ENIGMA

I. Cum funcţionează 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. Criptaţi mesajul ***ARTHUR SCHERBIUS***.
    i. Mai întâi, modificaţi mesajul într-un format compatibil, înlocuind spaţiul cu X.
    ii. Folosiţi cheia corespunzătoare zilei (14.03).
    iii. Consideraţi modul de criptare utilizat iniţial de operatorii germani (înainte de transmiterea mesajului, se trimitea duplicat o cheie de criptare a mesajului). Consideraţi cheia ***MOD*** pentru criptarea mesajului.

2. Vizualizaţi legăturile interne şi modul de funcţionare al maşinii Enigma.

III. Decriptare

i. Consideraţi acelaşi mod de criptare de mai sus.
ii. Cheia este cea corespunzătoare zilei (14.03).
iii. Decriptaţi mesajul ***AQPRV QYDWW BDDKJ CSEHG LYBK.***

IV. Criptanaliza poloneză (Marian Rejewski)

1. Determinarea caracteristicii zilei
    i. Consideraţi aceeaşi modalitate de criptare de mai sus.
    ii. Indicaţi o vulnerabilitate care rezultă din această modalitate de utilizare a maşinii Enigma.
    iii. 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…**

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 şasea).

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

3. Mai jos este un fragment dintr-o tabelă care evidenţiază corespondenţa 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)**
…	**…**	**…**

4. Folosind permutările determinate şi cele din tabelă, determinaţi tabela de conexiuni.

5. S-a interceptat mesajul: ***SZROW BOKOB XSSMD HFZDB ZCI.***
Ştiind că a fost criptat folosind:

- Ordinea rotorilor (Walzenlage): III, II, I;
- Iniţializarea inelului de caractere (Ringstellung): 1,1,1;
- Poziţia iniţială a rotorilor (Schluessel): de la 3;
- Tabela de conexiuni(Steckerverbindungen): de la 4;

- Reflectorul (UKW): B.

decriptaţi-l.

V. Criptanaliza britanică (Alan Turing)

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

ⓘ Mai multe informaţii:

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 Blatchley 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