

Zavelca_Miruna_Andreea_Tema_2

II. Criptarea, decriptarea și criptanaliza britanică

(a) Criptați mesajul:

CRYPTOGRAPHY AND SECURITY LABORATORY

ținând cont de:

- Se înlocuiește spațiul cu X

CRYPTOGRAPHYXANDXSECURITYXLABORATORY

- Folosim cheia corespunzătoare zilei de 02.03

03	C	III	V	II	21	06	04	W	R	S	AI	CV	EQ	GU	HZ	JN	LS	OX	RT	WY
02	B	V	I	II	18	02	02	A	N	D	AX	BK	CH	EP	FR	GM	IL	JY	NT	QW
01	B	IV	III	II	19	04	21	Q	Z	A	AJ	BY	EX	FG	KW	LT	MV	NZ	OS	RU

- Se folosește cheia LOL

LOLLOLCRYPTOGRAPHYXANDXSECURITYXLABORATORY

Rezultatul:

VIEW

Plaintext

LOLLOLCRYPTOGRAPHYXANDXSECURITYXLABORATORY

ENCODE DECODE

Enigma machine

MODEL

Enigma M3

REFLECTOR

UKW B

ROTOR 1

V

POSITION

- 1 A +

RING

- 18 R +

ROTOR 2

I

POSITION

- 14 N +

RING

- 2 B +

ROTOR 3

II

POSITION

- 4 D +

RING

- 2 B +

PLUGBOARD

ax bk ch ep fr gm il jy nt qw

VIEW

Ciphertext

exvpu dvcob aqcpr jzpkz graru
kepjk ohmuf kjqau pf

exvpu dvcob aqcpr jzpkz graru kepjk ohmuf kjqau pf

(b) Știind că se utilizează cheia din ziua 02.03, deciptați mesajul:

UXHVUV UCTOHLAIZNOGSUD

Rezultatul:

The screenshot shows a web-based Enigma machine simulator. It has three main panels: Ciphertext, Enigma machine, and Plaintext. The Ciphertext panel contains 'UXHVUV UCTOHLAIZNOGSUD'. The Enigma machine panel shows the following settings: MODEL: Enigma M3, REFLECTOR: UKW B, ROTOR 1: V (Position: - 1 A +, Ring: - 18 R +), ROTOR 2: I (Position: - 14 N +, Ring: - 2 B +), ROTOR 3: II (Position: - 4 D +, Ring: - 2 B +), and PLUGBOARD: ax bk ch ep fr gm il jy nt qw. The Plaintext panel shows the result 'bobbo bsrgez whmfk hucbs o'.

bobbo bsrgez whmfk hucbs o

Lipim literele:

bobbobsrgzwhmfkhucbso

Eliminăm cheia dublată și obținem mesajul:

srgzwhmfkhucbso

(c) S-a interceptat mesajul:

CETINFWUTYPED...

Care din următoarele mesaje des utilizate (cribs) ar putea corespunde acestuia?

WEATHERXREPORT

BATTLEXREPORT

ATTACKXREPORT

Presupunem că este folosită cheia repetată. În acest caz, știm că decriptarea mesajului va începe cu 6 litere irelevante pentru mesaj, pe care le vom nota cu *:

*****WEATHERXREPORT

*****BATTLEXREPORT

*****ATTACKXREPORT

Știm, de asemenea, că o literă nu poate fi criptată în ea însăși. Căutăm litere comune mesajului criptat și variantelor decriptate, pe aceeași poziție, pentru a elimina variante:

CETINFWUTYPED

*****WEATHERXREPORT

*****BATTLEXREPORT

*****ATTACKXREPORT

Se observă că niciuna dintre variantele date nu respectă condițiile prezentate anterior. Așadar, mesajul nu poate corespunde niciuneia dintre ele.