Criptografie și securitate CTI

Laborator 2

1. Considerați cifrul *cavalerilor de Malta* din următoarea figură

$A:$	$B:$	$C:$
$D:$	$E:$	$F:$
$G:$	$H:$	$I:$

$J.$	$K.$	$L.$
$M.$	$N.$	$O.$
$P.$	$Q.$	$R.$

S	T	U
V	W	X
Y	Z	

   (a) Criptați următoarele mesaje: $m_1 =$ CONFIDENTIALITATE, $m_2 =$ CRIPTAREA DATELOR.

   (b) Decriptați mesajul $\overline{\_\_.\_\_}\ \boxed{\_\_:\_\_}\ \underline{\_\_\_}\ \underline{\_\_:\_\_}\ \underline{\_\_.\_\_}$

2. Considerați cifrul *Polybius* cu cheie (I=J).

   (a) Criptați mesajele: $m_1 =$ INTEGRITATE, $m_2 =$ SEMNATURI DIGITALE folosind cheia $k =$ FUNCTIE HASH.

   (b) Folosind cheia $k =$ FUNCTIE HASH, decriptați mesajul $c = 14\ 15\ 21\ 45\ 12\ 35\ 55$.

   Link suplimentar: `https://en.wikipedia.org/wiki/Polybius_square`

3. (a) Considerați cifrul Caesar cu cheia $k =$ D. Criptați numele vostru.

   (b) Considerați cifrul Vigenere cu cheia $k =$ FMI. Decriptați mesajul $c =$ HAZJOB.

4. Rezolvați următoarea criptogramă

   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

folosind `https://scottbryce.com/cryptograms/`.

5. Sisteme de *transpoziție*

   (a) Criptați mesajul $m =$ SPATIUL MESAJELOR CLARE folosind permutarea $\sigma = (2, 3, 1)$.

   (b) Decriptați mesajul criptat $c_1 =$ SFCMETAEAENLR folosind permutarea $\sigma = (1, 2, 3)$.
   Decriptați mesajul criptat $c_2 =$ ICRSCLFLOMCUIIPIITEIAREC folosind permutarea $\sigma = (3, 5, 2, 4, 1)$.

   Link suplimentar: `https://en.wikipedia.org/wiki/Transposition_cipher`

6. Considerați cifrul Playfair cu cheie (I=J).

   (a) Folosind cheia $k =$ CHEIE FOARTE SECRETA, criptați mesajul $m =$ NEVOIE AJUTOR.

   (b) Folosind cheia $k =$ CRYPTOOL, decriptați measjul $c =$ PIGO YCLE TYAE YLQV SFWN.

   Link suplimentar: `https://en.wikipedia.org/wiki/Playfair_cipher`