

ENIGMA

I. Cum funcționează Enigma?

Vizualizați cele 2 filmulețe ca să înțelegeți cum funcționează Enigma:

<https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/case-study-ww2-encryption-machines>

https://www.youtube.com/watch?v=ASfAPOiq_eQ

II. Criptare

1. Criptați mesajul **MECHANISATION OF SECRECY**.
 - i. Mai întâi, modificați mesajul într-un format compatibil, înlocuind spațiul cu X.
 - ii. Folosiți cheia corespunzătoare zilei (04.03).
 - iii. Considerați modul de criptare utilizat inițial de operatorii germani (înainte de transmiterea mesajului, se trimitea duplicat o cheie de criptare a mesajului). Considerați cheia **DOP** pentru criptarea mesajului.
2. Vizualizați legăturile interne și modul de funcționare al mașinii Enigma.

III. Decriptare

- i. Considerați același mod de criptare de mai sus.
- ii. Cheia este cea corespunzătoare zilei (04.03).
- iii. Decriptați mesajul **RPVLU JHNBT NLQMN OCAA**.

IV. Criptanaliza poloneză (Marian Rejewski)

1. Determinarea caracteristicii zilei
 - i. Considerați aceeași modalitate de criptare de mai sus.
 - ii. Indicați o vulnerabilitate care rezultă din această modalitate de utilizare a mașinii Enigma.
 - iii. În aceeași zi s-au recepționat 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...

- iv. 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 șasea).
2. Ulterior s-a recepționat și: **LOC** Știind că orice text recepționat începe cu transmiterea dublată a cheii de criptare a mesajului, puteți spune care sunt următoarele litere?
3. Mai jos este un fragment dintr-o tabelă care evidențiază corespondența dintre caracteristica zilei și poziția inițială a rotorilor. Care este aceasta poziție?

Poziția 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)(FPXKWZYLQO)(BC)(RV)
BIY	13,13	(AULOITYHGRWVB)(CJXPQZNEDSKMF)
BIZ	8,8,4,4,1,1	(BIXTZNKJ)(EPVH0QFW)(CYDR)(GMLS)(A)(U)
...

4. Folosind permutările determinate și cele din tabelă, determinați tabela de conexiuni.
5. S-a interceptat mesajul: **BLGH XNST PVBX WMUZ P**.
Știind că a fost criptat folosind:
- Ordinea rotorilor (Walzenlage): III, II, I;
 - Inițializarea inelului de caractere (Ringstellung): 1,1,1;
 - Poziția inițială a rotorilor (Schlüssel): de la 3;

- Tabela de conexiuni(Steckerverbindungen): de la 4;
 - Reflectorul (UKW): B.
- decriptați-l.

V. Criptanaliza britanică (Alan Turing)

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

① Mai multe informații:

1. Simon Singh, The Enigma Machine.
<http://www.youtube.com/watch?v=2b6xSuMsoY8>
2. Enigma Simulator.
<http://users.telenet.be/d.rijmenants/en/enigmasim.htm>
3. Enigma Simulator (online):
<https://cryptii.com/pipes/enigma-machine>
4. Crypto Museum, Enigma Cipher Machine.
<http://www.cryptomuseum.com/crypto/enigma/index.htm>
5. Wikipedia, Arthur Scherbius.
http://en.wikipedia.org/wiki/Arthur_Scherbius
6. Technical Details of the Enigma Machine
<http://users.telenet.be/d.rijmenants/en/enigmatech.htm>
7. IEEE Computing: Alan Turing at Bletchley Park
http://www.youtube.com/watch?v=5nK_ft0Lf1s&playnext=1&list=PL54E3809040EE1338&feature=results_main
8. Enigma – A Very Famous Story of Cryptology
<http://www.mlb.co.jp/linux/science/genigma/enigma-referat/enigma-referat.html>