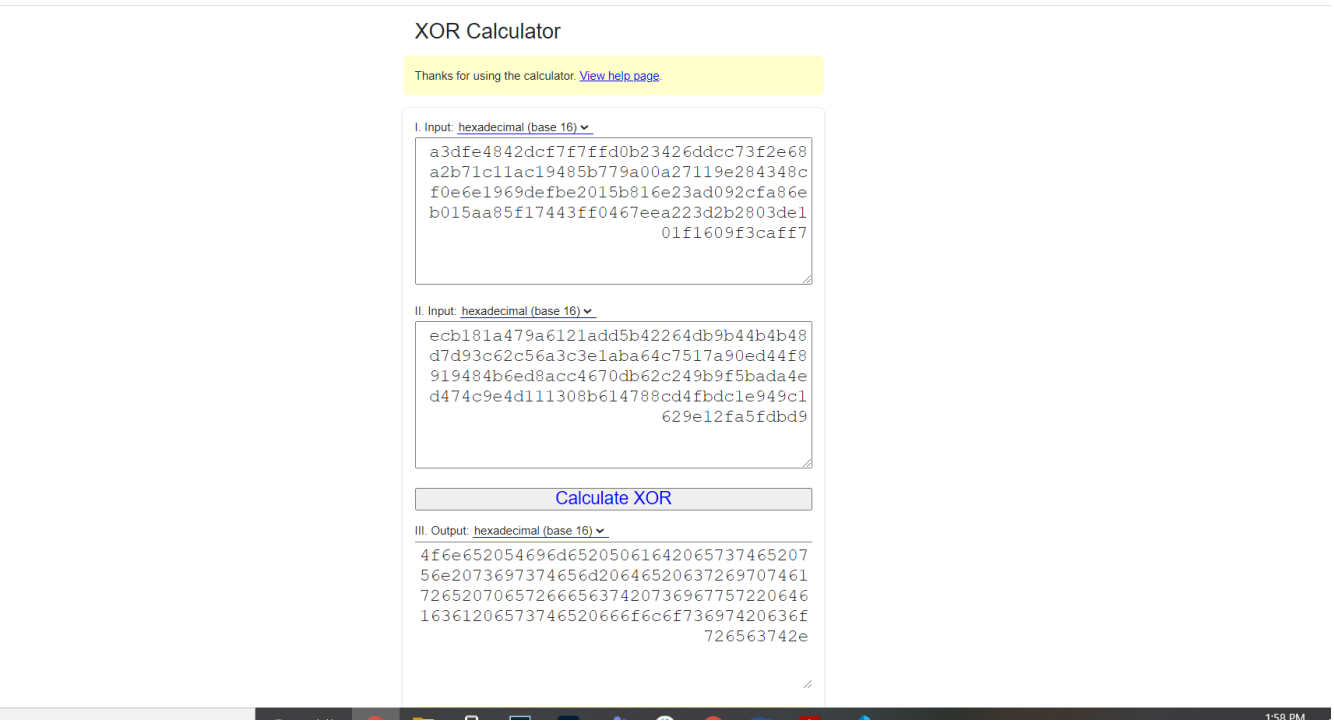
1.

Pasi inositi de print screen:

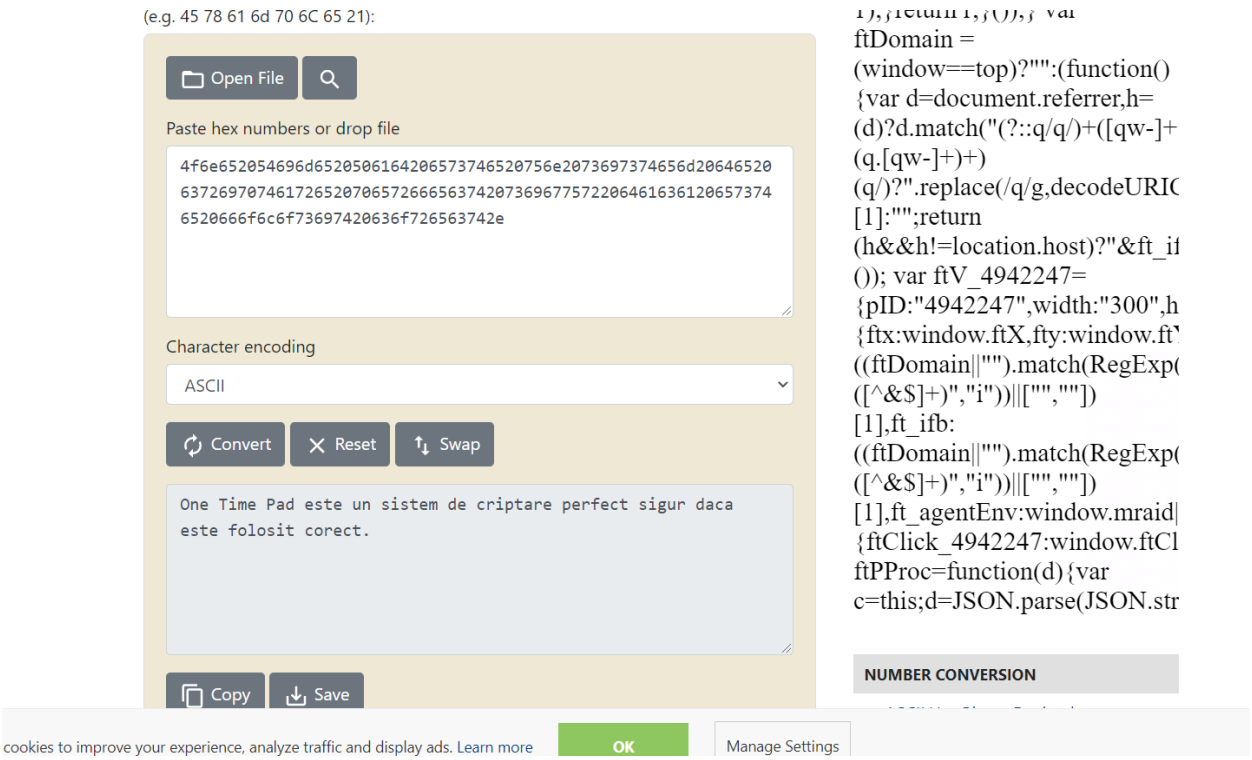
1) Transformarea mesajului din base64 in hex folosind: https://base64.guru/converter/decode/hex



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



3) Transformare rezultat XOR din hex in ASCIIfolosind:
https://www.rapidtables.com/convert/number/hex-to-ascii.html



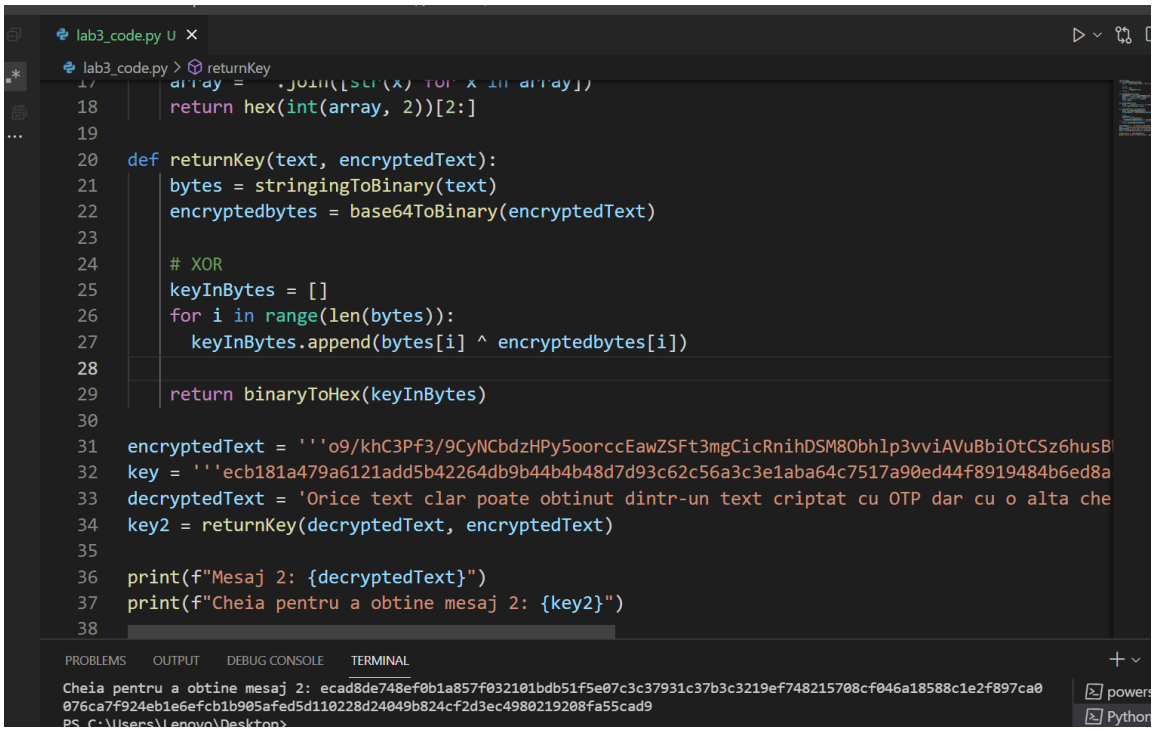
Rezultat - mesajul clar este:

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

Cheia noua am generat-o folosind codul:

```python
import base64
def stringingToBinary(string):
    new = ''.join(format(ord(i), '08b') for i in string)

    l = []
    for x in new:
        l.append(int(x))
    return l

def base64ToBinary(string):
    decodedText = base64.decodebytes(string)
    bytes = "".join(["{:08b}".format(x) for x in decodedText])
    bytes = [int(x) for x in bytes]
    return bytes

def binaryToHex(array):
    array = ''.join([str(x) for x in array])
    return hex(int(array, 2))[2:]

def returnKey(text, encryptedText):
    bytes = stringingToBinary(text)
```

```
Cheia pentru a obtine mesaj 2: ecad8de748ef0b1a857f032101bdb51f5e07c3c37931c37b3c3219ef748215708cf046a18588c1e2f897ca0
076ca7f924eb1e6efcb1b905afed5d110228d24049b824cf2d3ec4980219208fa55cad9
```



Rezultat:

ecad8de748ef0b1a857f032101bdb51f5e07c3c37931c37b3c3219ef748215708cf046a18588c1e2f897ca0076ca7f924eb1e6efcb1b905afed5d110228d24049b824cf2d3ec4980219208fa55cad9

Ce impact are refolosirea cheii?

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

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 incât sa se obtina cuvinte cu sens, utilizate des. Daca se va obtine un

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

Exemplu de functionare folosindsite-ul : https://www.dcode.fr/caesar-cipher

mesaj = Ana are mere

cifru = dqd duh phuh

- 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)

permu tarea

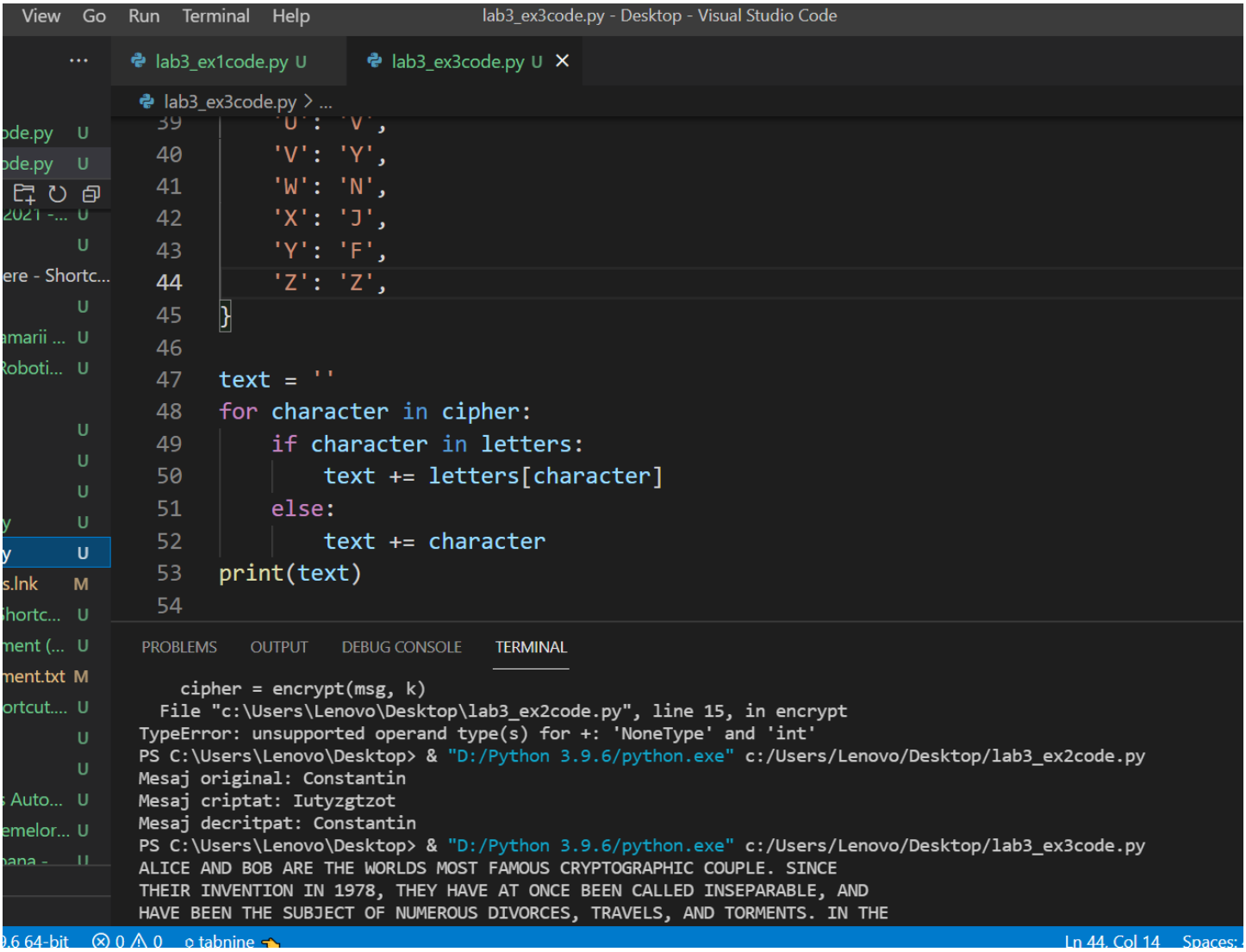
cifru = urpem artae

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.

Dima Oana-Teodora 341

3. Analiza de frecventa

Rezolvarea exercitiului folosind codul de mai jos:



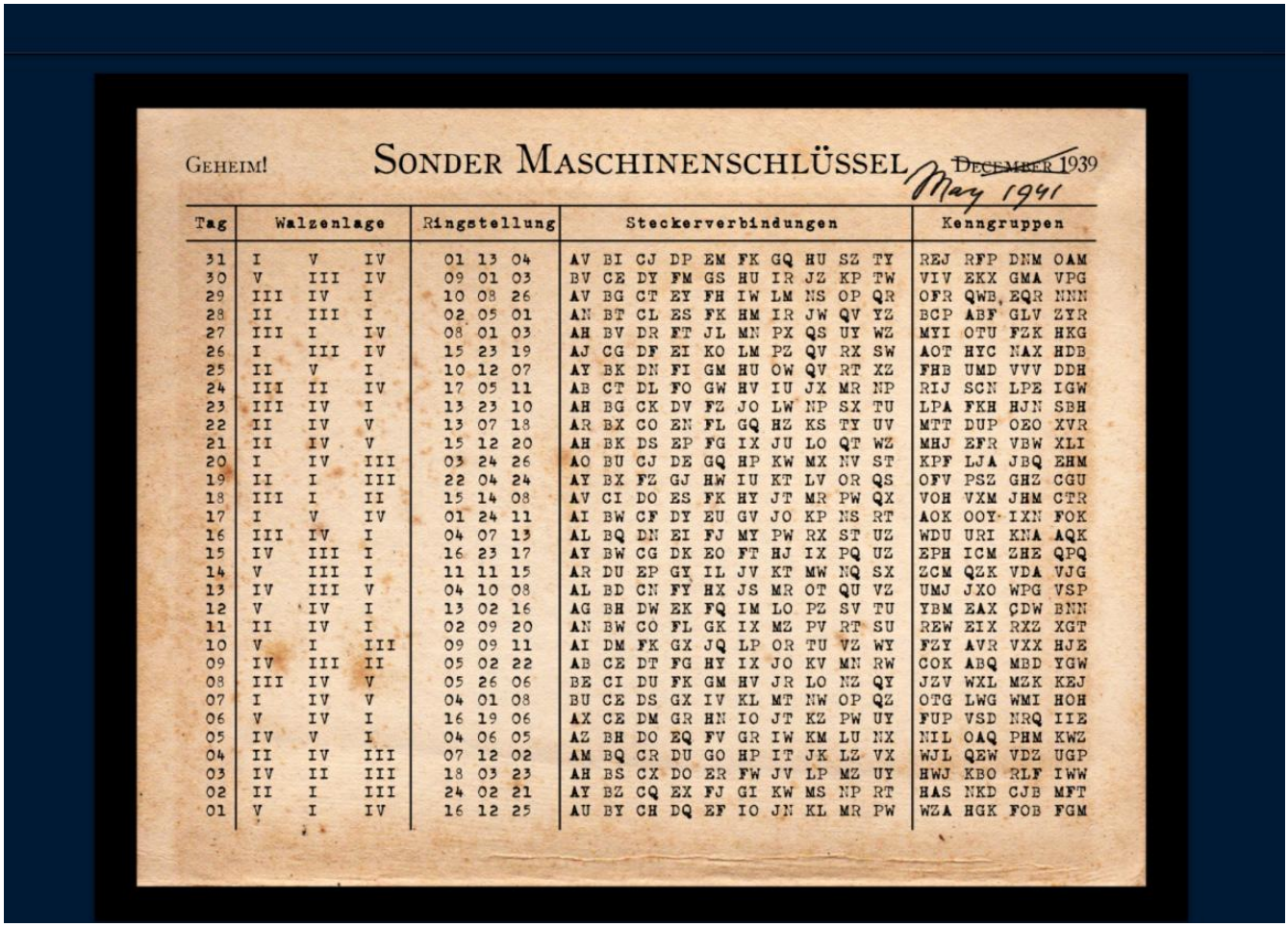
Rezultat:

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/



GEHEIM!

SONDER MASCHINENSCHLÜSSEL ~~DECEMBER~~ 1939 May 1941

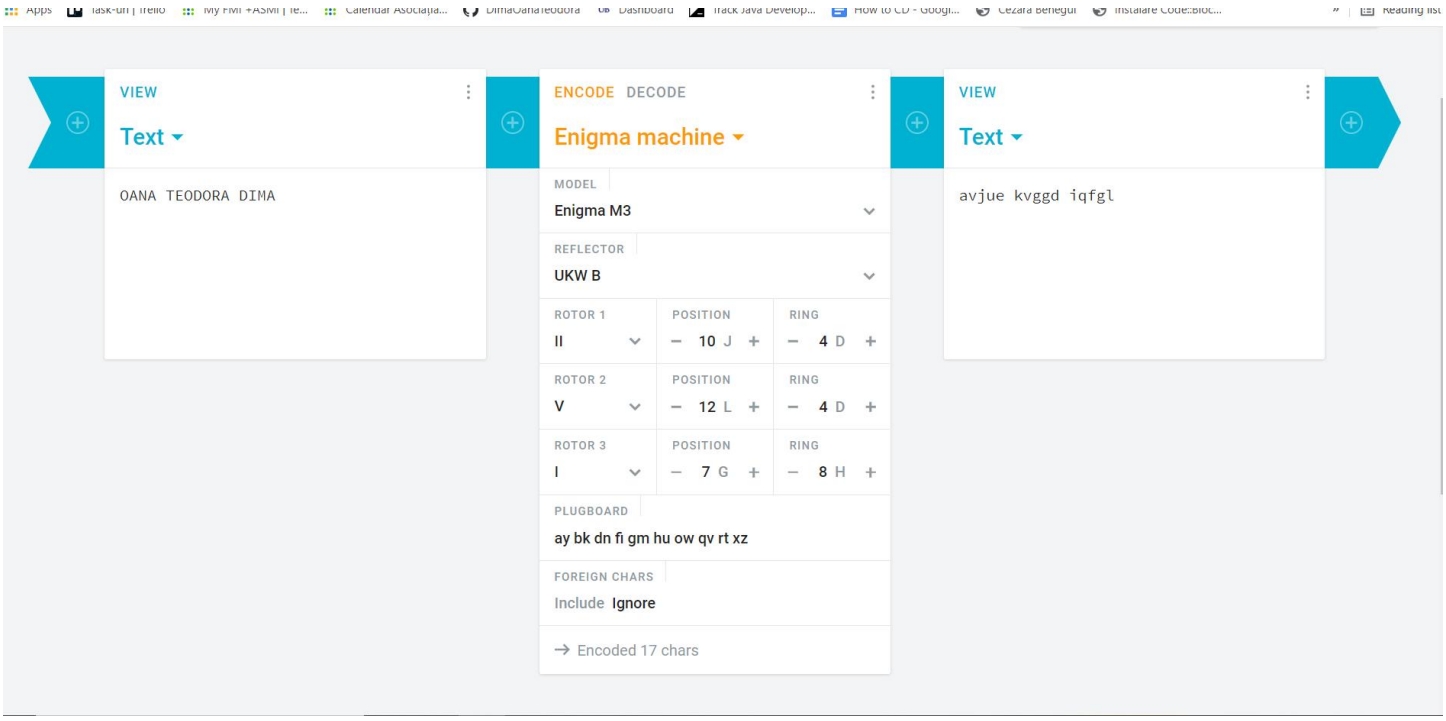
Tag	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
31	I	V	IV	01	13	04	AV	BI	CJ	DP	EM	FK	GQ	HU	SZ	TY	REJ	RFP	DNM	OAM
30	V	III	IV	09	01	03	BV	CE	DY	FM	GS	HU	IR	JZ	KP	TW	VIV	EKX	GMA	VPG
29	III	IV	I	10	08	26	AV	BG	CT	EY	FH	IW	LM	NS	OP	QR	OFR	QWB	EQR	NNN
28	II	III	I	02	05	01	AN	BT	CL	ES	FK	HM	IR	JW	QV	YZ	BCP	ABF	GLV	ZYR
27	III	I	IV	08	01	03	AH	BV	DR	FT	JL	MN	PX	QS	UY	WZ	MYI	OTU	FZK	HKG
26	I	III	IV	15	23	19	AJ	CG	DF	EI	KO	LM	PZ	QV	RX	SW	AOT	HYC	NAX	HDB
25	II	V	I	10	12	07	AY	BK	DN	FI	GM	HU	OW	QV	RT	XZ	FHB	UMD	VVV	DDH
24	III	II	IV	17	05	11	AB	CT	DL	FO	GW	HV	IU	JX	MR	NP	RIJ	SCN	LPE	IGW
23	III	IV	I	13	23	10	AH	BG	CK	DV	FZ	JO	LW	NP	SX	TU	LPA	FKH	HJN	SBH
22	II	IV	V	13	07	18	AR	BX	CO	EN	FL	GQ	HZ	KS	TY	UV	MTT	DUP	OEO	XVR
21	II	IV	V	15	12	20	AH	BK	DS	EP	FG	IX	JU	LO	QT	WZ	MHJ	EFR	VBW	XLI
20	I	IV	III	03	24	26	AO	BU	CJ	DE	GQ	HP	KW	MX	NV	ST	KPF	LJA	JBQ	EHM
19	II	I	III	22	04	24	AY	BX	FZ	GJ	HW	IU	KT	LV	OR	QS	OFV	PSZ	GHZ	CGU
18	III	I	II	15	14	08	AV	CI	DO	ES	FK	HY	JT	MR	PW	QX	VOH	VXM	JHM	CTR
17	I	V	IV	01	24	11	AI	BW	CF	DY	EU	GV	JO	KP	NS	RT	AOK	OOY	IXN	FOK
16	III	IV	I	04	07	13	AL	BQ	DN	EI	FJ	MY	PW	RX	ST	UZ	WDU	URI	KNA	AQK
15	IV	III	I	16	23	17	AY	BW	CG	DK	EO	FT	HJ	IX	PQ	UZ	EPH	ICM	ZHE	QPQ
14	V	III	I	11	11	15	AR	DU	EP	GY	IL	JV	KT	MW	NQ	SX	ZCM	QZK	VDA	VJG
13	IV	III	V	04	10	08	AL	BD	CN	FY	HX	JS	MR	OT	QU	VZ	UMJ	JXO	WPG	VSP
12	V	IV	I	13	02	16	AG	BH	DW	EK	FQ	IM	LO	PZ	SV	TU	YBM	EAX	CDW	BNN
11	II	IV	I	02	09	20	AN	BW	CO	FL	GK	IX	MZ	PV	RT	SU	REW	EIX	RXZ	XGT
10	V	I	III	09	09	11	AI	DM	FK	GX	JQ	LP	OR	TU	VZ	WY	FZY	AVR	VXX	HJE
09	IV	III	II	05	02	22	AB	CE	DT	FG	HY	IX	JO	KV	MN	RW	COK	ABQ	MBD	YGW
08	III	IV	V	05	26	06	BE	CI	DU	FK	GM	HV	JR	LO	NZ	QY	JZV	WXL	MZK	KEJ
07	I	IV	V	04	01	08	BU	CE	DS	GX	IV	KL	MT	NW	OP	QZ	OTG	LWG	WMI	HOH
06	V	IV	I	16	19	06	AX	CE	DM	GR	HN	IO	JT	KZ	PW	UY	FUP	VSD	NRQ	IIE
05	IV	V	I	04	06	05	AZ	BH	DO	EQ	FV	GR	IW	KM	LU	NX	NIL	OAQ	PHM	KWZ
04	II	IV	III	07	12	02	AM	BQ	CR	DU	GO	HP	IT	JK	LZ	VX	WJL	QEW	VDZ	UGP
03	IV	II	III	18	03	23	AH	BS	CX	DO	ER	FW	JV	LP	MZ	UY	HWJ	KBO	RLF	IWW
02	II	I	III	24	02	21	AY	BZ	CQ	EX	FJ	GI	KW	MS	NP	RT	HAS	NKD	CJB	MFT
01	V	I	IV	16	12	25	AU	BY	CH	DQ	EF	IO	JN	KL	MR	PW	WZA	HGK	FOB	FGM

Dima Oana-Teodora 341

Am ales ziua 25 :

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

Encoding



OANA DIMA -> avjue kvggd iqfgl

Decoding