Capitolul 3

Sisteme mecanice de criptare

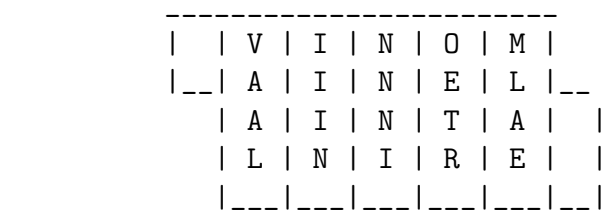
Sistemele de criptare pot fi aduse la un grad mai mare de complexitate şi securitate dacă se folosesc mijloace mecanice de criptare. Astfel de mecanisme special construite vor uşura – pe de-o parte – operaţiile de criptare/decriptare, iar pe de-altă parte vor fi capabile să creeze un număr mult mai mare de chei posibile.

3.1 Sistemul *Skitala*

*Skit*ala ("baston" în greceşte) este o unealtă folosită pentru realizarea unui sistem de criptare cu permutări. El este sub formă aproximativ cilindrică, în jurul lui fiind înfăşurată o bandă de hârtie. Mesajul se scrie în mod normal pe această bandă, după care hârtia este desfăcută. La primire se foloseşte un băţ asemănător pe care se înfăşoară sulul de hârtie, mesajul devenind din nou inteligibil (pentru detalii, a se vedea [8], [23]). Conform istoricilor greci, spartanii foloseau – începând cu sec. V î.H. – acest mod de comunicare, în timpul campaniilor militare[1]. El avea avantajul de a fi rapid şi nu comportă erori de transmitere. Dezavantajul este acela că este uşor de spart.

Exemplul 3.1 *Să presupunem că dimensiunile băţului permit scrierea a* 4 *rânduri, cu* 5 *caractere pe fiecare rând. Fie "VINO MAINE LA INTALNIRE" textul care trebuie criptat. Ignorând spaţiile, mesajul va apare scris sub forma*

[1]Skitala a fost menţionată prima oară de poetul grec Archilochus (sec. VII î.H). Deşi apare ulterior şi în alte texte, abia la mijlocul secolului III î.H. Apollonius din Rhodos specifică limpede utilizarea lui ca mijloc de criptare. De remarcat că pentru perioada respectivă, sistemele de criptare folosite de greci erau de tip steganografic. O descriere a modului de operare este dată apoi de Plutarh (50-120 A.D.).



După derularea de pe skitala, mesajul scris pe banda de hârtie este:

VAALIIINNNNIOETRMLAE.

La decriptare, banda va fi rulată din nou şi fiecare a patra literă va fi pe aceeaşi linie.

Criptanaliza este foarte simplă. Se iau pe rând valorile $n = 2, 3, 4, \ldots$. *Pentru o astfel de valoare fixată, se formează* n *rânduri de tipul*

$$n + i, 2n + i, 3n + i, \ldots \quad (i = 1, 2, \ldots, n)$$

care ulterior se concatenează. Există o valoare a lui n *pentru care textul astfel format este inteligibil.*

3.2 Cilindrul Jefferson

Ideea de maşină de criptare apare clar prima dată la Thomas Jefferson, primul secretar de Stat al Statelor Unite; acesta a inventat un aparat de criptat numit *roată de criptare*, folosit pentru securitatea corespondenţei cu aliaţii – în special cei francezi[2].

Un cilindru Jefferson este format din n discuri de dimensiuni egale (iniţial $n = 26$ sau $n = 36$, dar valoarea este nerelevantă pentru descrierea sistemului) aşezate pe un ax. Discurile se pot roti independent pe ax, iar pe muchea fiecăruia sunt inscrise cele 26 litere ale alfabetului, într-o ordine aleatoare (dar diferită pentru fiecare disc).

La criptare, textul clar se împarte în blocuri de n caractere. Fiecare astfel de bloc se scrie pe o linie (generatoare) a cilindrului, rotind corespunzător fiecare disc pentru a aduce pe linie caracterul căutat. Oricare din celelalte 25 linii va constitui blocul de text criptat.

Pentru decriptare este necesar un cilindru identic, în care se scrie pe o linie textul criptat (de n caractere) şi apoi se caută printre celelalte 25 linii un text cu semnificaţie semantică. Probabilitatea de a avea un singur astfel de text creşte cu numărul de discuri din cilindru.

O mică diferenţă apare dacă textul clar nu are nici o semnificaţie semantică (s-a folosit o dublă criptare). Atunci trebuie convenită dinainte o anumită distanţă de criptare s ($1 \leq s \leq 25$).

[2]Thomas Jefferson a folosit acest aparat în perioada 1790 – 1802, după care se pare că ideea s-a pierdut. Devenit preşedinte, Jefferson a fost atras de sistemul Vigenere, pe care îl consideră mai sigur şi-l recomandă secretarului său de stat James Madison ca înlocuitor al sistemului pe care îl inventase anterior.

Ordinea discurilor poate fi de asemenea schimbată. De exemplu, un cilindru cu $n = 10$ discuri poate realiza $10! = 3.628.800$ texte criptate diferite pentru acelaşi text clar.

Cilindrul Jefferson realizează o substituţie polialfabetică de perioadă n. Dacă ar fi privit ca un sistem de criptare Vigenere, lungimea cheii este enormă (de multe ori n^n, în funcţie de modalităţile de aranjare a alfabetelor pe discuri), şi deci metoda de atac a lui Kasiski este inaplicabilă.

Exemplul 3.2 *Să considerăm* $n = 10$ *şi fie cilindrul, în care am desfăşurat literele de pe cele* 10 *discuri:*

	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
1	*A*	*A*	*A*	*A*	*A*	*A*	*A*	*A*	*A*	*A*
2	*R*	*R*	*P*	*N*	*V*	*S*	*P*	*E*	*I*	*I*
3	*I*	*O*	*S*	*I*	*O*	*O*	*U*	*S*	*R*	*H*
4	*E*	*S*	*Y*	*M*	*T*	*R*	*H*	*U*	*E*	*E*
5	*K*	*U*	*L*	*O*	*Y*	*P*	*I*	*P*	*S*	*T*
6	*O*	*V*	*U*	*C*	*L*	*M*	*S*	*B*	*L*	*O*
7	*B*	*I*	*K*	*U*	*E*	*U*	*E*	*L*	*B*	*M*
8	*C*	*J*	*B*	*L*	*B*	*B*	*N*	*C*	*C*	*U*
9	*U*	*L*	*R*	*T*	*C*	*D*	*R*	*D*	*D*	*C*
10	*D*	*B*	*C*	*Y*	*D*	*Y*	*Y*	*H*	*F*	*D*
11	*J*	*V*	*D*	*B*	*G*	*E*	*D*	*I*	*N*	*F*
12	*T*	*C*	*T*	*F*	*F*	*C*	*B*	*J*	*Y*	*G*
13	*L*	*G*	*F*	*G*	*K*	*V*	*F*	*F*	*T*	*J*
14	*N*	*K*	*G*	*S*	*N*	*H*	*G*	*O*	*G*	*P*
15	*P*	*N*	*O*	*H*	*H*	*F*	*V*	*G*	*H*	*Q*
16	*W*	*P*	*N*	*J*	*U*	*K*	*J*	*K*	*J*	*B*
17	*Q*	*Q*	*E*	*D*	*P*	*L*	*K*	*M*	*K*	*N*
18	*M*	*T*	*H*	*E*	*Q*	*Q*	*M*	*N*	*M*	*V*
19	*S*	*H*	*M*	*K*	*R*	*I*	*T*	*Q*	*P*	*W*
20	*V*	*E*	*Q*	*P*	*S*	*J*	*O*	*R*	*Q*	*X*
21	*X*	*D*	*V*	*Q*	*W*	*N*	*L*	*V*	*V*	*L*
22	*Z*	*Y*	*W*	*V*	*X*	*G*	*W*	*W*	*W*	*Y*
23	*G*	*W*	*X*	*X*	*M*	*T*	*Q*	*Y*	*O*	*K*
24	*H*	*X*	*Z*	*R*	*I*	*W*	*X*	*X*	*U*	*R*
25	*Y*	*Z*	*I*	*Z*	*J*	*X*	*Z*	*T*	*X*	*S*
26	*F*	*M*	*J*	*W*	*Z*	*Z*	*C*	*Z*	*Z*	*Z*

Cu ajutorul lui, textul clar TREI CULORI construit pe una din liniile generatoare ale cilindrului va genera următoarele linii (oricare din ele putând fi folosit drept text criptat):

T	*R*	*E*	*I*	*C*	*U*	*L*	*O*	*R*	*I*
L	*O*	*H*	*M*	*D*	*B*	*W*	*G*	*E*	*H*
N	*S*	*M*	*O*	*G*	*D*	*Q*	*K*	*S*	*E*
P	*U*	*Q*	*C*	*F*	*Y*	*X*	*M*	*L*	*T*
W	*V*	*V*	*U*	*K*	*E*	*Z*	*N*	*B*	*O*
Q	*I*	*W*	*L*	*N*	*C*	*C*	*Q*	*C*	*M*
M	*J*	*X*	*T*	*H*	*V*	*A*	*R*	*D*	*U*
S	*L*	*Z*	*Y*	*U*	*H*	*P*	*V*	*F*	*C*
V	*B*	*I*	*B*	*P*	*F*	*U*	*W*	*N*	*D*
X	*F*	*J*	*F*	*Q*	*K*	*H*	*Y*	*Y*	*F*
Z	*C*	*A*	*G*	*R*	*L*	*I*	*X*	*T*	*G*
G	*G*	*P*	*S*	*S*	*Q*	*S*	*T*	*G*	*J*
H	*K*	*S*	*H*	*W*	*I*	*E*	*Z*	*H*	*P*
Y	*N*	*Y*	*J*	*X*	*J*	*N*	*A*	*J*	*Q*
F	*P*	*L*	*D*	*M*	*N*	*R*	*E*	*K*	*B*
A	*Q*	*U*	*E*	*I*	*G*	*Y*	*S*	*M*	*N*
R	*T*	*K*	*K*	*J*	*T*	*D*	*U*	*P*	*V*
I	*H*	*B*	*P*	*Z*	*W*	*B*	*P*	*Q*	*W*
E	*E*	*R*	*Q*	*A*	*X*	*F*	*B*	*V*	*X*
K	*D*	*C*	*V*	*V*	*Z*	*G*	*L*	*W*	*L*
O	*Y*	*D*	*X*	*O*	*A*	*V*	*C*	*O*	*Y*
B	*W*	*T*	*R*	*T*	*S*	*J*	*D*	*U*	*K*
C	*X*	*F*	*Z*	*Y*	*O*	*K*	*H*	*X*	*R*
U	*Z*	*G*	*W*	*L*	*R*	*M*	*I*	*Z*	*S*
D	*M*	*O*	*A*	*E*	*P*	*T*	*J*	*A*	*Z*
J	*A*	*N*	*N*	*B*	*M*	*O*	*F*	*I*	*A*

Dacă se consideră o dublă criptare cu distanţa $s = 3$, atunci textul clar AAAAAAAAAA va fi criptat cu cilindrul anterior în ESYMTRHUEE.

Cilindrul Jefferson a fost reinventat ulterior de mai multe ori, cea mai notabilă fiind se pare maşina de criptat $M - 94$, care a fost utilizată până la începutul celui de al doilea război mondial.

3.3 Maşini de criptat

Prima jumătate a sec. XX este dominată de maşinile de criptat, o combinaţie între maşinile de scris şi sisteme de criptare mecanice bazate pe discuri.

3.3.1 Enigma

Poate cea mai celebră maşină de criptat a fost maşina germană *Enigma*. Sub acest nume se află o varietate largă de modele de maşini de criptat electro-mecanice, care asigură o criptare polialfabetică de tip Vigenere sau Beaufort.

Ea a fost proiectată la Berlin în 1918, de inginerul german Arthur Scherbius. Primul model (A) este prezentat la Congresele Uniunii Poştale Internaţionale din 1923 şi 1924. Modele ulterioare sunt folosite în mai multe ţări europene şi asiatice (Suedia, Olanda, Marea Britanie, Japonia, Italia, Spania, SUA, Polonia, Elveţia) în scopuri comerciale, militare sau diplomatice. Din 1926 începe să fie preluată şi de armata germană, care după 1928 îşi defineşte propriile modele (G, I, K).

În total au fost construite circa 100.000 maşini Enigma, din care 40.000 în timpul războiului. După 1945 aliaţii au capturat toate maşinile de pe teritoriul german, acestea fiind încă mult timp considerate sigure. Abia în 1970 au apărut primele informaţii despre decriptarea de către aliaţi (Biuro Szyfrow - Polonia şi Bletchley Park - Anglia) a unui mare număr de mesaje criptate prin modelul militar Enigma şi transmise prin radio în timpul războiului.

O descriere completă a maşinii este destul de lungă; recomand pentru detalii [47], [23]. În linii mari, ea are următoarele componente:

- *Tastatură*: Este o componentă mecanică formată din:
  - Un pupitru de taste (similar unei maşini de scris);
  - n discuri adiacente, care se rotesc în jurul unui ax. La marea majoritate a modelelor Enigma $n = 3$; sunt însă şi versiuni cu $n = 5, 6$ sau $n = 7$ discuri. Pe fiecare disc sunt scrise cele 26 caractere alfabetice (la care uneori se mai adaugă trei caractere speciale);
  - Un mecanism de avans (similar ceasurilor mecanice) care permite – la apăsarea unei taste – rotirea unuia sau mai multor discuri cu un număr de poziţii. Sunt folosite mai multe variante; cea mai frecventă constă în rotirea cu o poziţie a discului din dreapta, la fiecare apăsare a unei taste, acompaniată în anumite situaţii de rotirea discurilor vecine.

- *Circuite electrice*: Criptarea unui caracter se realizează electric. Componenta mecanică este concepută în aşa fel încât să formeze un circuit electric. La apăsarea unei taste circuitul se închide şi luminează una sau mai multe lămpi, indicând litera de ieşire.

- *Reflector (Umkehrwalze)*: Este o componentă specifică maşinilor de criptat Enigma (introdusă în 1926 la sugestia lui Willy Korn). Scopul ei este de a realiza un sistem de criptare Beaufort (maşina să poată fi capabilă de a cripta şi decripta mesaje).

  În majoritatea variantelor, reflectorul este aşezat pe ax după ultimul disc (din stânga); el realizează o substituţie (fixată), după care reintroduce noul caracter prin discuri în sens invers, dar pe alt drum. Deci o maşină Enigma cu n discuri va realiza criptarea unui caracter prin $2n + 1$ substituţii.

  O consecinţă a acestei proprietăţi este aceea că un caracter nu va fi niciodată criptat în el însuşi, slăbiciune exploatată adesea cu succes de criptanalişti.

- *Tabela de conexiuni (Steckerbrett)*[3]: Este o componentă (poziţionată în faţă, sub tastele literelor) în care se pot face conexiuni între perechi de litere, prin intermediul unor cabluri (similar centralelor telefonice vechi). Deci la un mesaj sunt posibile maxim 13 conexiuni. De exemplu, dacă printr-un cablu sunt conectate literele S şi W, de câte ori este tastat S, semnalul este comutat pe W înainte de a intra pe discuri.

  Introdusă în 1930, această componentă asigură un plus de securitate şi a fost principalul obstacol în criptanaliză.

Starea iniţială a unei maşini Enigma se referă la:

- *Ordinea discurilor (Walzenlage)*: alegerea numărului de discuri şi ordinea lor de utilizare;
- *Poziţia iniţială a discurilor*: poziţionarea în mod independent a fiecărui disc, diferită pentru fiecare mesaj;
- *Iniţializarea inelului de caractere (Ringstellung)*: poziţionarea alfabetului relativ la primul disc.
- *Iniţializarea conexiunilor (Steckerverbindungen)*: conexiunile dintre litere în cadrul tabelei de conexiuni.

Matematic, Enigma criptează fiecare literă după o procedură care poate fi exprimată prin produs de permutări. Să presupunem că avem o maşină Enigma cu 3 discuri şi fie P transformarea tabelei de conexiuni, U – reflectorul, S, M, D – acţiunile celor 3 discuri (din stânga, mijloc şi respectiv dreapta). Atunci criptarea e poate fi scrisă sub forma:

$$e = PDMSUS^{-1}M^{-1}D^{-1}P^{-1}$$

După fiecare apăsare a unei taste, discurile se rotesc schimbând transformarea. De exemplu, dacă discul din dreapta se roteşte cu i poziţii, atunci transformarea devine $\rho^i D\rho^{-i}$, where ρ este permutarea ciclică stânga a vectorului $(A, B, C, \ldots, Z)$. Similar, discurile din mijloc şi stânga pot fi reprezentate prin j respectiv k rotiri ale lui M respectiv S.

Atunci funcţia de criptare poate fi descrisă astfel:

$$e = P(\rho^i D\rho^{-i})(\rho^j M\rho^{-j})(\rho^j S\rho^{-k})U(\rho^j S^{-1}\rho^{-k})(\rho^j M^{-1}\rho^{-j})(\rho^i D^{-1}\rho^{-i})P^{-1}$$

Decriptarea se efectuează după aceeaşi formulă.

Să calculăm numărul de variante posibile pentru criptarea unui mesaj. Vom considera o maşină Enigma cu 3 discuri. Atunci numărul de situaţii iniţiale posibile este $26 \cdot 26 \cdot 26 =$

[3] *plugboard* în engleză.

17.576. Cum cele 3 discuri pot fi permutate în 6 moduri, numărul variantelor se ridică la $6 \cdot 17.576 = 105.456$.

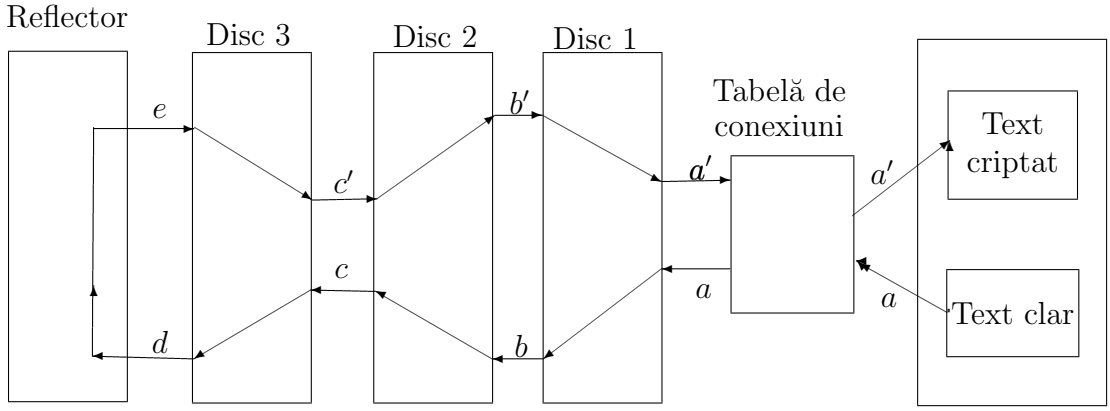
Pentru fiecare din acestea, o tabelă de conexiuni cu 10 perechi de litere conectate ridică numărul variantelor la 150.738.274.937.250.

La acestea se adaugă şi modul de poziţionare al inelului de caractere la mecanismul discurilor, care mai ridică ordinul de mărime al variantelor cu aproximativ 10^5. Aceste estimări arată că Enigma era cea mai sigură maşină de criptat a momentului respectiv.

Să detaliem funcţionarea unei maşini Enigma (din punct de vedere matematic):

- Fiecare disc poate fi reprezentat ca un set de permmutări pentru litere – codificate cu valori între 0 şi 25; fie $\alpha_1, \alpha_2, \alpha_3$ permutările de pe cele trei discuri (de la dreapta spre stânga).
- Fie r_1, r_2, r_3 setările iniţiale de pe cele trei discuri (caracterele situate iniţial pe poziţiile accesibile ale discurilor).
- Pentru simplificare, vom ignora rolul tabelei de conexiuni.
- Vom nota cu β substituţia reflectorului (reprezentată ca un set de permutări între perechi de caractere.

Să urmărim – pe un exemplu – un traseu care pleacă de la semnalul de intrare (un caracter din textul clar), trece prin cele trei discuri şi reflector şi dă ca rezultat caracterul criptat (a se vedea figura).



Exemplul 3.3 *Să presupunem că cele permutările celor trei discuri sunt:*

$\alpha_1 = (0\ 15\ 6\ 10\ 14\ 8\ 19\ 17\ 22\ 18\ 11)(1\ 2\ 9\ 13\ 21\ 25)(3\ 4\ 23\ 5\ 24\ 7\ 12\ 16\ 20)$
$\alpha_2 = (0\ 7\ 9\ 4\ 6\ 18\ 23\ 25\ 8)(1\ 17\ 19)(2\ 20\ 10)(3\ 12)(5\ 11\ 13\ 21)(14\ 22\ 15\ 16\ 24)$
$\alpha_3 = (0\ 2\ 4\ 7\ 16\ 17\ 19\ 5)(1\ 6\ 3\ 8\ 21\ 24\ 11\ 13\ 9\ 10\ 25\ 12\ 14\ 15)(18\ 23\ 20\ 22)$

Substituţia β este definită

$$\beta = (0\ 4)(1\ 7)(2\ 9)(3\ 16)(5\ 20)(6\ 8)(10\ 19)(11\ 17)(12\ 25)(13\ 18)(14\ 24)(15\ 22)(21\ 23).$$

Deci, cu α_1, 0 *este mutat în* 15, 15 *este mutat în* 6, 25 *este mutat în* 1 *etc.*
Inversele celor trei permutări (folosite "pe drumul de întoarcere") sunt:

$\alpha_1^{-1} = (11\ 18\ 22\ 17\ 19\ 8\ 14\ 10\ 6\ 15\ 0)(25\ 21\ 13\ 9\ 2\ 1)(20\ 16\ 12\ 7\ 24\ 5\ 23\ 4\ 3)$
$\alpha_2^{-1} = (8\ 25\ 23\ 18\ 6\ 4\ 9\ 7\ 0)(19\ 17\ 1)(10\ 20\ 2)(12\ 3)(21\ 13\ 11\ 5)(24\ 16\ 15\ 22\ 14)$
$\alpha_3^{-1} = (5\ 19\ 17\ 16\ 7\ 4\ 2\ 0)(15\ 14\ 12\ 25\ 10\ 9\ 13\ 11\ 24\ 21\ 8\ 3\ 6\ 1)(22\ 20\ 23\ 18)$

Setările iniţiale sunt $r_1 = 22$ *(deci primul rotor are "vizibilă" litera* V*),* $r_2 = 7$, $r_3 = 12$.
Substituţiile celor trei discuri sunt date – matematic – de formulele

$$b = [a + r_1 \ (mod\ 26)]^{\alpha_1}, \qquad c = [b + r_2 \ (mod\ 26)]^{\alpha_2}, \qquad d = [c + r_3 \ (mod\ 26)]^{\alpha_3},$$

unde $x^\alpha = y$, y *fiind elementul care urmează lui* x *în permutarea* α. *Astfel, de exemplu* $3^{\alpha_1} = 4$, $8^{\alpha_2} = 0$ *etc.*
Această notaţie permite să scriem de asemenea

$$e = d^\beta.$$

În continuare, semnalul parcurge cele trei discuri în sens invers:

$$c' = e^{\alpha_3^{-1}} - r_3 \ (mod\ 26), \qquad b' = (c')^{\alpha_2^{-1}} - r_2 \ (mod\ 26), \qquad a' = (b')^{\alpha_1^{-1}} - r_1 \ (mod\ 26).$$

După criptarea unui caracter, cele trei discuri sunt resetate după regula:
$r_1 := r_1 + 1 \ (mod\ 26)$*; dacă noua valoare* $r_1 = 0$ *atunci* $r_2 := r_2 + 1 \ (mod\ 26)$*; dacă noua valoare* $r_2 = 0$, *atunci* $r_3 := r_3 + 1 \ (mod\ 26)$.

Pentru exemplificare, să criptăm litera K *(al cărei cod numeric este* 10*).*

$a = 10$*;*
$b = [a + r_1 \ (mod\ 26)]^{\alpha_1} = [10 + 22 \ (mod\ 26)]^{\alpha_1} = 6^{\alpha_1} = 10$*;*
$c = [b + r_2 \ (mod\ 26)]^{\alpha_2} = [10 + 7 \ (mod\ 26)]^{\alpha_2} = 17^{\alpha_2} = 22$*;*
$d = [c + r_3 \ (mod\ 26)]^{\alpha_3} = [22 + 12 \ (mod\ 26)]^{\alpha_3} = 8^{\alpha_3} = 21$.

Trecerea prin reflector dă $e = d^\beta = 21^\beta = 23$.

Acum se parcurg cele trei discuri în sens invers:

$c' = e^{\alpha_3^{-1}} - r_3 \ (mod\ 26) = 23^{\alpha_3^{-1}} - 12 \ (mod\ 26) = 18 - 12 \ (mod\ 26) = 6$*;*
$b' = (c')^{\alpha_2^{-1}} - r_2 \ (mod\ 26) = 6^{\alpha_2^{-1}} - 7 \ (mod\ 26) = 4 - 7 \ (mod\ 26) = 23$*;*
$a' = (b')^{\alpha_1^{-1}} - r_1 \ (mod\ 26) = 23^{\alpha_1^{-1}} - 22 \ (mod\ 26) = 4 - 22 \ (mod\ 26) = 8$.

Deci criptarea caracterului K *este* I *(litera corespunzătoare codului* 8*).*

Setările pentru criptarea următorului caracter sunt $r_1 := 23$, $r_2 = 7$, $r_3 = 12$.

Detalii despre modul de construcţie al maşinii de criptat Enigma se pot găsi în [4], [34] şi – mai ales din punct de vedere al criptanalizei – în [24].

3.3.2 $C-36$ ($M-209$ C)

Maşina $C-36$ este concepută de inginerul suedez Boris Hagelin, la solicitarea armatei americane de a avea o maşină de criptat portabilă, uşor de mânuit, care să poată fi folosită după un instructaj sumar. Este cunoscută şi sub numele de $M-209$ C, la bază fiind un model creat de Hagelin în Suedia la sfârşitul anilor $'30$. Ea începe să fie produsă – după câteva modificări legate de design – în 1940 şi înlocuieşte treptat maşina de criptat $M-94$. Se apreciază că în timpul războiului au fost produse circa 140.000 maşini de criptat $C-36$.

Nu au fost specificate măsuri speciale de securitate; $C-36$ nu a fost realizată pentru a fi criptografic sigură, ea fiind destinată zonelor militare tactice, unde era nevoie doar de o siguranţă de câteva ore faţă de o eventuală criptanaliză.

Vom da o prezentare matematică a principiilor sale de construcţie; pentru alte detalii, a se vedea [22] şi [48].

Definiţia 3.1 *Se numeşte matrice lug o matrice binară $M_{6\times 27}$ în care fiecare din cele* 27 *coloane conţine cel mult doi de* 1.

Exemplul 3.4 *([35]). Toate exemplificările referitoare la $M-209$ vor fi făcute pentru matricea*

$$M=\begin{pmatrix}
0&0&0&1&0&0&0&0&1&0&1&0&0&0&1&1&1&0&0&0&0&0&0&0&0&0&1\\
1&0&0&0&1&0&0&0&1&0&0&1&1&0&0&0&1&0&0&1&0&0&1&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&1&0&0&0&1&0&1&0&0&0&0&1&0&0&1&0&0&0&1&1&1&1&1&1\\
0&0&1&0&1&0&0&0&0&0&0&1&0&0&0&1&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&1&0&0&1&0&0&0&0&0&1&0&0&0&1&0&0&0
\end{pmatrix}$$

Fie v un vector binar de dimensiune 6. Atunci $c\cdot M$ este un vector cu 27 componente având elemente din mulţimea $\{0,1,2\}$. Numărul de elemente nenule din $v\cdot M$ se numeşte *ponderea lui v în raport cu M*.

O *configuraţie de început* se obţine prin aşezarea unul sub altul (aliniaţi la stânga) a şase vectori binari de lungimi $17,19,21,23,25,26$.

Exemplul 3.5 *Structura*

0 1 1 0 0 0 1 0 0 0 0 0 0 0 1 1 0
0 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 1 0 0 0 1 0 0 0 1
1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 1 0 0 0 0 0 0 0 1

formează o posibilă configuraţie de început.

Spre deosebire de matricea lug, la configuraţia de început nu există restricţii privind numărul de 1.

Plecând de la o configuraţie de început, se pot genera o infinitate de vectori de dimensiune 6 în felul următor:

1. Primii 17 vectori sunt coloanele complete ale configuraţiei de început.

2. Fiecare vector linie se repetă ciclic din momentul când s-a terminat.

Pe baza acestor elemente se poate descrie sistemul de criptare al maşinii $C-36$. Reamintim, codificarea numerică a literelor este de la $A-0$ până la $Z-25$; toate calculele se vor face modulo 26.

Fie x codul celui de-al i-lea caracter din textul clar şi h ponderea celui de-al i-lea vector generat de configuraţia de început în raport cu matricea *lug*. Atunci

$$y = h - x - 1.$$

Exemplul 3.6 *Să considerăm textul clar*

NU PUTEM REUSI DECAT IMPREUNA

împreună cu matricea lug şi configuraţia de început din exemplele anterioare. Codificarea numerică a textului este

13 20 15 20 19 4 12 17 4 20 18 8 3 4 2 0 19 8 12 15 17 4 20 13 0.

După ignorarea spaţiilor libere[4]*, lungimea textului clar este* 25.

Vom calcula ponderile primilor 25 *vectori şi vom aranja totul sub forma unui tablou:*

h	10	17	16	9	9	9	7	0	0	0	0	12	0
x	13	20	15	20	19	4	12	17	4	20	18	8	3
$h-x-1$	22	20	0	14	15	4	20	8	21	5	7	3	22
	W	*W*	*A*	*O*	*P*	*E*	*U*	*I*	*V*	*F*	*H*	*D*	*W*

h	0	18	7	0	0	18	7	9	9	19	14	9
x	4	2	0	19	8	12	15	17	4	20	13	0
$h-x-1$	21	15	6	6	17	5	17	17	4	24	0	8
	V	*P*	*G*	*G*	*R*	*F*	*R*	*R*	*E*	*Y*	*A*	*I*

Deci textul criptat este

WWAOPEUIVFHDWVPGGRFRREYAI

Matricea *lug* şi configuraţia de început formează cheia pentru maşina $C-36$. De fapt, maşina însăşi este o realizare fizică a acestui sistem: ea operează conform cu o cheie stabilită anterior prin fixarea unor roţi dinţate şi a unui disc (pentru detalii vezi [48]).

[4]În aplicaţiile practice, spaţiul se înlocuieşte uneori cu o literă de frecvenţă redusă.

Observaţia 3.1 *Ecuaţia de decriptare este identică cu cea de criptare:*

$$x = h - y - 1.$$

Deci din acest punct de vedere sistemul de criptare este de tip Beaufort şi maşina $C - 36$ *poate fi folosită atât pentru criptare cât şi pentru decriptare.*

Deoarece liniile din configuraţia de început au lungimi numere prime între ele, vectorii generaţi încep să se repete sigur după $17 \cdot 19 \cdot 21 \cdot 23 \cdot 25 \cdot 26 = 101.405.850$ paşi; deci cuvântul cheie poate fi considerat mai lung decât orice text clar. Sunt însă cazuri când această perioadă poate fi mai scurtă. De exemplu, dacă configuraţia de început conţine numai 1, se va genera un singur vector, deci perioada este 1. De asemenea se obţin perioade scurte pentru matrici *lug* cu foarte puţini 1 sau configuraţii de început în care raportul dintre numărul de 0 şi 1 este disproporţionat.

Nu există o condiţie matematică pentru existenţa a exact 6 linii în configuraţia de început. Acest număr a fost ales ca un compromis între securitatea criptografică şi uşurinţa de a cripta. În general perioada creşte cu numărul de linii.

Maşina de criptat $M - 209$ avea şi ea o serie de slăbiciuni (un atac cu texte clare alese care au anumite componente comune poate duce la informaţii asupra matricii *lug*), astfel că în 1943 criptanaliştii germani puteau decripta mesajele. Totuşi – din punct de vedere militar tactic – ea a fost considerată perfect adaptată necesităţilor şi a fost folosită de armata americană până după războiul din Coreea ($1953 - 1956$).

Ulterior, Hagelin a elaborat un model îmbunătăţit: maşina $C - 52$. Aceasta avea o perioadă de 2.756.205.443; discurile puteau şi scoase şi reinserate în altă ordine; exista un disc al cărui alfabet putea fi permutat.

$C - 52$ a făcut parte din ultima generaţie de maşini de criptat clasice, noua tehnologie (cea a computerelor) permiţând dezvoltarea altor mecanisme cu o putere de calcul mult mai mare.

3.4 Exerciţii

1. Să se cripteze, folosind sistemul skitala pe 6 rânduri - primul vers din Iliada:
   CANTA ZEITA MANIA CE-APRINSE PE-AHIL PELEIANUL

2. Se interceptează trei zile la rând câte un mesaj:

   (*a*) *UKMV UIEE LBIM KPHN KGMR MVUI EVMI KHKN KMNK RI*;

   (*b*) *DOSX DEKK NCES OWYP OHSI SXDE KXSE OYOP OSPO IE*;

   (*c*) *JBVZ JKOO PUKV BQFW BYVE VZJK OZVK BFBW BVWB EK*.

   Despre aceste mesaje ştim că:

   - Reprezintă acelaşi text clar;

- Sunt criptate folosind un cilindru Jefferson având trei discuri identice;

- Criptarea s-a făcut în prima zi cu deplasarea 1, în a doua zi cu deplasarea 2, iar în a treia zi cu deplasarea 3.

Să se decripteze mesajul iniţial şi să se reconstituie cilindrul Jefferson cu care s-a făcut criptarea.

3. Se dă matricea

$$\begin{array}{cccccccccccccccccccccccccc}
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & & & & & & & & \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & & & & & & \\
1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & & & & \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & & \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}$$

Nu se cunoaşte matricea lug, dar din textul criptat

$$CSDZ\ RGGV\ PSLA\ BCBU\ PTEU\ SHDO\ HBNO\ CDTO\ YBMS$$
$$NUKD\ GAAY\ WZRS\ WPV$$

s-au putut decripta primele 20 caractere:

$$CUMQITIQASTERNIQASAQVEIQSTA$$

Să se decripteze restul textului.

4. Maşina Enigma asigură un cifru de substituţie sau un cifru de transpoziţie ?

De ce ?

5. Utilizând discurile, reflectorul şi setările iniţiale din Exemplul 3.3, să se cripteze textul clar

MASINA DE CRIPTARE.

6. Utilizând discurile, reflectorul şi setările iniţiale din Exemplul 3.3, să se decripteze textul

YDDMYU.

Bibliografie

[1] Anderson R. ş.a. - *Serpent: A proposal for the Advanced Encryption Standard*, http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/serpent.pdf

[2] Atanasiu A. - *Teoria codurilor corectoare de erori*, Editura Univ. Bucureşti, 2001;

[3] D. Bayer, S. Haber, W. Stornetta; Improving the efficiency and reliability of digital time-stamping. Sequences II, Methods in Communication, Security and Computer Science, Springer Verlag (1993), 329-334.

[4] A. Bruen, M. Forcinito, *Cryptography, Information Theory, and Error - Correction*, Wiley Interscience 2005.

[5] Bos J.N., Chaum D. - Provably unforgable signatures; Lecture Notes in Computer Science, $740(1993), 1-14$

[6] D. Chaum, H. van Antwerpen - Undeniable signatures; Lecture Notes in Computer Science, $435(1990), 212-216$

[7] D. Chaum, E. van Heijst, B. Pfitzmann; Cryptographically strong undeniable signatures, unconditionally secure for the signer. Lecture Notes in Computer Science, 576 (1992), 470-484.

[8] Brigitte Collard - *Secret Language in Graeco-Roman antiquity* (teză de doctorat) $http://bcs.fltr.ucl.ac.be/FE/07/CRYPT/Intro.html$

[9] Cook S., $http://www.claymath.org/millennium/P\_vs\_NP/Official\_Problem\_Description.pdf$

[10] Coppersmith D. ş.a. - *MARS - a candidate cypher for AES*, http://www.research.ibm.com/security/mars.pdf

[11] Daemen J., Rijmen V. - *The Rijndael Block Cipher Proposal*, http://csrc.nist.gov/CryptoToolkit/aes/

[12] I.B. Damgard; A design principle for hash functions. Lecture Notes in Computer Science, 435 (1990), 516-427.

[13] Diffie D.W., Hellman M.E. - *New Directions in Cryptography*, IEEE Transactions on Information Theory, IT-22, 6 (1976), pp. 644-654

[14] W. Diffie, M.E. Hellman - Multiuser cryptographic techniques; AFIPS Conference Proceedings, $45(1976), 109 - 112$

[15] L´ Ecuyer P. - *Random Numbers for Simulation*, Comm ACM 33, 10(1990), 742-749, 774.

[16] Enge A. - *Elliptic Curves and their applications to Cryptography*, Kluwer Academic Publ, 1999

[17] El Gamal T., *A public key cryptosystem and a signature scheme based on discrete algorithms*, IEEE Transactions on Information Theory, 31 (1985), 469-472

[18] Fog A. - *http://www.agner.org/random/theory*;

[19] Gibson J., *Discrete logarithm hash function that is collision free and one way*. IEEE Proceedings-E, 138 (1991), 407-410.

[20] S. Haber, W. Stornetta; How to timestamp a digital document. Journal of Cryptology, 3(1991), 99-111.

[21] van Heyst E., Petersen T.P. - How to make efficient fail-stop signatures; Lecture Notes in Computer Science, $658(1993), 366 - 377$

[22] Kahn D. - *The Codebreakers*, MacMillan Publishing Co, New York, 1967

[23] Kelly T. - *The myth of the skytale*, Cryptologia, Iulie 1998, pp. 244 - 260.

[24] A. Konheim - *Computer Security and Cryptography*, Wiley Interscience, 2007.

[25] Knuth D. - *The art of computer Programming*, vol 2 (Seminumerical Algorithms)

[26] R.C. Merkle; A fast software one-way functions and DES. Lecture Notes in Computer Science, 435 (1990), 428-446

[27] Mitchell C.J., Piper F., Wild, P. - Digital signatures; Contemporary Cryptology, The Science of Information Integrity, IEEE Press, $(1992), 325 - 378$

[28] Menezes A., Oorschot P., Vanstome S., *Handbook pf Applied Cryptography*

[29] B. Preneel, R. Govaerts, J. Vandewalle; Hash functions based on block ciphers: a syntetic approach. Lecture Notes in Computer Science, 773 (1994), 368-378

[30] Rivest R. ş.a - *The RC6^{TM} Block Cipher*,
ftp://ftp.rsasecurity.com/pub/rsalabs/rc6/rc6v11.pdf

[31] R.L. Rivest; The **MD4** message digest algorithm. Lecture Notes in Computer Science, 537, (1991), 303-311

[32] Rivest R., Shamir A., Adleman A., *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM, Vol. 21 (2), 1978, pages 120–126.

[33] Rosing, M, *Implementing Elliptic Curve Cryptography*, Manning, 1998

[34] D. Salmon, *Data Privacy and Security*, Springer Professional Computing, 2003

[35] Salomaa A., *Criptografie cu chei publice*, Ed. Militară, Bucureşti 1994

[36] Schneier B., *Applied Cryptography*, John Wiley and Sons, 1995

[37] Schneier B ş.a. - *Twofish*, http://www.counterpane.com/twofish.html

[38] Selmer E.S. - *Linear Recurrence over Finite Field*, Univ. of Bergen, Norway, 1966;

[39] Sibley E.H. - *Random Number Generators: Good Ones are Hard to Find*, Comm ACM 31, 10(1988), 1192-1201.

[40] Smid M.E., Branstad, D.K. - Response to comments on the $NIST$ proposed digital signature standard; Lecture Notes in Computer Science, $740(1993), 76 - 88$

[41] Stinton D., *Cryptography, Theory and Practice*, Chapman& Hall/CRC, 2002

[42] Wiener M.J. - *Cryptanalysis of short RSA secret exponents*, IEEE Trans on Information Theory, 36 (1990), 553-558

[43] Williams H.C. - *Some public-key criptofunctions as intractable as factorisation*, Cryptologia, 9 (1985), 224-237.

[44] Zeng K.G., Yang C.H., Wei D.Y., Rao T.R.N.- *Pseudorandom Bit Generators in Stream Cipher Cryptography*, IEEE Computer, 24 (1991), 8.17.

[45] Secure hash Standard. National Bureau of Standards, FIPS Publications 180, 1993

[46] Digital signature standard; National Bureau of Standards, FIPS Publications 186, 1994

[47] $http://en.wikipedia.org/wiki/Enigma\_machine$

[48] $http://en.wikipedia.org/wiki/M-209$

[49] *http://en.wikipedia.org/wiki/Caesar_ cipher# History_ and_ usage*

[50] *http://psychcentral.com/psypsych/Polybius_ square*

[51] *http://www.answers.com/topic/vigen-re-cipher*

[52] *http://en.wikipedia.org/wiki/Rosetta_ stone*

[53] *Serpent homepage*, http://www.cl.cam.ac.uk/ rja14/serpent.html

[54] *P versus NP homepage*, http://www.win.tue.nl/ gwoegi/P-versus-NP.htm

[55] http://www.win.tue.nl/ gwoegi/P-versus-NP.htm

[56] http://en.wikipedia.org/wiki/Complexity_ classes_ P_ and_ NP