③ Decriptati folosind Cezar, (A-Z), K=5

c	H	W	D	U	Y	T	L	W	F	U	M	D
C	7	22	3	20	24	19	11		5		12	
K	5	5	5	5	5	5	5		5		5	
m(mod 26)	2	17	$-2 \overset{24}{\equiv}$	15	19	14	6		0		7	
M	C	R	Y	P	T	O	G		R		A	P	H	Y

$-2 \pmod{26} = 24$

④ $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \in M_{2\times 2}(\mathbb{Z}_{26}) \Rightarrow$ math. dec + FWMDiQ

$A^t = \begin{pmatrix} 2 & 7 \\ 3 & 8 \end{pmatrix} \Rightarrow A^* = \begin{pmatrix} 8 & -3 \\ -7 & 2 \end{pmatrix} \Rightarrow A^{-1} = (\det A)^{-1} \cdot A^* =$

$= (16 - 21)^{-1} \cdot A^* = (-5)^{-1} \pmod{26}\ A^*$

$-5^{-1} \pmod{26} \equiv 21^{-1} \pmod{26} \Rightarrow$ Euclid

$26 : 21 = 1$ R $5 \Rightarrow x_5 = x_{26} - 1 \cdot x_{21} = (1,0) - (0,1) = (1,-1)$

$21 : 5 = 4$ R $1 \Rightarrow x_1 = x_{21} - 4 \cdot x_5 = (0,1) - 4(1,-1) = (-4,5)$

$\Rightarrow -5^{-1} \pmod{26} \equiv 5 \pmod{26} \Rightarrow$

$\Rightarrow A^{-1} = 5 \cdot \begin{pmatrix} 8 & -3 \\ -7 & 2 \end{pmatrix} \pmod{26} \equiv 5 \cdot \begin{pmatrix} 8 & 23 \\ 19 & 2 \end{pmatrix} = \begin{pmatrix} 40 & 115 \\ 95 & 10 \end{pmatrix} \equiv$

$\pmod{26} \equiv \begin{pmatrix} 14 & 9 \\ 17 & 10 \end{pmatrix} / \bullet \begin{pmatrix} F & M & I \\ W & D & Q \end{pmatrix} =$

$= \begin{pmatrix} 14 & 9 \\ 17 & 10 \end{pmatrix} \begin{pmatrix} 5 & 12 & 8 \\ 22 & 3 & 16 \end{pmatrix} \pmod{26} =$

$$= \begin{pmatrix} 115 & 276 & 184 \\ 594 & 81 & 432 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 9 & 16 & 2 \\ 22 & 3 & 16 \end{pmatrix} =$$

$$4 \cdot 26 = 104 \qquad = \begin{pmatrix} y & Q & C \\ W & D & Q \end{pmatrix}$$

Jwqdcq ?

---

(8) $A = \begin{pmatrix} 15 & 13 \\ 23 & 2 \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{Z}_{30})$ + cript. Hermione

$$\begin{pmatrix} 15 & 13 \\ 23 & 2 \end{pmatrix}\begin{pmatrix} H & R & i & N \\ E & M & O & E \end{pmatrix} = \begin{pmatrix} 15 & 13 \\ 23 & 2 \end{pmatrix}\begin{pmatrix} 7 & 17 & 8 & 13 \\ 4 & 12 & 14 & 4 \end{pmatrix} =$$

$$= \begin{pmatrix} 28\cdot 7 & 28\cdot 17 & 28\cdot 8 & 28\cdot 13 \\ 25\cdot 4 & 25\cdot 12 & 25\cdot 14 & 25\cdot 4 \end{pmatrix} =$$

$$= \begin{pmatrix} 196 & 476 & 224 & 364 \\ 100 & 300 & 350 & 100 \end{pmatrix} \pmod{30} \equiv \begin{pmatrix} 16 & 26 & 14 & 4 \\ 10 & 0 & 20 & 10 \end{pmatrix} =$$

$$= \begin{pmatrix} Q & \_ & O & E \\ K & A & U & K \end{pmatrix} \Rightarrow \text{QK\_AOUEK}$$

---

(2) Cript. cu Vigenère cu cheia CHEIE, $(A\text{-}Z\_?)^{28}$:

ce_algoritm_stă_la_baza_criptosistemului_des?

m	C	E	_	A	L	G	O	R	i	T	M	_	S	T	A	_	L	A	_
m	2	4	26	0	11	6	14	17	8	19	12	26	18	19	0	26	11	0	26
K	C	H	E	i	E	C	H	E	i	E	C	H	E	i	E	C	H	E	i
K	2	7	4	8	4	2	7	4	8	4	2	7	4	8	4	2	7	4	8
c(mod28)	4	11	2	8	15	8	21	21	16	13	14	5	22	27	4	0	18	4	6
C	E	L	C	i	P	i	V	V	Q	N	O	F	W	?	E	A	S	E	G

m	B	A	Z	A	_	C	R	i	P	T	O	S	i	S	T	E	M	U	L
m	1	0	25	0	26	2	17	8	16	19	14	18	8	18	19	4	12	20	11
K	E	C	H	E	i	E	C	H	E	i	E	C	H	E	i	E	C	H	E
K	4	2	7	4	8	4	2	7	4	8	4	2	7	4	8	4	2	7	4
(mod28)	5	2	4	4	6	6	19	15	19	27	18	20	15	22	27	8	14	27	15
C	F	C	E	E	G	G	T	P	T	?	S	U	P	W	?	i	O	?	P

m	U	i	_	D	E	S
m	20	8	26	3	4	18
K	i	E	C	H	E	i
K	8	4	2	7	4	8
(mod28)	0	12	0	10	8	26
C	A	M	A	K	i	_