Problema 1 Analizati urmatoarele criptograme

1. FYVDV ZE TI WIDRV ZT FYV GTZHVDEV EFDITXVD FYOT FYV WIDRV FYOF YIAUE WZHV=XOAAIT QGRLVFE FIXVFYVD.

2. TZO DBY BDDOSBIJWT JHIRXBIJ IQJ HREJ ZK TZOS KZZ CT DBWDOWBIRYM IQJ GRHIBYDJ CJIPJJY TZOS JWCZP BYG TZOS PSRHI.

3. PBJKAYT EN JLHQPQYM EN KUA NPKKAJK, RA JUELMT UYQA JLHQPQYM EN KUA RPKKPAJK. KUYK RYW RA SYB YMM TPA MYLDUPBD.

4. TN'O XFF FBDN X LNJRQXQBIH EIL YNHNLIPBQV, XHO TN'O XFF FBDN QI ZRV BQ MANXJ. *GBYHIH *GMFXRYAFBH, *XGNLBMXH CIRLHXFBPQ

5. WHP EGIT LW GHWLBPK: Y SGH'L VW YHLW GEE LBP IPLGYEX. Y'NP GEKPGIT LWEI TWM FWKP GOWML YL LBGH Y'NP BPGKI FTXPEA.

6. KCKY SNK NGTJKOS SNQYMO GTK OZ OQXRWK QY TKSTZORKIS. NZA OQWWD ZL PO SZ OSTPMMWK SZ QYCKYS SNKX, ANKY SNKD AKTK OZ ZHCQZPO!

7. LXR VCQJ C SOTOWM DL FNCA LXR MJA, DRA LXR VCQJ C SOKJ DL FNCA LXR MOTJ. *FOWEAXW *EYJWGJH *GNRHGNOSS

8. WT RP PIPUM CTHU TY WCP QEZCW VAX XVUB EG V REUVOQP, PIPUM OHSEO EAOC TY GDVOP EG V REUVOQP. *JVQW *JCEWRVA

9. NYT QYZTV STVTQN FV J STEFQMJQG ZI NYJN FRWG NYT UFWZNZQJW UJMNG FDN FV UFBTM ORFBI YFB NF MDR NYT XFATMRETRN.

10. WPBUK *DSGCWE RSDNSIPFED RPBBCWV HWPTSID CIES DTPRW HCEZ EZWN, CI RPDW EZW BWEFBI EBCT HSFIV FT CI *DCQWBCP.

Problema 2 Realizați criptanaliza poloneză (Marian Rejewski) urmărind următorii pași:

1. În aceeaşi zi s-au recepţionat următoarele chei pentru criptarea mesajelor

APN VIS...	GBD PEE...	NCK QZW...	TMJ FJM...
CDX MBK...	GOU PFQ...	NVE QGO...	UGX RCK...
CKC MLV...	HCI IZD...	OCT JZF...	VAN COS...
DEY NRX...	HDA IBJ...	OHV JPC...	VXP CVL...
DGF NCY...	ISO YDH...	QOJ XFM...	WXU UVQ...
EVT TGF...	KVU ZGQ...	QUW XKZ...	XPD BIE...
EZG TWN...	LMS AJA...	SJI OYD...	YTL EAU...
FLI GXD...	MWV SUC...	TAE FOO...	ZYY LMX...

2. Care este caracteristica zilei? (lungimea ciclilor celor 3 permutări compuse: prima literă în a patra, a doua literă în a cincea, a treia literă în a şasea).

3. Ulterior s-a recepţionat şi: LOC ... . Ştiind că orice text recepţionat începe cu transmiterea dublată a cheii de criptare a mesajului, puteţi spune care sunt următoarele litere?

4. Mai jos este un fragment dintr-o tabelă care evidenţiază corespondenţa dintre caracteristica zilei şi poziţia iniţială a rotorilor. Care este poziția inițială?

Poziţia rotorilor	Caracteristica	Permutarea (fără plugboard)
⋮	⋮	⋮
BIR	$13, 13$	(AEJHNTCSUFMLY)(BRGXZOKWVQPID)
BIS	$12, 12, 1, 1$	(ATKEGXFLYHUD)(BONVICRQSZMJ)(P)(W)
BIT	$13, 13$	(AHFUBZKIGLNVP)(CTXORMWYDQESJ)
BIU	$12, 12, 1, 1$	(BNSPIMZKXRJE)(CHTDLYGOFVWU)(A)(Q)
BIV	$13, 13$	(AVRMSTJWUCKZL)(BHIPEOFGYDNQX)
BIW	$9, 9, 3, 3, 1, 1$	(ATFSDBECO)(GRZWUKLXV)(HYI)(JPM)(N)(Q)
BIX	$11, 11, 2, 2$	(AJMIDETHGNS)(FPXKWZYLUQO)(BC)(RV)
BIY	$13, 13$	(AULOITYHGRWVB)(CJXPQZNEDSKMF)
BIZ	$8, 8, 4, 4, 1, 1$	(BIXTZNKJ)(EPVH0QFW)(CYDR)(GMLS)(A)(U)
⋮	⋮	⋮

5. Folosind permutările aferente poziției inițiale determinate anterior, determinaţi tabela de conexiuni.

6. Utilizând detaliile determinate anterior, decriptați următorul mesaj $c =$ BLGHXNPOVRKXJMCOYPTTAVPRUJELWRSSBWKKWXMW știind că s-a folosit reflectorul B, ordinea rotorilor este III, II, I și inițializarea inelului de caractere este $1, 1, 1$.

Link suplimentar:
`https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma` - Capitolul Rejewski's characteristics method