Sisteme mecanice de criptare

Prof. Dr. Adrian Atanasiu

February 13, 2011

Ordin crescut de complexitate și securitate.

Ordin crescut de complexitate și securitate.

Simplifică operațiile de criptare/decriptare.

Ordin crescut de complexitate și securitate.

Simplifică operațiile de criptare/decriptare.

Capabile să genereze un număr semnificativ de chei posibile.

Sistemul *Skitala*

Permite realizarea unui sistem de criptare cu permutări.

Sistemul *Skitala*

Permite realizarea unui sistem de criptare cu permutări. Spartanii foloseau skitala (începând cu sec. V î.H.) în timpul campaniilor militare.

Sistemul *Skitala*

Permite realizarea unui sistem de criptare cu permutări.
Spartanii foloseau skitala (începând cu sec. V î.H.) în timpul campaniilor militare.
Menționat de poetul grec Archilochus (sec. VII î.H).
La mijlocul secolului III î.H. Apollonius din Rhodos specifică clar utilizarea lui ca mijloc de criptare.
O descriere a modului de operare este dată de Plutarh (50-120 A.D.).

Sistemul *Skitala*

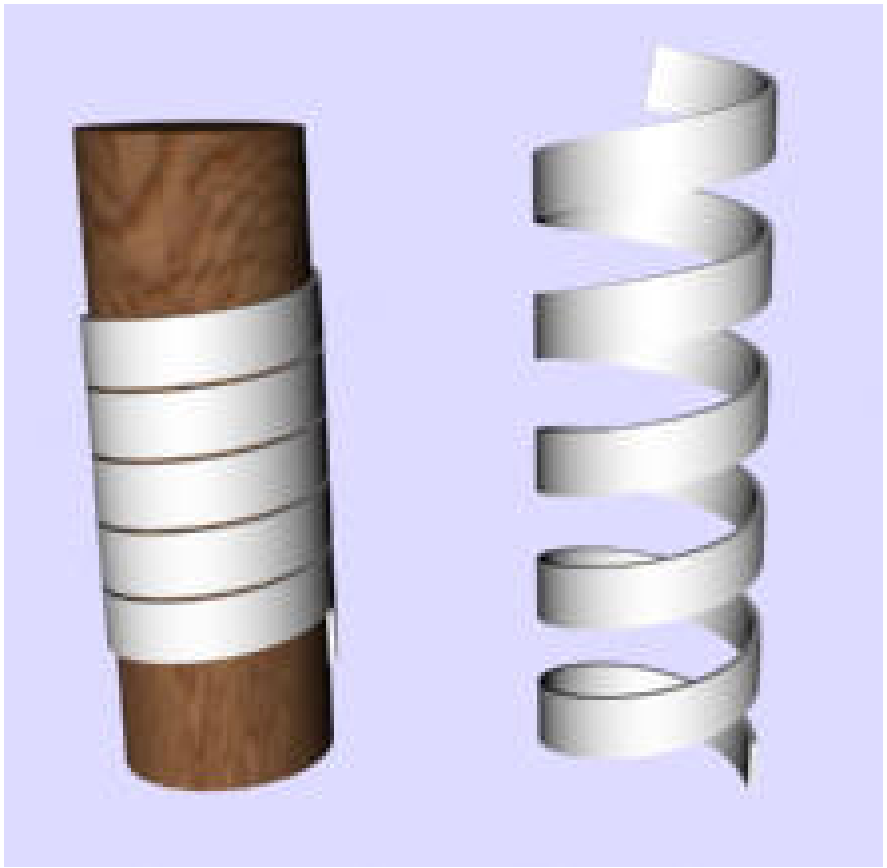
Permite realizarea unui sistem de criptare cu permutări.
Spartanii foloseau skitala (începând cu sec. *V* î.H.) în timpul campaniilor militare.
Menționat de poetul grec Archilochus (sec. VII î.H).
La mijlocul secolului III î.H. Apollonius din Rhodos specifică clar utilizarea lui ca mijloc de criptare.
O descriere a modului de operare este dată de Plutarh (50-120 A.D.).

Avantaj: rapid; nu comportă erori de transmitere.

Sistemul *Skitala*

Permite realizarea unui sistem de criptare cu permutări.
Spartanii foloseau skitala (începând cu sec. V î.H.) în timpul campaniilor militare.
Menționat de poetul grec Archilochus (sec. VII î.H).
La mijlocul secolului III î.H. Apollonius din Rhodos specifică clar utilizarea lui ca mijloc de criptare.
O descriere a modului de operare este dată de Plutarh (50-120 A.D.).

Avantaj: rapid; nu comportă erori de transmitere.
Dezavantaj: ușor de spart.



Exemplu

O skitala ale cărei dimensiuni permite scrierea a 4 *rânduri, cu* 5 *caractere pe fiecare rând.*

VINE MAINE LA INTALNIRE

Exemplu

O skitala ale cărei dimensiuni permite scrierea a 4 *rânduri, cu* 5 *caractere pe fiecare rând.*

VINE MAINE LA INTALNIRE

Ignorând spațiile, mesajul va apare scris sub forma:

	V	*I*	*N*	*E*	*M*	
	A	*I*	*N*	*E*	*L*	
	A	*I*	*N*	*T*	*A*	
	L	*N*	*I*	*R*	*E*	

Exemplu

O skitala ale cărei dimensiuni permite scrierea a 4 *rânduri, cu* 5 *caractere pe fiecare rând.*

VINE MAINE LA INTALNIRE

Ignorând spațiile, mesajul va apare scris sub forma:

	V	*I*	*N*	*E*	*M*	
	A	*I*	*N*	*E*	*L*	
	A	*I*	*N*	*T*	*A*	
	L	*N*	*I*	*R*	*E*	

După derulare, mesajul scris pe banda de hârtie este:

VAALIIINNNNIOETRMLAE.

Exemplu

O skitala ale cărei dimensiuni permite scrierea a 4 *rânduri, cu* 5 *caractere pe fiecare rând.*

VINE MAINE LA INTALNIRE

Ignorând spațiile, mesajul va apare scris sub forma:

	V	*I*	*N*	*E*	*M*	
	A	*I*	*N*	*E*	*L*	
	A	*I*	*N*	*T*	*A*	
	L	*N*	*I*	*R*	*E*	

După derulare, mesajul scris pe banda de hârtie este:

VAALIIINNNNIOETRMLAE.

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

Criptanaliza

Se iau pe rând valorile $n = 2, 3, 4, \ldots$.

Criptanaliza

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

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

care ulterior se concatenează.

Criptanaliza

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

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

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

Cilindrul Jefferson

Thomas Jefferson (primul secretar de Stat al Statelor Unite) a inventat un aparat de criptat numit *roată de criptare*, folosit pentru securitatea corespondenței cu aliații.

Thomas Jefferson a folosit acest aparat în perioada 1790 – 1802, după care se pare că ideea s-a pierdut.

Descriere

Un cilindru Jefferson este format din n discuri de dimensiuni egale (inițial $n = 26$ sau $n = 36$) așezate 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.

La criptare, textul clar se împarte în blocuri de n caractere.

La criptare, textul clar se împarte în blocuri de n caractere.
Fiecare astfel de bloc se scrie pe o linie a cilindrului, rotind corespunzător fiecare disc pentru a aduce pe linie caracterul căutat.

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

La criptare, textul clar se împarte în blocuri de n caractere. Fiecare astfel de bloc se scrie pe o linie 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) și apoi se caută printre celelalte 25 linii un text cu semnificație semantică.

La criptare, textul clar se împarte în blocuri de n caractere. Fiecare astfel de bloc se scrie pe o linie 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) și apoi se caută printre celelalte 25 linii un text cu semnificație semantică.

Probabilitatea de a avea un singur astfel de text crește cu numărul de discuri din cilindru.

Dacă textul clar nu are nici o semnificație semantică (s-a folosit o dublă criptare), trebuie convenită apriori o anumită distanță de criptare s ($1 \leq s \leq 25$).

Dacă textul clar nu are nici o semnificație semantică (s-a folosit o dublă criptare), trebuie convenită apriori o anumită distanță de criptare s ($1 \leq s \leq 25$).
Un cilindru cu $n = 10$ discuri poate realiza $10! = 3.628.800$ texte criptate diferite pentru același text clar.

Dacă textul clar nu are nici o semnificație semantică (s-a folosit o dublă criptare), trebuie convenită apriori o anumită distanță de criptare s ($1 \leq s \leq 25$).
Un cilindru cu $n = 10$ discuri poate realiza $10! = 3.628.800$ texte criptate diferite pentru același text clar.

Cilindrul Jefferson realizează o substituție polialfabetică de perioadă n.

Exemplu

	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

Text clar **TREI CULORI**

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 distanța $s = 3$, atunci textul clar

AAAAAAAAAA

va fi criptat cu cilindrul anterior în

ESYMTRHUEE

Dacă se consideră o dublă criptare cu distanța $s = 3$, 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 mașina de criptat $M - 94$, care a fost utilizată până la începutul celui de al doilea război mondial.

Enigma

Prima jumătate a sec. XX este dominată de mașinile de criptat, o combinație între mașinile de scris și sisteme de criptare mecanice bazate pe discuri.

Enigma

Prima jumătate a sec. XX este dominată de mașinile de criptat, o combinație între mașinile de scris și sisteme de criptare mecanice bazate pe discuri.
Cea mai cunoscută a fost mașina germană *Enigma*, proiectată la Berlin în 1918, de inginerul german Arthur Scherbius.

Enigma

Prima jumătate a sec. XX este dominată de mașinile de criptat, o combinație între mașinile de scris și sisteme de criptare mecanice bazate pe discuri.
Cea mai cunoscută a fost mașina germană *Enigma*, proiectată la Berlin în 1918, de inginerul german Arthur Scherbius.

Primul model (A) este prezentat la Congresele Uniunii Poștale Internaționale din 1923 și 1924.
Modele ulterioare sunt folosite în mai multe țări europene și asiatice (Suedia, Olanda, Marea Britanie, Japonia, Italia, Spania, SUA, Polonia, Elveția) în scopuri comerciale, militare sau diplomatice.

Din 1926 începe să fie preluată și de armata germană, care după 1928 își definește propriile modele (G, I, K).

Din 1926 începe să fie preluată și de armata germană, care după 1928 își definește propriile modele (G, I, K).

În total au fost construite circa 100.000 mașini Enigma, din care 40.000 în timpul războiului.

Din 1926 începe să fie preluată și de armata germană, care după 1928 își definește propriile modele (G, I, K).

În total au fost construite circa 100.000 mașini Enigma, din care 40.000 în timpul războiului.
După 1945 aliații au capturat toate mașinile de pe teritoriul german, acestea fiind încă mult timp considerate sigure.

Din 1926 începe să fie preluată și de armata germană, care după 1928 își definește propriile modele (G, I, K).

În total au fost construite circa 100.000 mașini Enigma, din care 40.000 în timpul războiului.
După 1945 aliații au capturat toate mașinile de pe teritoriul german, acestea fiind încă mult timp considerate sigure.

Abia în 1970 apar primele informații despre decriptarea de către aliați a unui mare număr de mesaje criptate prin modelul militar Enigma și transmise prin radio în timpul războiului.

Descriere

O masină Enigma este compusă din:

- *Tastatura*:
  Componentă mecanică formată din:
  - Un pupitru de taste (similar unei mașini de scris);
  - n discuri adiacente, care se rotesc în jurul unui ax.

O masină Enigma este compusă din:

- *Tastatura*:
  Componentă mecanică formată din:
  - Un pupitru de taste (similar unei mașini de scris);
  - n discuri adiacente, care se rotesc în jurul unui ax.
    Pe fiecare disc sunt scrise cele 26 caractere alfabetice (la care uneori se mai adaugă trei caractere speciale);

O masină Enigma este compusă din:

- *Tastatura*:
  Componentă mecanică formată din:
  - Un pupitru de taste (similar unei mașini de scris);
  - n discuri adiacente, care se rotesc în jurul unui ax.
    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 poziții.

- *Circuite electrice*:
  Criptarea se realizează electric.

- *Circuite electrice*:
  Criptarea se realizează electric.
  La apăsarea unei taste se închide un circuit și luminează una sau mai multe lămpi, indicând litera de ieșire.

- *Circuite electrice*:
  Criptarea se realizează electric.
  La apăsarea unei taste se închide un circuit și luminează una sau mai multe lămpi, indicând litera de ieșire.
- *Reflector (Umkehrwalze)*:
  Componentă specifică mașinilor de criptat Enigma, cu scopul de a realiza un sistem de criptare Beaufort.

- *Circuite electrice*:
  Criptarea se realizează electric.
  La apăsarea unei taste se închide un circuit și luminează una sau mai multe lămpi, indicând litera de ieșire.
- *Reflector (Umkehrwalze)*:
  Componentă specifică mașinilor de criptat Enigma, cu scopul de a realiza un sistem de criptare Beaufort.
  Reflectorul este așezat pe ax după ultimul disc (din stânga); el realizează o substituție (fixată), după care reintroduce noul caracter prin discuri în sens invers, dar pe alt drum.

- *Circuite electrice*:
  Criptarea se realizează electric.
  La apăsarea unei taste se închide un circuit și luminează una sau mai multe lămpi, indicând litera de ieșire.
- *Reflector (Umkehrwalze)*:
  Componentă specifică mașinilor de criptat Enigma, cu scopul de a realiza un sistem de criptare Beaufort.
  Reflectorul este așezat pe ax după ultimul disc (din stânga); el realizează o substituție (fixată), după care reintroduce noul caracter prin discuri în sens invers, dar pe alt drum.
  Deci o mașină Enigma cu n discuri va realiza criptarea unui caracter prin $2n + 1$ substituții.

- *Tabela de conexiuni (Steckerbrett)*:
  Poate face conexiuni între perechi de litere, prin intermediul unor cabluri.

- *Tabela de conexiuni (Steckerbrett)*:
  Poate face conexiuni între perechi de litere, prin intermediul unor cabluri.

Introdusă în 1930, asigură un plus de securitate și a fost principalul obstacol în criptanaliză.

Starea inițială a unei mașini Enigma se referă la:

- *Ordinea discurilor (Walzenlage)*: alegerea numărului de discuri și ordinea lor de utilizare;

Starea inițială a unei mașini Enigma se referă la:

- *Ordinea discurilor (Walzenlage)*: alegerea numărului de discuri și ordinea lor de utilizare;
- *Poziția inițială a discurilor*: poziționarea în mod independent a fiecărui disc, diferită pentru fiecare mesaj;

Starea inițială a unei mașini Enigma se referă la:

- *Ordinea discurilor (Walzenlage)*: alegerea numărului de discuri și ordinea lor de utilizare;
- *Poziția inițială a discurilor*: poziționarea în mod independent a fiecărui disc, diferită pentru fiecare mesaj;
- *Inițializarea inelului de caractere (Ringstellung)*: poziționarea alfabetului relativ la primul disc.

Starea inițială a unei mașini Enigma se referă la:

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

Criptare

Enigma criptează fiecare literă după o procedură care poate fi exprimată prin produs de permutări.

Criptare

Enigma criptează fiecare literă după o procedură care poate fi exprimată prin produs de permutări.
Fie o mașină Enigma cu 3 discuri și
- P transformarea tabelei de conexiuni,
- U – reflectorul,
- S, M, D – acțiunile celor 3 discuri (din stânga, mijloc și respectiv dreapta).

Criptare

Enigma criptează fiecare literă după o procedură care poate fi exprimată prin produs de permutări.
Fie o mașină Enigma cu 3 discuri și
- P transformarea tabelei de conexiuni,
- U – reflectorul,
- S, M, D – acțiunile celor 3 discuri (din stânga, mijloc și respectiv dreapta).

Atunci criptarea e poate fi scrisă sub forma:

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

Criptare

Enigma criptează fiecare literă după o procedură care poate fi exprimată prin produs de permutări.
Fie o mașină Enigma cu 3 discuri și
- P transformarea tabelei de conexiuni,
- U – reflectorul,
- S, M, D – acțiunile celor 3 discuri (din stânga, mijloc și 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 rotește cu i poziții, atunci transformarea devine

$$\rho^i D \rho^{-i}$$

where ρ este permutarea ciclică stânga a vectorului $(A, B, \ldots, Z)$. Similar, discurile din mijloc și stânga pot fi reprezentate prin j respectiv k rotiri ale lui M respectiv S.

De exemplu, dacă discul din dreapta se rotește cu i poziții, atunci transformarea devine

$$\rho^i D \rho^{-i}$$

where ρ este permutarea ciclică stânga a vectorului $(A, B, \ldots, Z)$.
Similar, discurile din mijloc și stânga pot fi reprezentate prin j respectiv k rotiri ale lui M respectiv S.
Atunci funcția de criptare este:

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

De exemplu, dacă discul din dreapta se rotește cu i poziții, atunci transformarea devine

$$\rho^i D \rho^{-i}$$

where ρ este permutarea ciclică stânga a vectorului $(A, B, \ldots, Z)$. Similar, discurile din mijloc și stânga pot fi reprezentate prin j respectiv k rotiri ale lui M respectiv S.
Atunci funcția de criptare este:

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

Decriptarea se efectuează după aceeași formulă.

Securitate – Studiu de caz

Fie o mașină Enigma cu 3 discuri.
Numărul de situații inițiale posibile este $26 \cdot 26 \cdot 26 = 17.576$.

Securitate – Studiu de caz

Fie o mașină Enigma cu 3 discuri.
Numărul de situații inițiale posibile este $26 \cdot 26 \cdot 26 = 17.576$.
Cum cele 3 discuri pot fi permutate în 6 moduri, numărul variantelor se ridică la $6 \cdot 17.576 = 105.456$.

Securitate – Studiu de caz

Fie o mașină Enigma cu 3 discuri.
Numărul de situații inițiale posibile este $26 \cdot 26 \cdot 26 = 17.576$.
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.

Securitate – Studiu de caz

Fie o mașină Enigma cu 3 discuri.
Numărul de situații inițiale posibile este $26 \cdot 26 \cdot 26 = 17.576$.
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 și modul de poziționare al inelului de caractere la mecanismul discurilor, care mai ridică ordinul de mărime al variantelor cu aproximativ 10^5.

Securitate – Studiu de caz

Fie o mașină Enigma cu 3 discuri.
Numărul de situații inițiale posibile este $26 \cdot 26 \cdot 26 = 17.576$.
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 și modul de poziționare 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 mașină de criptat a momentului respectiv.

Funcționarea matematică a unei mașini Enigma

- Fiecare disc poate fi reprezentat ca un set de permutări pentru litere – codificate cu valori între 0 și 25; fie $\alpha_1, \alpha_2, \alpha_3$ permutările de pe cele trei discuri (de la dreapta spre stânga).

Funcționarea matematică a unei mașini Enigma

- Fiecare disc poate fi reprezentat ca un set de permutări pentru litere – codificate cu valori între 0 și 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 inițiale de pe cele trei discuri (caracterele situate inițial pe pozițiile accesibile ale discurilor).

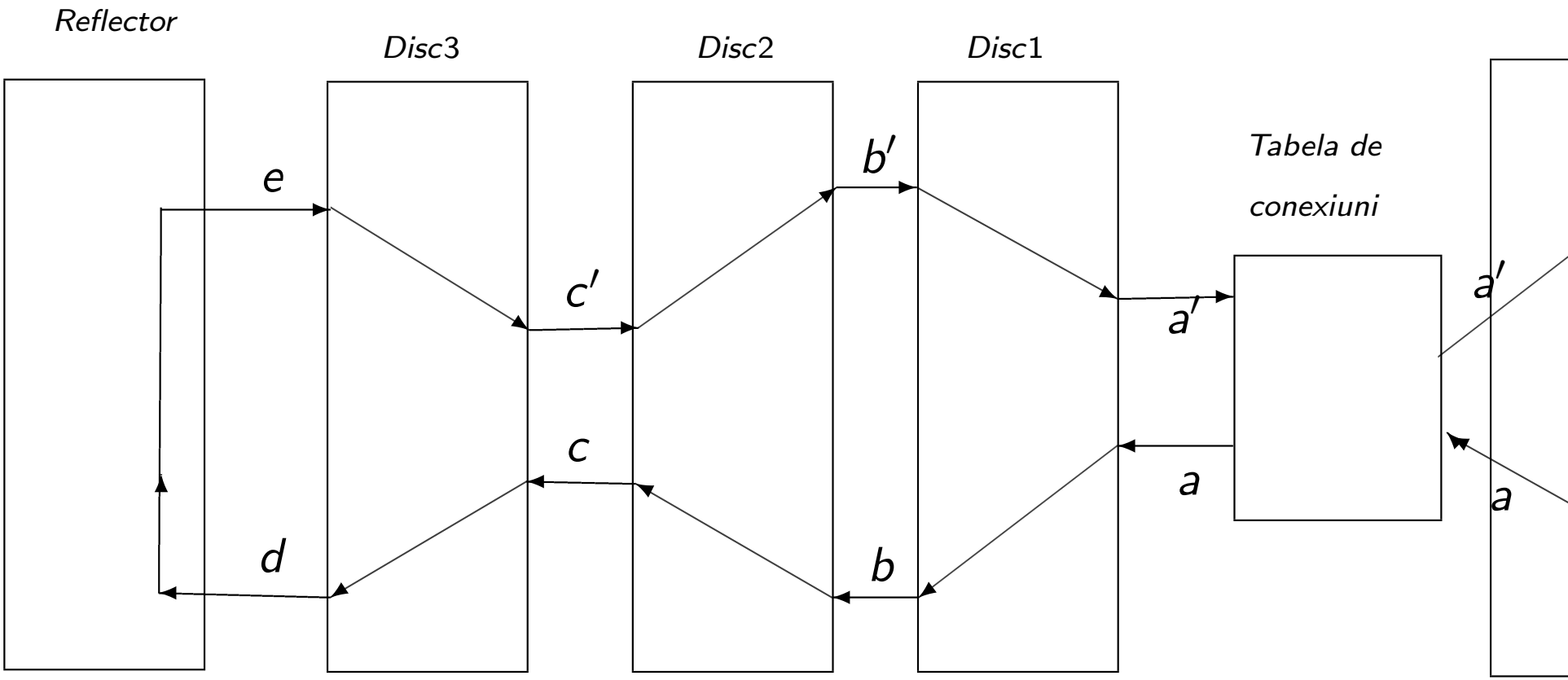
Funcționarea matematică a unei mașini Enigma

- Fiecare disc poate fi reprezentat ca un set de permutări pentru litere – codificate cu valori între 0 și 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 inițiale de pe cele trei discuri (caracterele situate inițial pe pozițiile accesibile ale discurilor).
- Pentru simplificare, ignorăm rolul tabelei de conexiuni.

Funcționarea matematică a unei mașini Enigma

- Fiecare disc poate fi reprezentat ca un set de permutări pentru litere – codificate cu valori între 0 și 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 inițiale de pe cele trei discuri (caracterele situate inițial pe pozițiile accesibile ale discurilor).
- Pentru simplificare, ignorăm rolul tabelei de conexiuni.
- Vom nota cu β substituția reflectorului (reprezentată ca un set de permutări între perechi de caractere).

Un traseu care pleacă de la semnalul de intrare (un caracter din textul clar), trece prin cele trei discuri și reflector și dă ca rezultat caracterul criptat.



Exemplu

Să presupunem că cele permutările celor trei discuri sunt:

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

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

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

Exemplu

Să presupunem că cele permutările celor trei discuri sunt:

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

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

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

Substituția β:

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

Exemplu

Să presupunem că cele permutările celor trei discuri sunt:

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

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

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

Substituția β*:*

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

Deci, cu α_1, 0 *este mutat în* 15, 15 *este mutat în* 6, 25 *este mutat în* 1 *etc.*

Exemplu

Să presupunem că cele permutările celor trei discuri sunt:

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

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

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

Substituția β*:*

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

Deci, cu α_1, 0 *este mutat în* 15, 15 *este mutat în* 6, 25 *este mutat în* 1 *etc.*

Inversele celor trei permutări sunt:

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

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

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

Exemplu

Setările inițiale:

$r_1 = 22$ *(primul rotor are "vizibilă" litera* V*)*, $r_2 = 7,\ r_3 = 12.$

Exemplu

Setările inițiale:

$r_1 = 22$ *(primul rotor are "vizibilă" litera* V*)*, $r_2 = 7,\ r_3 = 12.$

Substituțiile celor trei discuri:

$b = [a + r_1\ (mod\ 26)]^{\alpha_1}, c = [b + r_2\ (mod\ 26)]^{\alpha_2}, d = [c + r_3\ (mod\ 26)]^{\alpha_3},$
($x^{\alpha} = y$*,* y *fiind elementul care urmează lui* x *în permutarea* α*).*

Exemplu

Setările inițiale:
$r_1 = 22$ *(primul rotor are "vizibilă" litera* V*)*, $r_2 = 7,\ r_3 = 12$.

Substituțiile celor trei discuri:
$b = [a + r_1\ (mod\ 26)]^{\alpha_1}, c = [b + r_2\ (mod\ 26)]^{\alpha_2}, d = [c + r_3\ (mod\ 26)]^{\alpha_3},$
($x^{\alpha} = y$*,* y *fiind elementul care urmează lui* x *în permutarea* α*).*

De exemplu $3^{\alpha_1} = 4,\ 8^{\alpha_2} = 0$ *etc.*
Notația permite să scriem $e = d^{\beta}$.

Exemplu

Setările inițiale:
$r_1 = 22$ *(primul rotor are "vizibilă" litera* V*)*, $r_2 = 7,\ r_3 = 12$.

Substituțiile celor trei discuri:
$b = [a + r_1 \ (mod\ 26)]^{\alpha_1}, c = [b + r_2 \ (mod\ 26)]^{\alpha_2}, d = [c + r_3 \ (mod\ 26)]^{\alpha_3}$,
$(x^{\alpha} = y$, y *fiind elementul care urmează lui* x *în permutarea* $\alpha)$.

De exemplu $3^{\alpha_1} = 4,\ 8^{\alpha_2} = 0$ *etc.*
Notația permite să scriem $e = d^{\beta}$.

În continuare, semnalul parcurge cele trei discuri în sens invers:
$c' = e^{\alpha_3^{-1}} - r_3 \ (mod\ 26)$,
$b' = (c')^{\alpha_2^{-1}} - r_2 \ (mod\ 26)$,
$a' = (b')^{\alpha_1^{-1}} - r_1 \ (mod\ 26)$.

Exemplu

După criptarea unui caracter, cele trei discuri sunt resetate după regula:

$r_1 := r_1 + 1\ (mod\ 26)$;

dacă $r_1 = 0$ *atunci* $r_2 := r_2 + 1\ (mod\ 26)$;
dacă $r_2 = 0$, *atunci* $r_3 := r_3 + 1\ (mod\ 26)$.

Exemplu

Să criptăm litera K (cod numeric 10*):*

Exemplu

Să criptăm litera K (cod numeric 10):

$a = 10$;

$b = [a + r_1 \ (mod\ 26)]^{\alpha_1} = [10 + 22 \ (mod\ 26)]^{\alpha_1} = 6^{\alpha_1} = 10$;

$c = [b + r_2 \ (mod\ 26)]^{\alpha_2} = [10 + 7 \ (mod\ 26)]^{\alpha_2} = 17^{\alpha_2} = 22$;

$d = [c + r_3 \ (mod\ 26)]^{\alpha_3} = [22 + 12 \ (mod\ 26)]^{\alpha_3} = 8^{\alpha_3} = 21$.

Exemplu

Să criptăm litera K (cod numeric 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 $e = d^{\beta} = 21^{\beta} = 23$.

Exemplu

Să criptăm litera K (cod numeric 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 $e = d^{\beta} = 21^{\beta} = 23.$

Apoi se parcurg cele trei discuri în sens invers:

$c' = e^{\alpha_3^{-1}} - r_3\ (mod\ 26) = 23^{\alpha_3^{-1}} - 12\ (mod\ 26) = 18 - 12\ (mod\ 26) = 6;$

$b' = (c')^{\alpha_2^{-1}} - r_2\ (mod\ 26) = 6^{\alpha_2^{-1}} - 7\ (mod\ 26) = 4 - 7\ (mod\ 26) = 23;$

$a' = (b')^{\alpha_1^{-1}} - r_1\ (mod\ 26) = 23^{\alpha_1^{-1}} - 22\ (mod\ 26) = 4 - 22 = 8.$

Exemplu

Să criptăm litera K (cod numeric 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 $e = d^{\beta} = 21^{\beta} = 23$.

Apoi se parcurg cele trei discuri în sens invers:

$c' = e^{\alpha_3^{-1}} - r_3 \ (mod\ 26) = 23^{\alpha_3^{-1}} - 12 \ (mod\ 26) = 18 - 12 \ (mod\ 26) = 6$;

$b' = (c')^{\alpha_2^{-1}} - r_2 \ (mod\ 26) = 6^{\alpha_2^{-1}} - 7 \ (mod\ 26) = 4 - 7 \ (mod\ 26) = 23$;

$a' = (b')^{\alpha_1^{-1}} - r_1 \ (mod\ 26) = 23^{\alpha_1^{-1}} - 22 \ (mod\ 26) = 4 - 22 = 8$.

Deci criptarea caracterului K este I (cod 8).

Exemplu

Să criptăm litera K (cod numeric 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 $e = d^{\beta} = 21^{\beta} = 23$.

Apoi se parcurg cele trei discuri în sens invers:

$c' = e^{\alpha_3^{-1}} - r_3 \ (mod\ 26) = 23^{\alpha_3^{-1}} - 12 \ (mod\ 26) = 18 - 12 \ (mod\ 26) = 6$;

$b' = (c')^{\alpha_2^{-1}} - r_2 \ (mod\ 26) = 6^{\alpha_2^{-1}} - 7 \ (mod\ 26) = 4 - 7 \ (mod\ 26) = 23$;

$a' = (b')^{\alpha_1^{-1}} - r_1 \ (mod\ 26) = 23^{\alpha_1^{-1}} - 22 \ (mod\ 26) = 4 - 22 = 8$.

Deci criptarea caracterului K este I (cod 8).

Setările pentru criptarea următorului caracter sunt

$r_1 := 23, \ r_2 = 7, \ r_3 = 12$.

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

$C-36$ este concepută de inginerul suedez Boris Hagelin, la solicitarea armatei americane de a avea o mașină de criptat portabilă, ușor de mânuit, care să poată fi folosită după un instructaj sumar.

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

$C-36$ este concepută de inginerul suedez Boris Hagelin, la solicitarea armatei americane de a avea o mașină de criptat portabilă, ușor de mânuit, care să poată fi folosită după un instructaj sumar.
Este cunoscută și sub numele de $M-209$ C, la bază fiind un model creat de Hagelin în Suedia la sfârșitul anilor $'30$.

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

$C-36$ este concepută de inginerul suedez Boris Hagelin, la solicitarea armatei americane de a avea o mașină de criptat portabilă, ușor de mânuit, care să poată fi folosită după un instructaj sumar.
Este cunoscută și sub numele de $M-209$ C, la bază fiind un model creat de Hagelin în Suedia la sfârșitul anilor '30.

Ea începe să fie produsă – după câteva modificări legate de design – în 1940 și înlocuiește treptat mașina de criptat $M-94$.

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

$C-36$ este concepută de inginerul suedez Boris Hagelin, la solicitarea armatei americane de a avea o mașină de criptat portabilă, ușor de mânuit, care să poată fi folosită după un instructaj sumar.
Este cunoscută și sub numele de $M-209$ C, la bază fiind un model creat de Hagelin în Suedia la sfârșitul anilor '30.

Ea începe să fie produsă – după câteva modificări legate de design – în 1940 și înlocuiește treptat mașina de criptat $M-94$.

Se apreciază că în timpul războiului au fost produse circa 140.000 mașini de criptat $C-36$.

Descriere

HAGELIN M-209 CIPHER MACHINE (GVG / PD)

Definiție

Se numește matrice lug o matrice binară $M_{6\times 27}$ în care fiecare din cele 27 coloane conține cel mult doi de 1.

Exemplu

Fie matricea lug

$$M = \begin{pmatrix} 000100001010001110000000001 \\ 100010001001100010010010100 \\ 000000000000000000000000000 \\ 001100010100001001000111111 \\ 001010000001000100100000000 \\ 000000010010010000010001000 \end{pmatrix}$$

Fie v un vector binar de dimensiune 6.

Fie v un vector binar de dimensiune 6.
Atunci $c \cdot M$ este un vector cu 27 componente având elemente din mulțimea $\{0, 1, 2\}$.

Fie v un vector binar de dimensiune 6.
Atunci $c \cdot M$ este un vector cu 27 componente având elemente din mulțimea $\{0, 1, 2\}$.

Numărul de elemente nenule din $v \cdot M$ se numește *ponderea lui v în raport cu M*.

O *configurație de început* se obține prin așezarea unul sub altul (aliniați la stânga) a 6 șase vectori binari de lungimi $17, 19, 21, 23, 25, 26$.

Exemplu

Structura

0110001000000110
0111110000000000000
0010000010000000000
0000000000100100010001
1010000000000000000000000
1100000000000010001000001

formează o posibilă configurație de început.

Exemplu

Structura

0110001000000110
0111110000000000000
0010000010000000000000
0000000000100100010001
1010000000000000000000000
1100000000000010001000001

formează o posibilă configurație de început.

Spre deosebire de matricea lug, la configurația de început nu există restricții privind numărul de 1.

Se pot genera o infinitate de vectori de dimensiune 6 în felul următor:

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

Se pot genera o infinitate de vectori de dimensiune 6 în felul următor:

1. Primii 17 vectori sunt coloanele complete ale configurației 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 mașinii $C-36$.

Pe baza acestor elemente se poate descrie sistemul de criptare al mașinii $C-36$.
Folosim codificarea numerică a literelor: $A-0$ până la $Z-25$; toate calculele sunt modulo 26.

Pe baza acestor elemente se poate descrie sistemul de criptare al mașinii $C-36$.
Folosim codificarea numerică a literelor: $A-0$ până la $Z-25$; toate calculele sunt modulo 26.
Fie x codul celui de-al i-lea caracter din textul clar și h ponderea celui de-al i-lea vector generat de configurația de început în raport cu matricea *lug*.
Atunci

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

Exemplu

Text clar

NU PUTEM REUSI DECAT IMPREUNA

Exemplu

Text clar

NU PUTEM REUSI DECAT IMPREUNA

Matricea lug și configurația de început sunt cele anterioare.

Exemplu

Text clar

NU PUTEM REUSI DECAT IMPREUNA

Matricea lug și configurația de început sunt cele anterioare.

Codificarea numerică a textului:

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.

Exemplu

Text clar

NU PUTEM REUSI DECAT IMPREUNA

Matricea lug și configurația de început sunt cele anterioare.

Codificarea numerică a textului:

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.

Se calculează ponderile primilor 25 vectori și se formează tabela:

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*	

Exemplu

Text clar

NU PUTEM REUSI DECAT IMPREUNA

Matricea lug și configurația de început sunt cele anterioare.

Codificarea numerică a textului:

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.

Se calculează ponderile primilor 25 vectori și se formează tabela:

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

Decriptare

Ecuația de decriptare este identică cu cea de criptare:

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

Decriptare

Ecuația 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 și mașina $C-36$ poate fi folosită atât pentru criptare cât și pentru decriptare.

Decriptare

Ecuația 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 și mașina $C-36$ poate fi folosită atât pentru criptare cât și pentru decriptare.
Deoarece liniile din configurația de început au lungimi numere prime între ele, vectorii generați încep să se repete sigur după

$$17 \cdot 19 \cdot 21 \cdot 23 \cdot 25 \cdot 26 = 101.405.850$$

pași; deci cuvântul cheie poate fi considerat mai lung decât orice text clar.

Securitate

Mașina de criptat $M - 209$ nu rezista la un atac cu text clar ales; de aceea în 1943 criptanaliștii germani puteau decripta mesajele.

Securitate

Mașina de criptat $M - 209$ nu rezista la un atac cu text clar ales; de aceea în 1943 criptanaliștii germani puteau decripta mesajele. Totuși – din punct de vedere militar tactic – ea a fost considerată perfect adaptată necesităților și a fost folosită de armata americană până după războiul din Coreea (1953 – 1956).

Securitate

Mașina de criptat $M-209$ nu rezista la un atac cu text clar ales; de aceea în 1943 criptanaliștii germani puteau decripta mesajele. Totuși – din punct de vedere militar tactic – ea a fost considerată perfect adaptată necesităților și a fost folosită de armata americană până după războiul din Coreea (1953 – 1956).

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

Mulțumesc pentru atenție !