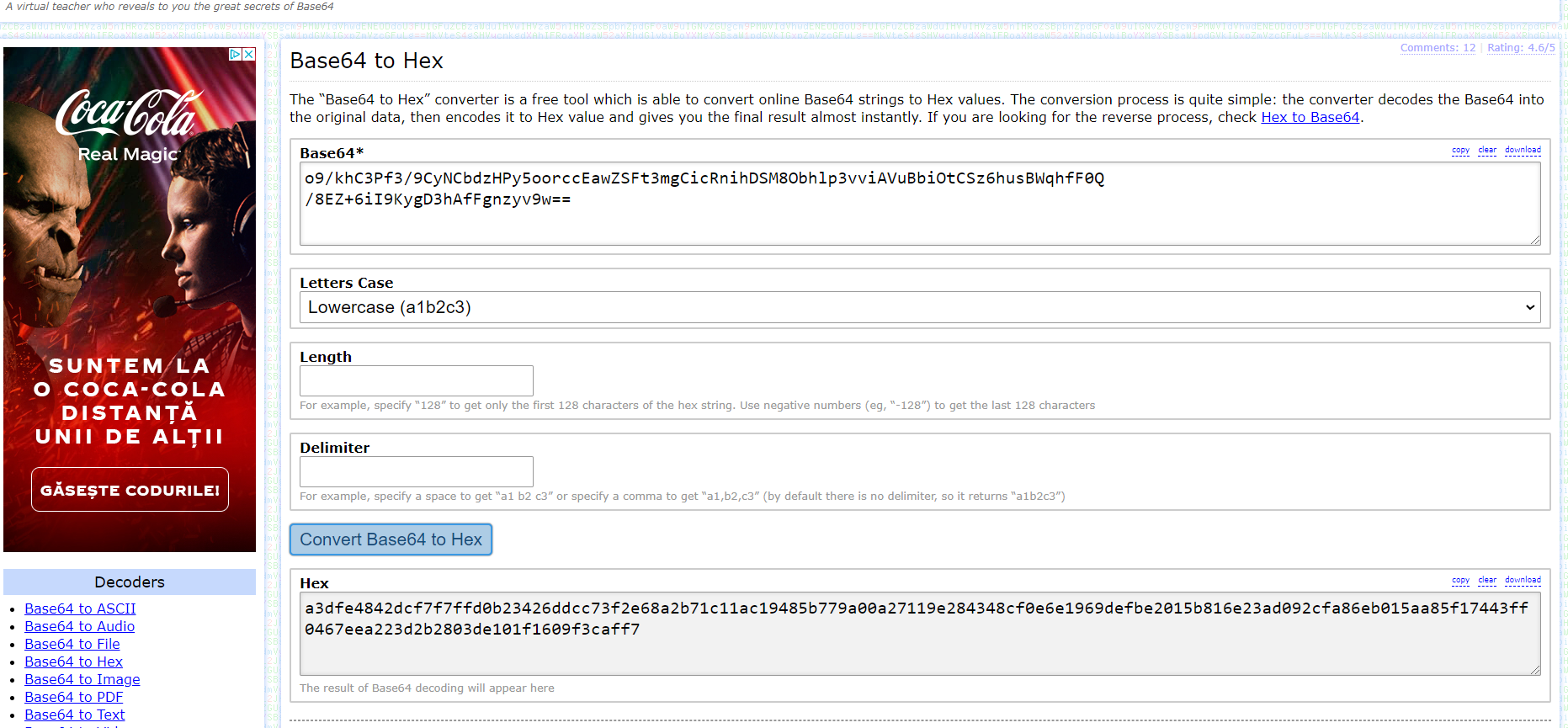
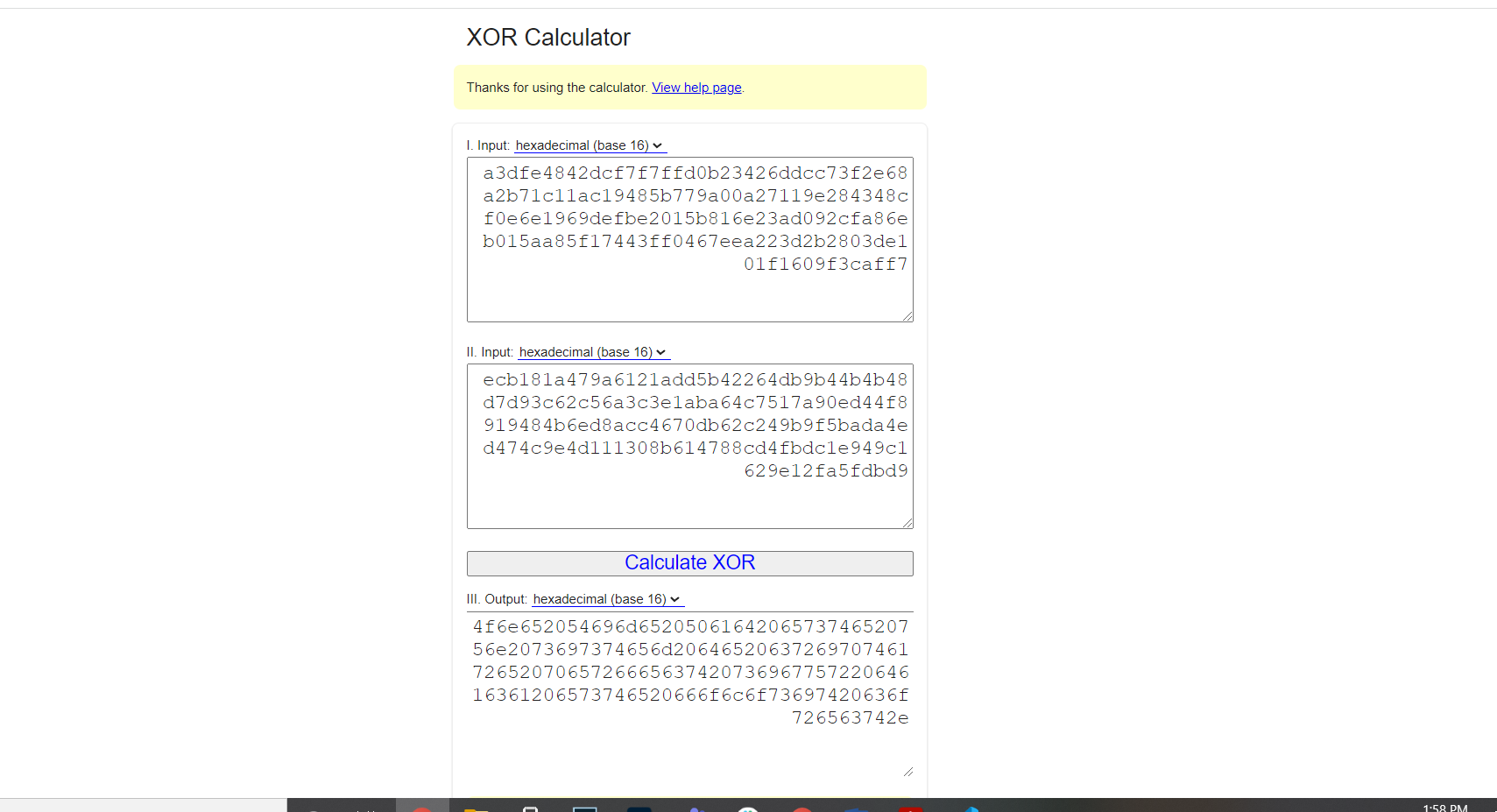
Securitatea Sistemelor Informatice – Laborator 3

1.

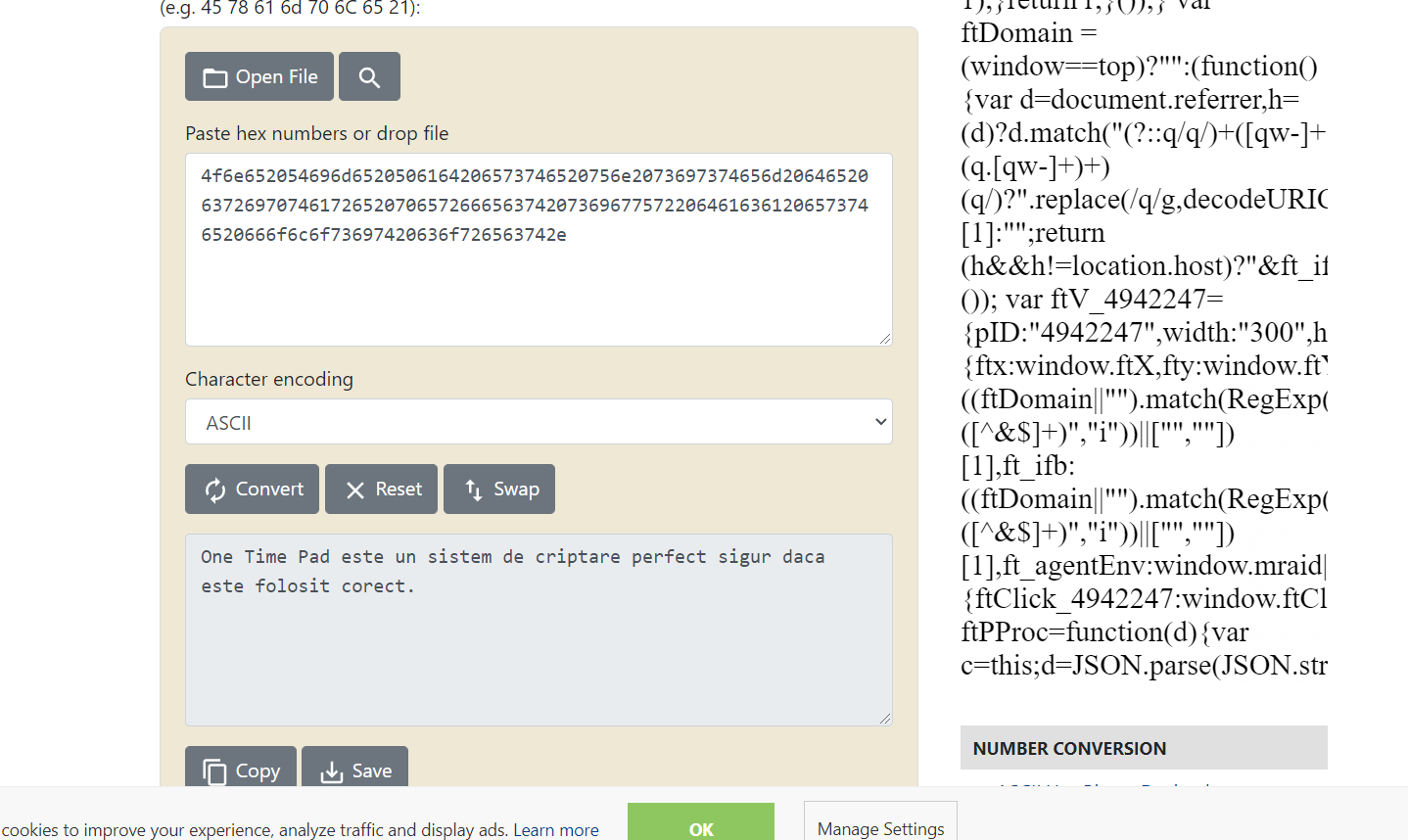
Pasi inositi de print screen:

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



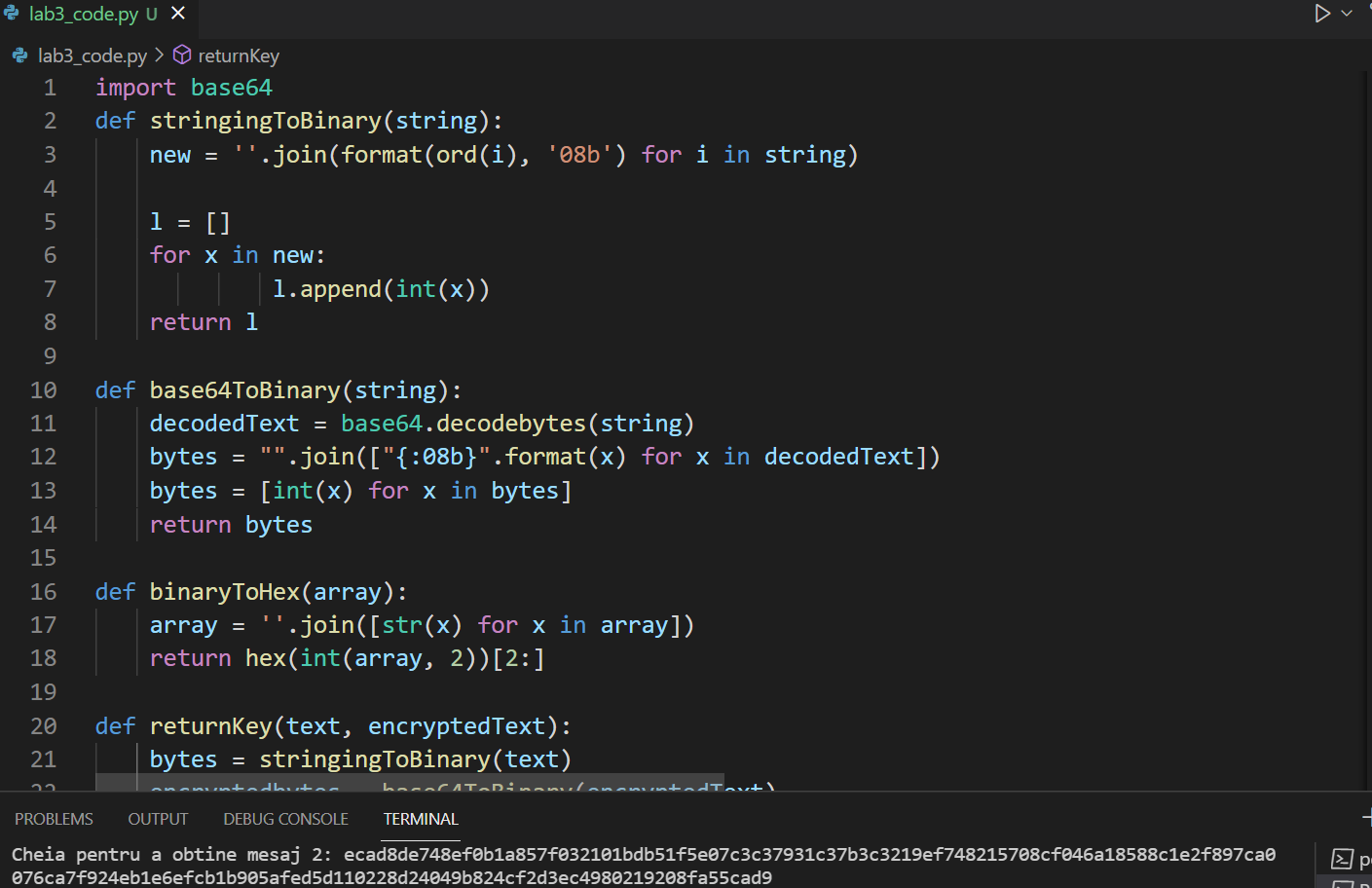
2) XOR intre textul transformat si cheie (XOR hex cu hex) folosind: [http://xor.pw/#](http://xor.pw/)

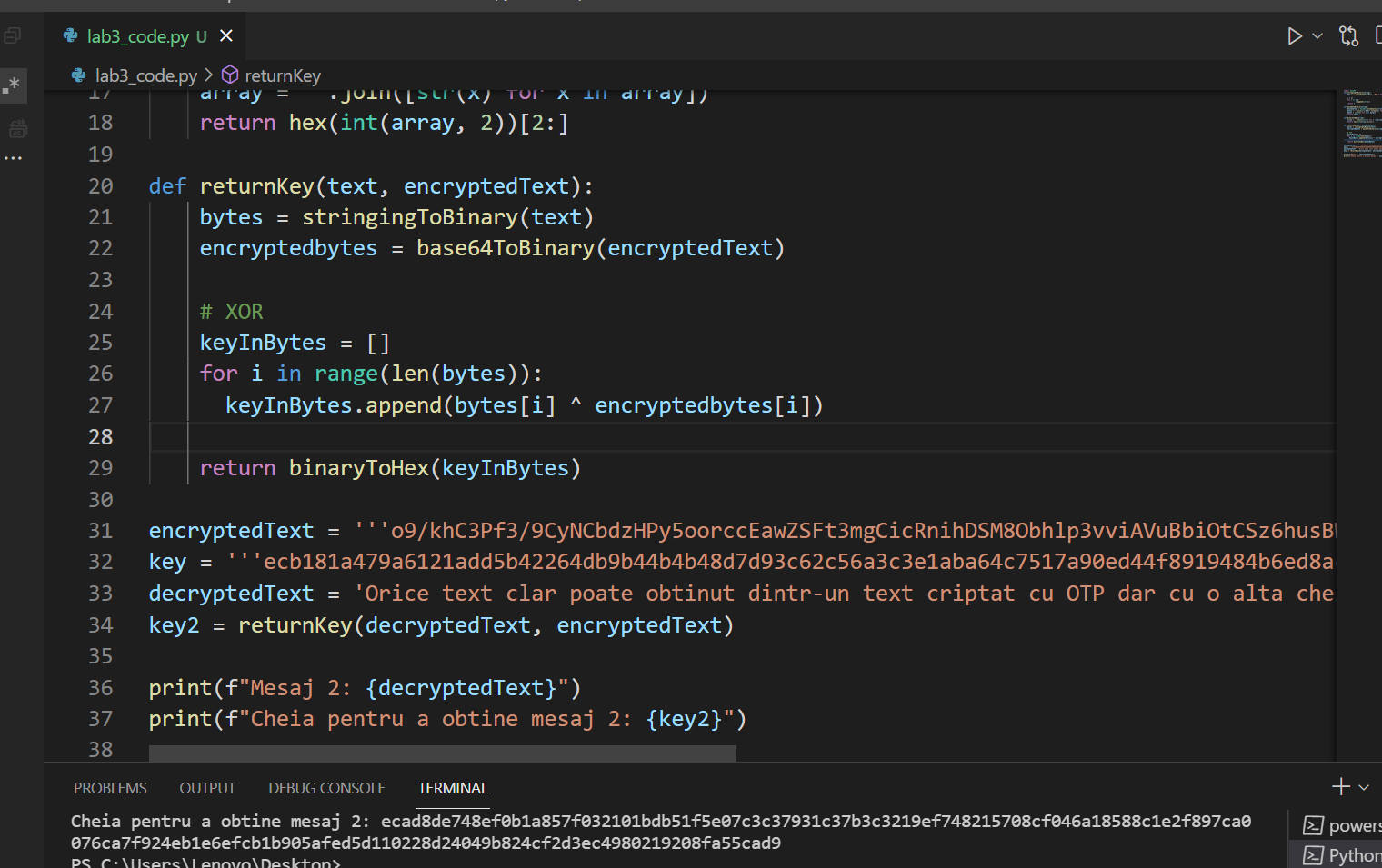
3) Transformare rezultat XOR din hex in ASCIIfolosind: <https://www.rapidtables.com/convert/number/hex-to-ascii.html>



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:



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)

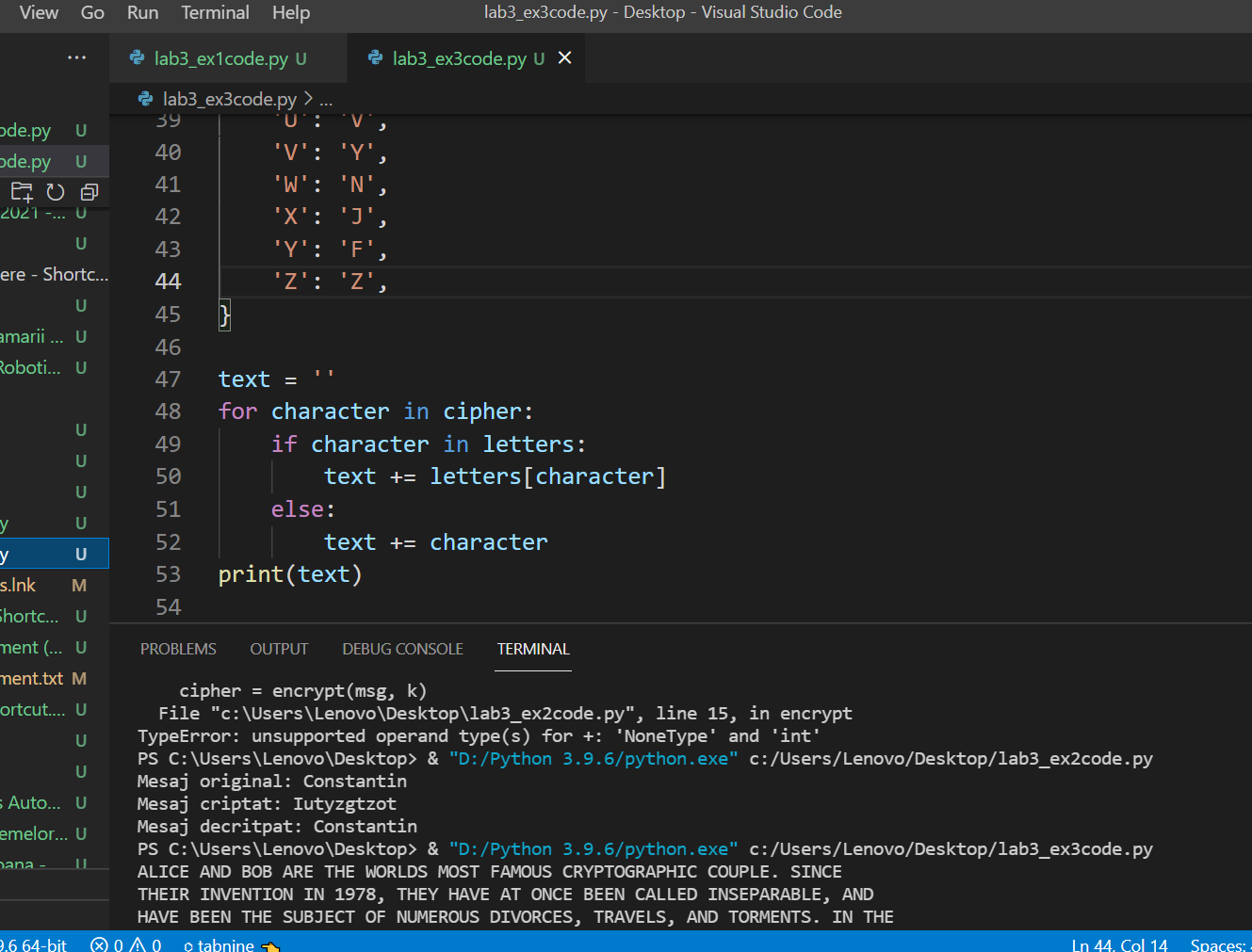
permu tarea

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.

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

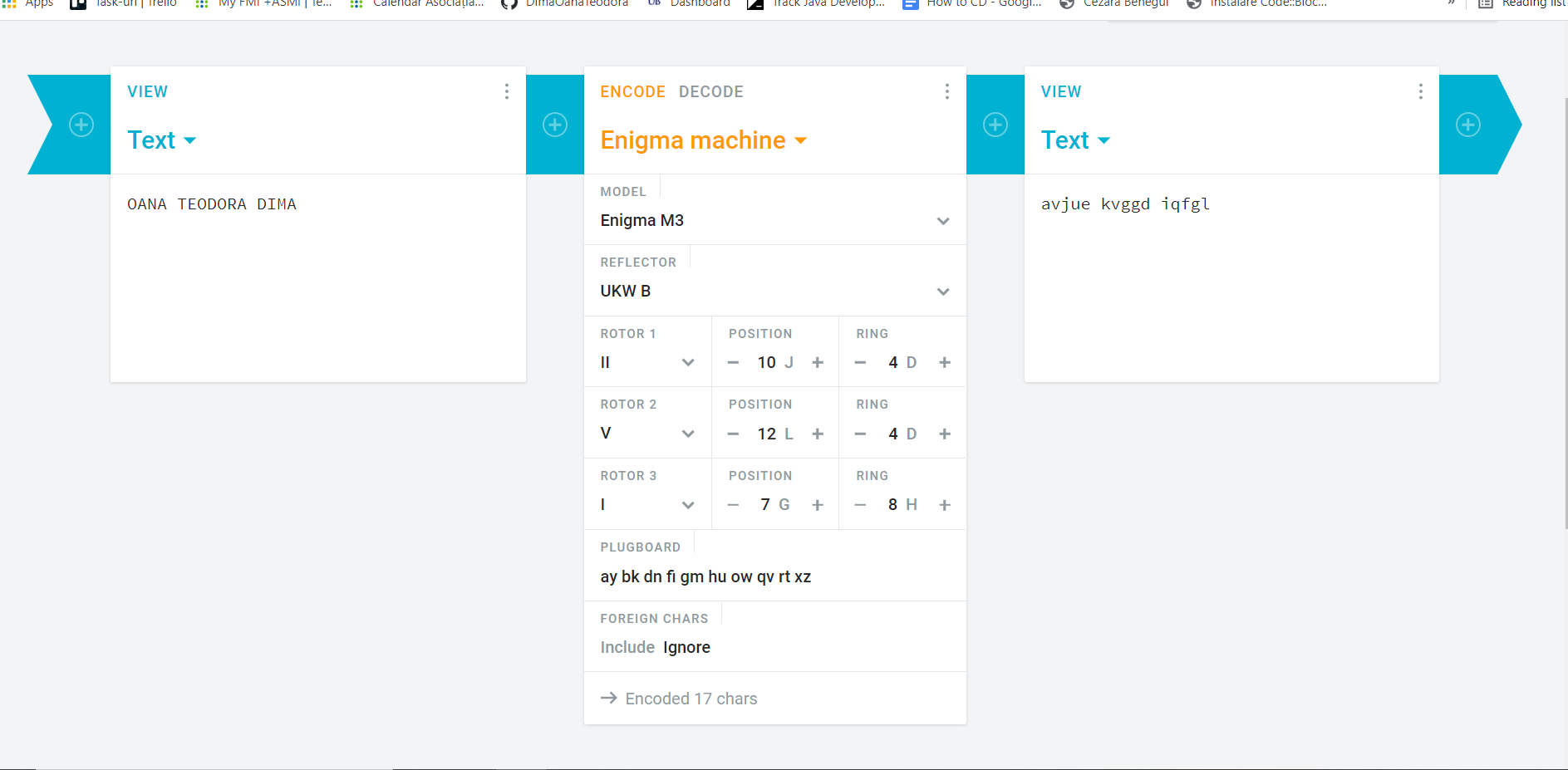
BROADER DIGITAL CULTURE. Q.DUPONT AND A.CATTAPAN CRYPTOCOUPLE

4.

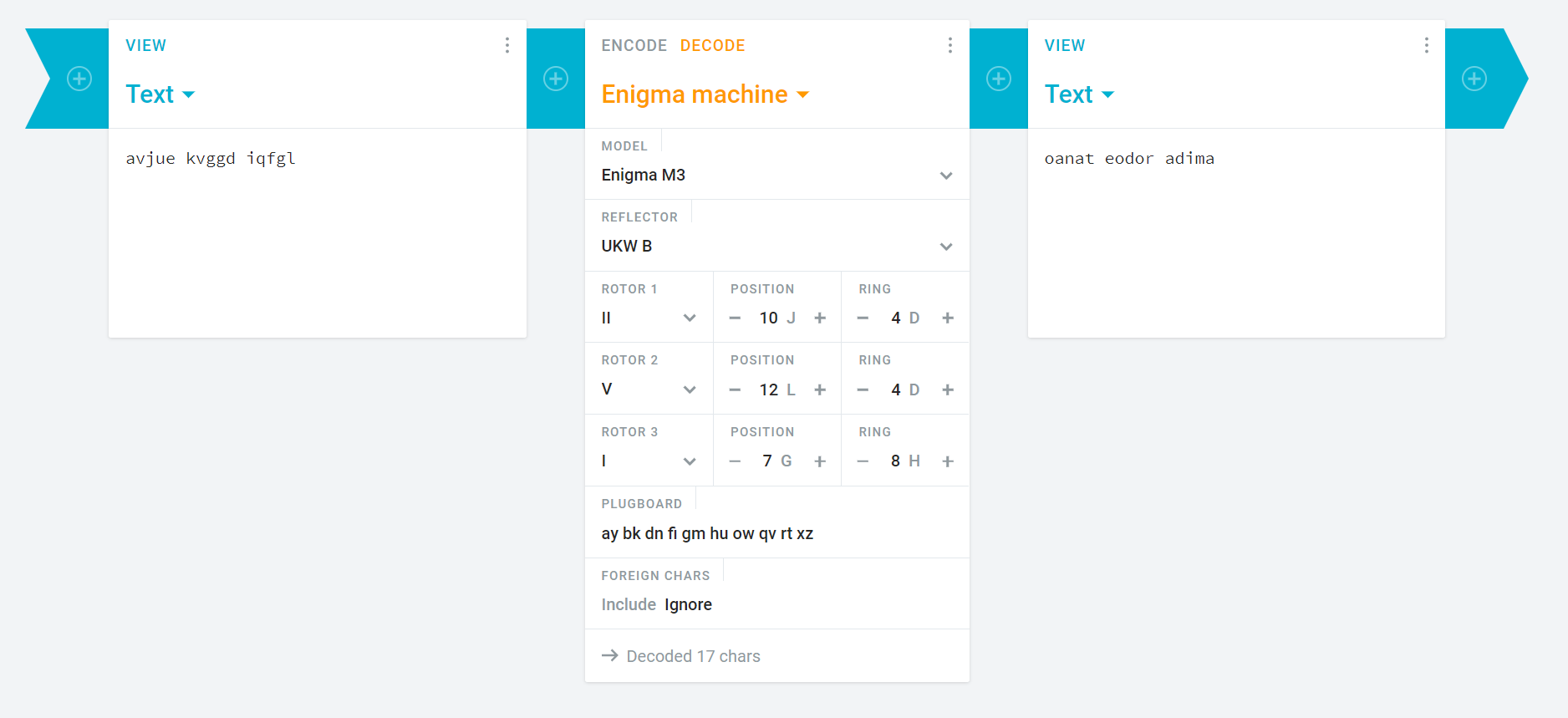
Simulator folosit: <https://cryptii.com/>

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