Tudorache Alexandru-Theodor

Grupa 342

Laborator 3

Securitatea Sistemelor Informatice

1.

*1.*

Mesajul

*o9/khC3Pf3/9CyNCbdzHPy5oorccEawZSFt3mgCicRnihDSM8Obhlp3vviAVuBbiOtCSz6husBWqhfF0Q/8EZ+6iI9KygD3hAfFgnzyv9w==*

transformat in format hex este:

*a3dfe4842dcf7f7ffd0b23426ddcc73f2e68a2b71c11ac19485b779a00a27119e284348cf0e6e1969defbe2015b816e23ad092cfa86eb015aa85f17443ff0467eea223d2b2803de101f1609f3caff7*

Pentru a transforma am folosit <https://base64.guru/converter/decode/hex>.

Mesajului obtinut

*a3dfe4842dcf7f7ffd0b23426ddcc73f2e68a2b71c11ac19485b779a00a27119e284348cf0e6e1969defbe2015b816e23ad092cfa86eb015aa85f17443ff0467eea223d2b2803de101f1609f3caff7*

ii este aplicata operatia de XOR cu cheia

*ecb181a479a6121add5b42264db9b44b4b48d7d93c62c56a3c3e1aba64c7517a90ed44f8919484b6ed8acc4670db62c249b9f5bada4ed474c9e4d111308b614788cd4fbdc1e949c1629e12fa5fdbd9*

si se obtine

*4f6e652054696d6520506164206573746520756e2073697374656d20646520637269707461726520706572666563742073696775722064616361206573746520666f6c6f73697420636f726563742e*

Pentru a transforma am folosit <http://xor.pw>.

Mesajul obtinut

*4f6e652054696d6520506164206573746520756e2073697374656d20646520637269707461726520706572666563742073696775722064616361206573746520666f6c6f73697420636f726563742e*

este transformat din format hex in string:

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

Acesta este mesajul clar primit.

Pentru a transforma am folosit <https://string-functions.com/hex-string.aspx>.

*2.*

Da, exista o astfel de cheie.

Pentru a o gasi trebuie parcursi urmatorii pasi:

Transformam mesajul clar in format hex.

*Orice text clar poate obtinut dintr-un text criptat cu OTP dar cu o alta cheie.*

in format hex este:

*4f72696365207465787420636c617220706f617465206f6274696e75742064696e74722d756e20746578742063726970746174206375204f545020646172206375206f20616c74612063686569652e20*

Pentru a transforma am folosit <https://string-functions.com/string-hex.aspx>.

Mesajului obtinut

*4f72696365207465787420636c617220706f617465206f6274696e75742064696e74722d756e20746578742063726970746174206375204f545020646172206375206f20616c74612063686569652e*

ii este aplicata operatia de XOR cu mesajul initial in format hex

*a3dfe4842dcf7f7ffd0b23426ddcc73f2e68a2b71c11ac19485b779a00a27119e284348cf0e6e1969defbe2015b816e23ad092cfa86eb015aa85f17443ff0467eea223d2b2803de101f1609f3caff7*

si se obtine:

*ecad8de748ef0b1a857f032101bdb51f5e07c3c37931c37b3c3219ef748215708cf046a18588c1e2f897ca0076ca7f924eb1e6efcb1b905afed5d110228d24049b824cf2d3ec4980219208fa55cad9*

Aceasta este cheia ceruta.

Pentru a transforma am folosit <http://xor.pw>

*3.*

Daca este refolosita aceeasi cheie, integritatea acesteia scade, intrucat sansele atacatorului de a o ghici cresc.

2.

*1. Cifrul lui Cezar*

Pentru criptare am ales mesajul:

*Laborator trei SSI*

Folosind Cifrul lui Cezar cu o shiftare de 6 litere, se obtine:

*Rghuxgzux zxko YYO*

Pentru decriptare am ales mesajul:

*Denybkmro Droynyb*

Folosind Cifrul lui Cezar cu o shiftare de 10 litere, se obtine:

*Tudorache Theodor*

Pentru transformari am folosit <https://cryptii.com/pipes/caesar-cipher>.

*2. Rail Fence Cipher*

Pentru criptare am ales mesajul:

*my cup of tea*

Folosind Rail Fence Cipher, se obtine:

*MUFAYCPO E T*

Pentru decriptare am ales mesajul:

*QITULT IEAYM*

Folosind Rail Fence Cipher, se obtine:

*quality time*

Pentru transformari am folosit <https://crypto.interactive-maths.com/rail-fence-cipher.html>.

3.

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

Pentru transformare am folosit:

<http://scottbryce.com/cryptograms/> si <https://www.dcode.fr/monoalphabetic-substitution>.

4.

*1.*

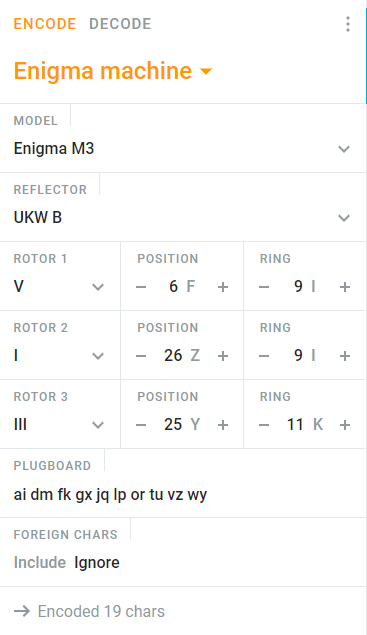
Am ales ziua 10 din <https://operationturing.tumblr.com/image/143702293214>:



*2.*

Am folosit simulatorul <https://cryptii.com/pipes/enigma-machine>.

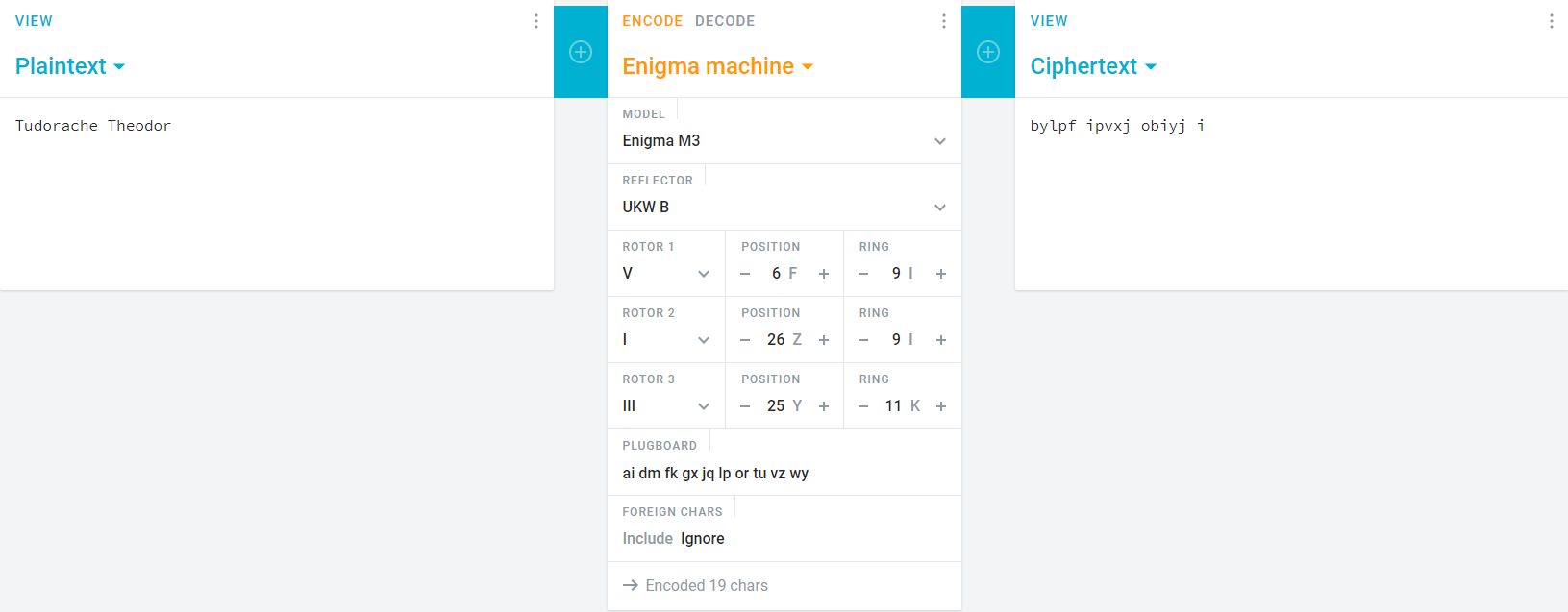
Am facut setarile aferente zilei (cu pozitia initiala a rotoareler FZY):



*3.*

Rezultatul obtinut:

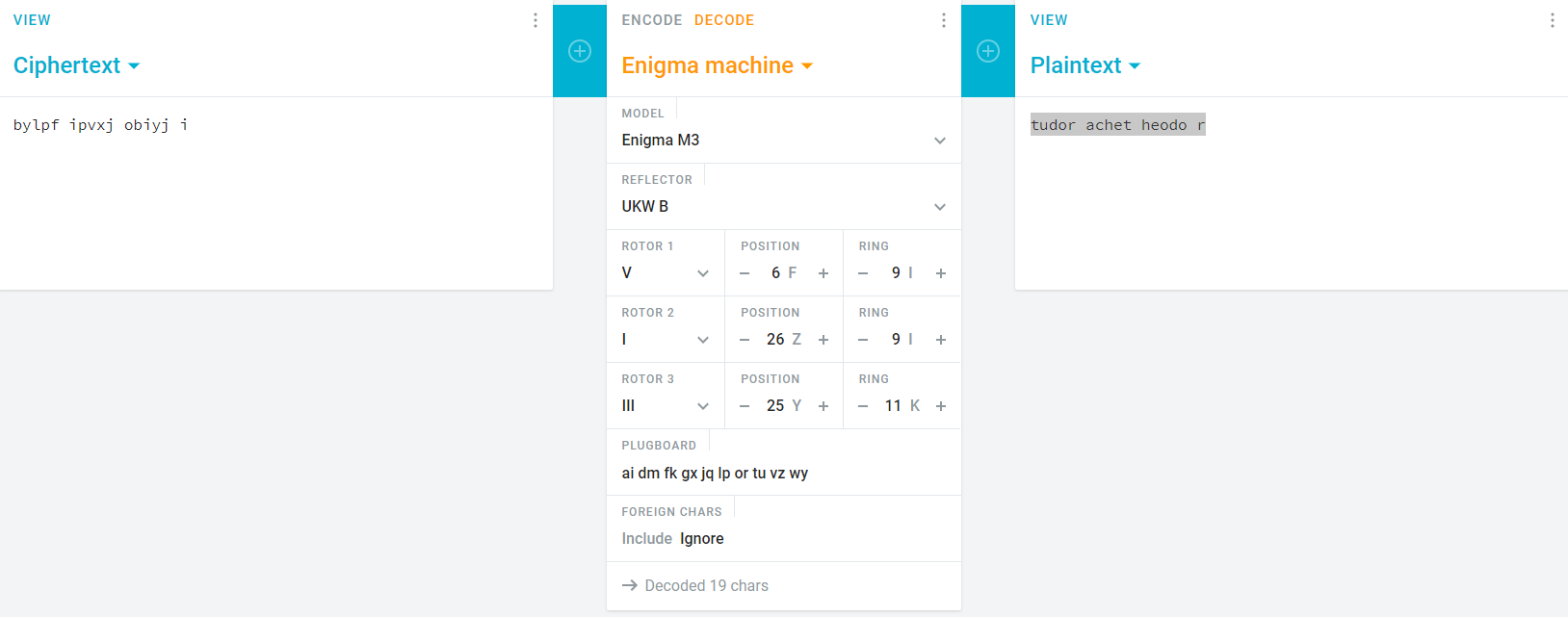
*bylpf ipvxj obiyj i*



*4.*

Rezultatul obtinut:

*tudor achet heodo r*



*5.*

Exemplu de text criptat care nu ar putea fi criptatea numelui:

*tomod iphej aoedk l*

Literele subliniate sunt aceleasi cu cele din nume, ceea ce este imposibil, intrucat Enigma Machine nu cripteaza niciodata o litera in ea insasi.