Laborator 2 Criptografie si securitate

Martie 2021

I Cum functionează maşina Enigma?

- Khan Academy
- World Science Festival
- Numberphile

II Criptarea, decriptarea şi criptanaliza britanică

(a) Criptati mesajul
CRYPTOGRAPHY AND SECURITY LABORATORY
ţinând cont de:
- Se înlocuieşte spaţiul cu **X**.
- Folosim cheia corespunzătoare zilei de 02.03
- Se foloseşte cheia **LOL**.

(b) Ştiind că se utilizează cheia din ziua 02.03. Decriptaţi mesajul
UXHVUV UCTOHLAIZNOGSUD

(c) S-a interceptat mesajul **CETINFWUTYPED....**. Care din următoarele mesaje des utilizate (cribs) ar putea corespunde acestuia?
- WEATHERXREPORT
- BATTLEXREPORT
- ATTACKXREPORT

III Criptarea, decriptarea şi criptanaliza poloneză (Marian Rejewski)

(a) Determinarea caracteristicii zilei
- Consideraţi aceeaşi modalitate de criptare de mai sus.
- Indicaţi o vulnerabilitate care rezultă din această modalitate de utilizare a maşinii Enigma.
- În aceeaşi zi s-au recepţionat următoarele chei pentru criptarea mesajelor:

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

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

(b) Ulterior s-a recepţionat şi: **FOC...** .Ştiind că orice text recepţionat începe cu transmiterea dublă a cheii, care sunt urmă toarele litere?

(c) Mai jos este un fragment dintr-o tabelă care evidenţiază coresponden cta dintre caracteristica zilei şi poziţia iniţială a rotorilor. Care este aceasta poziţie?

Poziţia rotorilor	Caracteristica	Permutarea (fără conexiuni)
...	...	...
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)
...	...	...

(d) Folosind permuările determinate şi cele din tabelă, determinaţi tabela de conexiuni.

(e) S-a interceptat mesajul:

OJRJ YBZK ABHN PIIR NX

Ştiind că a fost criptat folosind:

- Ordinea rotorilor: III, II, I
- Iniţializarea inelului de caractere: 1, 1, 1
- Poziţia iniţială a rotorilor: de la c)
- Tabela de conexiuni: de la d)
- Reflectorul: B

decritaţi-l.

(f) Linkuri utile:

- Simulator enigma
- Simulator online enigma
- Detalii tehnice