Criptografie și securitate CTI

Laborator 4

MAȘINĂRIA ENIGMA - Descriere și Criptanaliză

1. Folosind link-urile următoare, urmărind pașii de mai jos criptați mesajul $m =$ APARATI CAPITALA CU ORICE PRET.

   (a) Modificaţi mesajul într-un format compatibil, înlocuind spaţiul cu X.

   (b) Folosiţi cheia corespunzătoare zilei de 16 setând ordinea rotorilor (Walzenlage), iniţializarea inelului de caractere (Ringstellung), poziţia iniţială a rotorilor (Schluessel).

   (c) Consideraţi modul de criptare utilizat iniţial de operatorii germani (înainte de transmiterea mesajului, se trimitea duplicat o cheie de criptare a mesajului). Consideraţi cheia DOP pentru criptarea mesajului.

   (d) Realizați decriptarea mesajului obținut.

   Link suplimentar:
   `https://www.101computing.net/enigma-machine-emulator/`,
   `https://www.101computing.net/enigma-daily-settings-generator/`.

2. Folosind link-urile anterioare, decriptați mesajul $c =$ FVODO SZKTT ZSEYR HQRAO RV urmărind următorii pași:

   (a) Folosiţi cheia corespunzătoare zilei de 15.

   (b) Verificați dacă cheia inițială se repetă așa cum este necesar.

3. Determinați numărul total al cheilor posibile astfel:

   (a) Numărul alegerilor posibile ale rotoarelor;

   (b) Numărul tuturor pozițiilor posibile ale fiecărui rotor;

   (c) Numărul combinațiilor din *plugboard* dacă avem 8 cabluri de conectare.

4. Realizați criptanaliza britanică (Alan Turing) știind că a fost interceptat următorul mesaj: CBTINFWUTYBEDJ... Care dintre următoarele mesaje des utilizate (cribs) ar putea corespunde acestuia?

   (a) WEATHERXREPORT

   (b) BATTLEXREPORTS

   (c) GENERALXORDERS

   Cum ați gândit?

5. Realizați criptanaliza poloneză (Marian Rejewski) urmărind următorii pași:

(a) 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...

(b) 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).

(c) 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?

(d) 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)
⋮	⋮	⋮

(e) Folosind permutările aferente poziției inițiale determinate anterior, determinaţi tabela de conexiuni.

(f) 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-uri suplimentar:
`https://www.youtube.com/watch?v=G2_Q9FoD-oQ`
`https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma` - Rejewski's characteristics method