Lab3

joi, 26 octombrie 2023 15:50

ex.1

Base64: o9/khC3Pf3/9CyNCbdzHPy5oorccEawZSFt3mgCicRnihDSM8Obhlp3vviAVuBbiOtCSz6hu
sBWqhfF0Q/8EZ+6iI9KygD3hAfFgnzyv9w==

transformam in binar:

10100011 11011111 11100100 10000100 00101101 11001111 01111111 01111111 11111101
00001011 00100011 01000010 01101101 11011100 11000111 00111111 00101110 01101000
10100010 10110111 00011100 00010001 10101100 00011001 01001000 01011011 01110111
10011010 00000000 10100010 01110001 00011001 11100010 10000100 00110100 10001100
11110000 11100110 11100001 10010110 10011101 11101111 10111110 00100000 00010101
10111000 00010110 11100010 00111010 11010000 10010010 11001111 10101000 01101110
10110000 00010101 10101010 10000101 11110001 01110100 01000011 11111111 00000100
01100111 11101110 10100010 00100011 11010010 10110010 10000000 00111101 11100001
00000001 11110001 01100000 10011111 00111100 10101111 11110111
decriptam cheia din hex in binar:
Hex: ecb181a479a6121add5b42264db9b44b4b48d7d93c62c56a3c3e1aba64c7517a90ed44f891
9484b6ed8acc4670db62c249b9f5bada4ed474c9e4d111308b614788cd4fbdc1e949c1629e12fa5
fdbd9

in binar:

11101100101100011000000110100100011110011010011000010010000110101101110101011
10110100001000100110010011011011100110110100010010110100101101001000110101111
11011001001111000110001011000101011010100011110000111110000110101011101001100
01001100011101010001011110101001000011101101010001001111100010010001100101000
10000100101101101110110110001010110011000100011001110000110110110110001011000
00100100100110111001111101011011101011011010010011101101010001110100110010011
11100100110100010001000100110000100010110110000101000111100010001100110101000
11111011110111000001111010010100100111000001011000101001111000010010111110100
0101111111011011110110 01
Aplicam XOR intre cele doua val binare:

10011110110111001100101001000000101010001101001011011010110010100100000001010
00001100000101100100001000000110010101110011011101000110010100100000011101010
11011100010000001110011011010010111001101110100011001010110110100100000001100
10001100101001000000110001101110010011010010111000001110100011000010111001000
11001010010000001110000011001010111001001100110011001010110001101110100000100
00001110011011010010110011101110101011100100010000001100100011000010110001100
11000010010000001100101011100110111010001100101001000000110011001101111011010
10001101111011100110110100101110100001000000110001101101111011100100110010100
1100011011101000010111 0

si convertim in ASCII:

String rezultat:

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

1.2
ca sa aflam otp am luat cheia cu mesajul, le am transf in binar si am apl xor si am convertit in ASCII
acum facem invers

transf textului final (orice …) in binar:
01001111 01110010 01101001 01100011 01100101 00100000 01110100 01100101 01111000
01110100 00100000 01100011 01101100 01100001 01110010 00100000 01110000 01101111
01100001 01110100 01100101 00100000 01101111 01100010 01110100 01101001 01101110
01110101 01110100 00100000 01100100 01101001 01101110 01110100 01110010 00101101
01110101 01101110 00100000 01110100 01100101 01111000 01110100 00100000 01100011
01110010 01101001 01110000 01110100 01100001 01110100 00100000 01100011 01110101
00100000 01001111 01010100 01010000 00100000 01100100 01100001 01110010 00100000
01100011 01110101 00100000 01101111 00100000 01100001 01101100 01110100 01100001
00100000 01100011 01101000 01100101 01101001 01100101 00101110

facem xor si descoperim cheia biinara :

10100011110111111110010010000100001011011100111101111111011111111111111010000
10110010001101000010011011011101110011000111001111110010111001101000101000010
10110111000111000001000110101100000110010100100001011011011101111001101000000
00001010001001110001000110011110001010000100001101001000110011110000111001100
11100001100101101001110111011110111110111110001000000001010110111000000101101110
00100011101011010000100100101100111110101000011011101011000000001010110101010
10000101111100010111010001000011111111110000010001100111111011101010001000100
00111101001010110010100000000011110111100001000000011111000101100000100111111
00111100101011111111110111

hex: A3DFE4842DCF7F7FFD0B23426DDCC73F2E68A2B71C11AC19485B779A00A27119E284348
CF0E6E1969DEFBE2015B816E23AD092CFA86EB015AA85F17443FF0467EEA223D2B2803DE101
F1609F3CAFF7

1.3
refolosirea cheii reduce siguranta oferita de aceasta, deoarece atacatorul a mai intalnit o o data deci posibil sa o cunoasca

ex.2

1. Criptare prin substituție (Cifrul Vigenère):

- Criptare: Criptul Vigenère este un sistem de criptare care implică o cheie secretă, care este o șir de litere. Pentru a cripta un text clar, fiecare literă a textului clar este înlocuită cu o literă corespunzătoare din cheie. Dacă cheia este mai scurtă decât textul clar, ea se repetă pentru a acoperi întregul text clar.
- Exemplu: Text clar - "HELLOWORLD", Cheie - "KEY". Criptare: H + K = O, E + E = X, L + Y = B, etc. Astfel, textul clar devine "OXHNOTTYMLK".

- Decriptare: Pentru a decripta textul criptat, destinatarul cunoaște cheia. El folosește cheia pentru a face operația inversă a criptării și pentru a obține textul clar original.

- Exemplu de decriptare: Text criptat - "OXHNOTTYMLK", Cheie - "KEY". Decriptare: O - K = H, X - E = E, B - Y = L, etc. Astfel, textul criptat este redat ca "HELLOORLDW".

- Securitate: Cifrul Vigenère este considerat o îmbunătățire a cifrului lui Caesar, dar nu oferă o securitate foarte puternică în fața metodelor moderne de criptanaliză. Atacurile frecvente includ analiza frecvenței literelor și determinarea lungimii cheii. Dacă lungimea cheii este descoperită, cifrul poate fi spart cu ușurință.

2. Criptare prin transpoziție (Cifrul de Permutare):
- Criptare: Criptarea prin transpoziție implică rearanjarea literelor din textul clar într-un alt mod, în funcție de o regulă sau o cheie. De exemplu, să presupunem că avem un text clar "HELLOWORLD" și cheia este "312". În acest caz, litera "H" se va muta pe a treia poziție, "E" pe prima, "L" pe a doua, și așa mai departe. Textul criptat devine "EHLLOOWLRD".

- Decriptare: Pentru a decripta textul, destinatarul trebuie să cunoască cheia de permutare. El va inversa procesul de permutare pentru a obține textul clar original. În exemplul de mai sus, cheia de decriptare este "312", deci textul criptat "EHLLOOWLRD" devine "HELLOORLDW".

- Securitate: Cifrul de permutare poate oferi securitate în funcție de lungimea și complexitatea cheii de permutare. Cu toate acestea, dacă se folosește o cheie simplă sau dacă atacatorul are cunoștințe despre modul de permutare, acest sistem de criptare poate fi spart. O metodă obișnuită de criptanaliză este încercarea tuturor permutărilor posibile până când textul clar devine inteligibil.

ex.3

Fie textul criptat monoalfabetic:

ENHFJ EWK LML EOJ GDJ BMONKC PMCG YEPMAC FOVQGMROEQDHF FMAQNJ. CHWFJ GDJHO HWUJWGHMW HW 1978, GDJV DEUJ EG MWFJ LJJW FENNJK HWCJQEOELNJ, EWK DEUJ LJJW GDJ CALXJFG MY WAPJOMAC KHUMOFJC, GOEUJNC, EWK GMOPJWGC. HW GDJ JWCAHWR VJEOC, MGDJO FDEOEFGJOC DEUJ XMHWJK GDJHO FOVQGMROEQDHF YEPHNV. GDJOJC JUJ, GDJ QECCHUJ EWK CALPHCCHUJ JEUJCKOMQQJO, PENNMOV GDJ PENHFHMAC EGGEFTJO, EWK GOJWG, GOACGJK LV ENN, XACG GM WEPJ E YJB. BDHNJ ENHFJ, LML, EWK GDJHO JSGJWKJK YEPHNV BJOJ MOHRHWENNV ACJK GM JSQNEHW DMB QALNHF TJV FOVQGMROEQDV BMOTC, GDJV DEUJ CHWFJ LJFMPJ BHKJNV ACJK EFOMCC MGDJO CFHJWFJ EWK JWRHWJJOHWR KMPEHWC. GDJHO HWYNAJWFJ FMWGHWAJC GM ROMB MAGCHKJ MY EFEKJPHE EC BJNN: ENHFJ EWK LML EOJ WMB E QEOG MY RJJT NMOJ, EWK CALXJFG GM WEOOEGHUJC EWK UHCAEN KJQHFGHMWC GDEG FMPLHWJ QJKERMRV BHGD HW-XMTJC, MYGJW OJYNJFGHWR MY GDJ CJSHCG EWK DJGJOMWMOPEGHUJ JWUHOMWPJWGC HW BDHFD GDJV BJOJ LMOW EWK FMWGHWAJ GM LJ ACJK. PMOJ GDEW XACG GDJ BMONKC PMCG YEPMAC FOVQGMROEQDHF FMAQNJ, ENHFJ EWK LML DEUJ LJFMPJ EW EOFDJGVQJ MY KHRHGEN JSFDEWRJ, EWK E NJWC GDOMARD BDHFD GM UHJB
LOMEKJO KHRHGEN FANGAOJ. I.KAQMWG EWK E.FEGGEQEW FOVQGMFMAQNJ

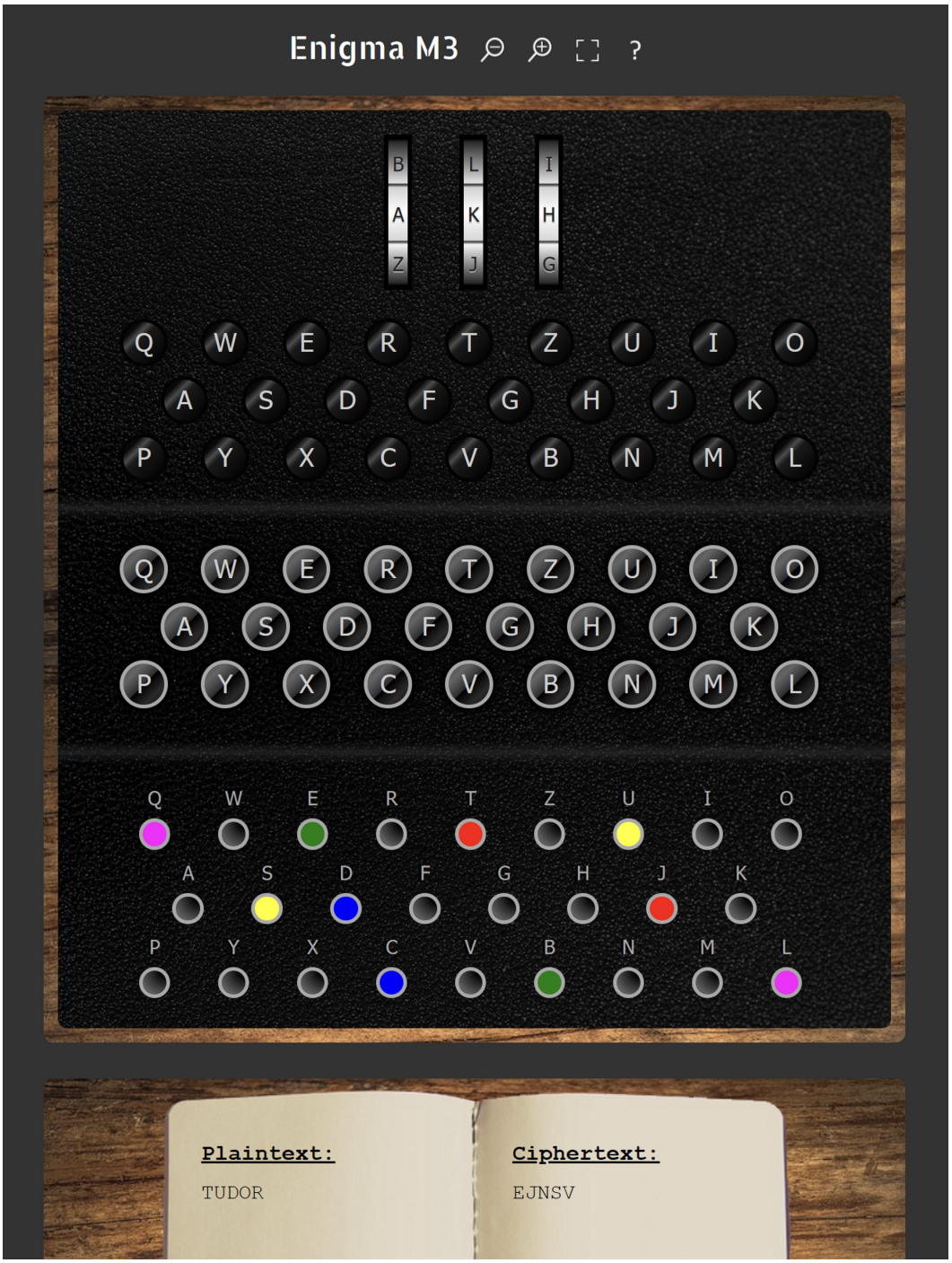
Cel mai frecvent apar

- J: 122 ori - inlocuim cu E
- E de 79 ori - inlocuim cu A
- G: 71 ori - inlocuim cu T
- M: 66 ori - inlocuim cu O
- W: 66 ori - inlocuim cu N
- H: 62 ori - inlocuim cu I

Text decriptat:

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

ex.4



- nume: TUDOR
  criptat: EJNSV

- am decriptat EJNSV in TUDOR fiindca am retinut literele care se apasa

- un exemplu de aceeasi lungime care n ar putea reprezenta criptarea numelui ar fi EEXJJ deoarece nu pot fi criptate si T si U in aceeasi litera, la fel si cu O si R