344, Polifronie Dragos-Constantin

tema 2

Ex1:

One time pad este o tehnica de criptare care nu poate fi crackuita, dar este nevoie de o cheie pe care sa o aiba doar cele 2 capete care comunica, cheie care nu poate mai fi mai scurta decat mesajul trimis. In aceasta tehnica, este folosita o cheie random secreta. Fiecare bit din mesaj este combinat cu bitul din cheie, iar mai apoi este impartit la 26.

Mesajul nu poate fi decriptat daca sunt respectate urmatoarele reguli:

1. Cheia trebuie sa fie cel putin la fel de lunga ca mesajul
2. Cheia trebuie sa fie random (distribuita uniform si independent de textul clar)

Exemplu: hardware random number generator (genereaza nr random prin proces fizic)

3. Cheia are folosinta unica.
4. Cheia trebuie tinuta secret.

A) Cum un mesaj este in Base64 si unul in hex le vom aduce la aceeasi forma transformand si primul mesaj intr-unul hexazecimal:
o9/khC3Pf3/9CyNCbdzHPy5oorccEawZSFt3mgCicRnihDSM8Obhlp3vviAVuBbiOtCSz6husBWqhfF0Q/8EZ+6iI9KygD3hAfFgnzyv9w==

va deveni
a3dfe4842dcf7f7ffd0b23426ddcc73f2e68a2b71c11ac19485b779a00a27119e284348cf0e6e1969defbe2015b816e23ad092cfa86eb015aa85f17443ff0467eea223d2b2803de101f1609f3caff7
Apoi vom face xor in textul criptat modificat si cheie si obtinem:

4f6e652054696d65205061642065737465207 56e2073697374656d20646520637269707461726520706572666563742073696775722064616361206573746520666f6c6f73697420636f726563742e

Iar rezultatul obtinut il convertim in ASCII si obtinem mesajul clar:

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

b) Avem mesajul criptat, mesajul clar si trebuie sa aflam cheia. Pentru a obtine cheia, transformam atat mesajul criptat, cat si mesajul clar in binar, iar apoi aplicam operatia de XOR.

o9/khC3Pf3/9CyNCbdzHPy5oorccEawZSFt3mgCicRnihDSM8Obhlp3vviAVuBbiOtCSz6husBWqhfF0Q/8EZ+6iI9KygD3hAfFgnzyv9w== va deveni

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

Iar Orice text clar poate obtinut dintr-un text criptat cu OTP dar cu alta cheie.. va deveni

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 01100001 01101100 01110100 01100001 00100000 01100011 01101000 01100101 01101001 01100101 00101110 00101110 XOR-am binarele, iar apoi rezultatul il transformam in hexazecimal si ramanem cu cheia:

A39096ed4eaa5f0b987357620eb0a64d0e18cdd668748c762a2f1ef475d6517d8bea40fedd938fb6e98ac65435db648b4aa4f3bb880dc535e5d1a154279e76478dd703b3def45cc1629905f65981d9

C) Cu cat refolosim mai mult cheia, cu atat cineva rau intentionat are sanse mai mari sa o afle, iar mai apoi sa puna mana si pe toate mesajele criptate cu acea cheie.

EX2.

<u>Metoda substitutiei:</u>

Cifrul Vigenère

Metoda poate fi considerata o generalizare a cifrului lui Cezar; in loc sa deplaseze intotdeauna litera pentru a fi criptata de acelasi numar de locuri, este mutata de un numar variabil, dar repetat de locuri, determinat pe baza unui cuvant cheie, care sa fie convenit intre expeditor si destinatar si sa fie scris in mod repetat sub mesaj, caracter cu caracter

Exemplu:

Plain text: STUDENT

Cheie: DRAGOS; CIPHER : **vkujsfw**

L = lungimea cifrului – numarul de elemente ale setului (26)

a = numarul literei cuvantului (0-25)

b = numarul literei cheii (0-25)

c = numarul litere textului criptat (0-25)

Pentru a cripta: n = a + b (mod 26); Pentru a decripta: n = c – b mod 26

Prima litera:

A[S] = 18

B[D] = 3

N = 21 mod 26 = 21

F(21) = V => c[0] = V

Decriptare: c[0] = V; A[v] = 21 = > 21 – 3 mod 26 = 18 => prima litera = A[18] = S

Criptanaliza Vigenère: Slabiciunea Vigenère consta în a fi, de fapt, un set de n cifrari Cezar, unde n este lungimea cheii; daca criptanalistul poate determina lungimea cheii (în cazul nostru, n) decriptarea devine foarte simpla. Pentru a face acest lucru, metodele statistice pot fi folosite pentru a gasi n, și ulterior se aplica analiza de frecventa pentru fiecare alfabet cifrat. Adica, daca avem cheia VIERME, este suficient sa analizam frecventele pentru toate literele criptate de V, apoi pentru cele criptate de I etc. Prin urmare, primul, al saselea, al unsprezecelea etc. litera va avea același alfabet cifrat. Cea mai complicata parte este, prin urmare, sa aflati lungimea cheii de criptare, chiar daca nu este imposibil. De fapt, în textul cifrat, daca cheia utilizată este scurta, vor exista probabil serii de litere repetate. Aceste serii de litere, daca sunt suficient de lungi (5-6 caractere), vor fi generate probabil din acelasi cuvant simplu. Apoi va fi suficient sa calculati distanta dintre un cuvant si altul si lungimea repetarii pentru a reveni la lungimea n a tastei. Facand acest lucru, este posibil sa înțelegeti care litere utilizeaza primul alfabet

cifrat, care al doilea și asa mai departe, continuand apoi cu analiza frecventelor pentru fiecare alfabet.

METODA TRANSPOZITIEI:

Cifrul rutei:

Cifrul rutei presupune scrierea textului in clar intr-o matrice de dimensiuni date, si folosirea unei chei ce ne spune in ce ordine trebuie transpus textul.

De exemplu: cuvant in clar: **WE ARE DISCOVERED FLEE AT ONCE**

MATRICE:

```
W R I O R F E O E
E E S V E L A N J
A D C E D E T C X
```

Key:

In spirala, in sensul acelor de ceasornic, incepand din dreapta-sus

Avem textul cifrat: **EJXCTEDEC DAEWRIORF EONALEVSE**

Metode de spargere:

O ruta aleasa prost ar putea lasa cuvinte in clar, sau bucati, sau chiar cuvinte intoarse.

Daca nu se descopera astfel de slabiciuni se pot incerca urmatoarele metode, metode generale pentru textele cifrate prin transpozitie:

Se poate folosi numarul frecventei, metoda anagramei: gasirea in textul cifrat a unei anagrame, iar mai apoi rezolvarea acesteia, gasind astfel patternuri pentru transpozitie.

Transpozitiile mai simple sunt vulnerabile la ‘incercari’, deoarce o cheie gresita, dar apropiata de cheia corecta, va descifra o parte din text, dand astfel indicii despre cheia corecta.

Ex 3:

Cum avem un sistem de subtitutie monoalfabetic stim ca o litera va fi inlocuita de aceeasi litera in textul criptat de cate ori apare. Cautam cele mai frecvente 5 litere in acesta si gasim pe J, E, G, M si W. In engleza cele mai frecvente sunt E, T, A, O si I.

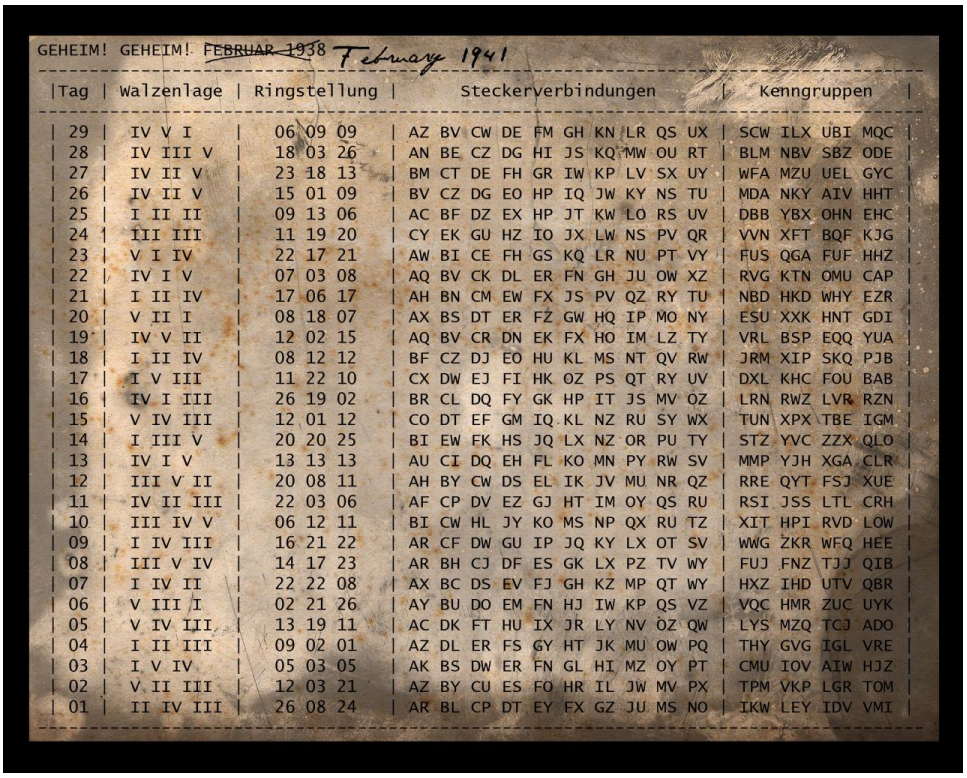
Inlocuim in primul cuvant si am obtine TNHFE, nu e satisfactor. Mai facem o permutare si avem E, A, T, O si I si obtinem in primul cuvant ANHFE si in al doilea AIK. Incercam sa obtinem

in al doilea cuvant AND pentru asta am ajunge la permutarea E, A, T, O, N, urmand sa mai potrivim ulterior cateva litere si obtinem textul 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.

EX4:

Voi folosi urmatoarea carte:



GEHEIM! GEHEIM! ~~FEBRUAR 1938~~ February 1941

Tag	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
29	IV V I	06 09 09	AZ BV CW DE FM GH KN LR QS UX	SCW ILX UBI MQC
28	IV III V	18 03 26	AN BE CZ DG HI JS KQ MW OU RT	BLM NBV SBZ ODE
27	IV II V	23 18 13	BM CT DE FH GR IW KP LV SX UY	WFA MZU UEL GYC
26	IV II V	15 01 09	BV CZ DG EO HP IQ JW KY NS TU	MDA NKY AIV HHT
25	I II II	09 13 06	AC BF DZ EX HP JT KW LO RS UV	DBB YBX OHN EHC
24	III III	11 19 20	CY EK GU HZ IO JX LW NS PV QR	VVN XFT BQF KJG
23	V I IV	22 17 21	AW BI CE FH GS KQ LR NU PT VY	FUS QGA FUF HHZ
22	IV I V	07 03 08	AQ BV CK DL ER FN GH JU OW XZ	RVG KTN OMU CAP
21	I II IV	17 06 17	AH BN CM EW FX JS PV QZ RY TU	NBD HKD WHY EZR
20	V II I	08 18 07	AX BS DT ER FZ GW HQ IP MO NY	ESU XXK HNT GDI
19	IV V II	12 02 15	AQ BV CR DN EK FX HO IM LZ TY	VRL BSP EQQ YUA
18	I II IV	08 12 12	BF CZ DJ EO HU KL MS NT QV RW	JRM XIP SKQ PJB
17	I V III	11 22 10	CX DW EJ FI HK OZ PS QT RY UV	DXL KHC FOU BAB
16	IV I III	26 19 02	BR CL DQ FY GK HP IT JS MV OZ	LRN RWZ LVR RZN
15	V IV III	12 01 12	CO DT EF GM IQ KL NZ RU SY WX	TUN XPX TBE IGM
14	I III V	20 20 25	BI EW FK HS JQ LX NZ OR PU TY	STZ YVC ZZX QLO
13	IV I V	13 13 13	AU CI DQ EH FL KO MN PY RW SV	MMP YJH XGA CLR
12	III V II	20 08 11	AH BY CW DS EL IK JV MU NR QZ	RRE QYT FSJ XUE
11	IV II III	22 03 06	AF CP DV EZ GJ HT IM OY QS RU	RSI JSS LTL CRH
10	III IV V	06 12 11	BI CW HL JY KO MS NP QX RU TZ	XIT HPI RVD LOW
09	I IV III	16 21 22	AR CF DW GU IP JQ KY LX OT SV	WWG ZKR WFQ HEE
08	III V IV	14 17 23	AR BH CJ DF ES GK LX PZ TV WY	FUJ FNZ TJJ QIB
07	I IV II	22 22 08	AX BC DS EV FJ GH KZ MP QT WY	HXZ IHD UTV QBR
06	V III I	02 21 26	AY BU DO EM FN HJ IW KP QS VZ	VQC HMR ZUC UYK
05	V IV III	13 19 11	AC DK FT HU IX JR LY NV OZ QW	LYS MZQ TCJ ADO
04	I II III	09 02 01	AZ DL ER FS GY HT JK MU OW PQ	THY GVG IGL VRE
03	I V IV	05 03 05	AK BS DW ER FN GL HI MZ OY PT	CMU IOV AIW HJZ
02	V II III	12 03 21	AZ BY CU ES FO HR IL JW MV PX	TPM VKP LGR TOM
01	II IV III	26 08 24	AR BL CP DT EY FX GZ JU MS NO	IKW LEY IDV VMI

Cu ziua 23: Rotoarele V I IV cu pozitiile 22 17 21 si literele de inceput HHZ,

Litere corelate: aw bi ce fh gs kq lr nu pt vy

Text clar: dragos

Cifrat: FPTED V

Decriptare:

FPTED V => dragos

Pasi:

Keyboard Input: F
Rotors Position: HHA
Plugboard Encryption: H
Wheel 3 Encryption: B
Wheel 2 Encryption: B
Wheel 1 Encryption: V
Reflector Encryption: W
Wheel 1 Encryption: T
Wheel 2 Encryption: K
Wheel 3 Encryption: D

Plugboard Encryption: D
Output (Lampboard): D

Keyboard Input: P
Rotors Position: HHB
Plugboard Encryption: T
Wheel 3 Encryption: X
Wheel 2 Encryption: H
Wheel 1 Encryption: X
Reflector Encryption: J
Wheel 1 Encryption: O
Wheel 2 Encryption: M
Wheel 3 Encryption: L
Plugboard Encryption: R
Output (Lampboard): R

Keyboard Input: T
Rotors Position: HHC
Plugboard Encryption: P
Wheel 3 Encryption: E
Wheel 2 Encryption: R
Wheel 1 Encryption: F
Reflector Encryption: S
Wheel 1 Encryption: L
Wheel 2 Encryption: H
Wheel 3 Encryption: W
Plugboard Encryption: A
Output (Lampboard): A

Keyboard Input: E
Rotors Position: HHD
Plugboard Encryption: C
Wheel 3 Encryption: Z
Wheel 2 Encryption: G
Wheel 1 Encryption: A
Reflector Encryption: Y
Wheel 1 Encryption: N
Wheel 2 Encryption: J
Wheel 3 Encryption: S
Plugboard Encryption: G
Output (Lampboard): G

Keyboard Input: D
Rotors Position: HHE
Plugboard Encryption: D
Wheel 3 Encryption: X
Wheel 2 Encryption: H
Wheel 1 Encryption: X
Reflector Encryption: J
Wheel 1 Encryption: O
Wheel 2 Encryption: M
Wheel 3 Encryption: O
Plugboard Encryption: O
Output (Lampboard): O

Keyboard Input: V
Rotors Position: HHF
Plugboard Encryption: Y
Wheel 3 Encryption: F
Wheel 2 Encryption: K
Wheel 1 Encryption: T
Reflector Encryption: Z
Wheel 1 Encryption: C
Wheel 2 Encryption: U
Wheel 3 Encryption: G
Plugboard Encryption: S
Output (Lampboard): S

Am folosit masina de la https://www.101computing.net/enigma-machine-emulator/

Un text criptat care nu ar putea fi numele meu:

FVNED M (CRIPTAT) = DLWGOG (TEXT CLAR)

Intrucat rotoarele isi misca pozitia dupa fiecare input, in functie de litera, am folosit F ca litera de inceput pentru a pastra D ul din nume, intrucat L ul este legat la R, am folosit criptarea lui, iar mai apoi W este legat la A, deci in loc sa criptam A vom cripta W.