Capitolul 2

Sisteme simetrice de criptare

În general, sistemele de criptare clasice se numesc şi *sisteme simetrice*. Motivul este acela că odată cu aflarea cheii de criptare e_K, cheia de decriptare d_K se obţine imediat, fiind funcţia inversă.

Sistemele de criptare simetrice se împart în două clase mari: *cifruri de permutare* şi *cifruri de substituţie*.

2.1 Cifruri de permutare

La aceste sisteme de criptare, textul clar se împarte în blocuri de n ($n \geq 2$) caractere, după care fiecărui bloc i se aplică o permutare $\pi \in S_n$ (mulţimea permutărilor de n elemente). Elementele n şi π sunt fixate. π este cheia de criptare, iar π^{-1} va fi cheia de decriptare.

Exemplul 2.1. *Să presupunem că avem cheia de criptare* $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. *Atunci un text clar, de exemplu FLOARE ALBASTRA se împarte în grupuri de câte trei caractere (s-a considerat şi caracterul spaţiu, notat _)*

FLO ARE _AL BAS TRA

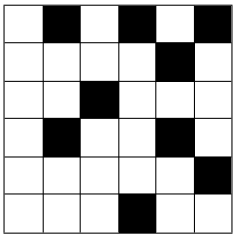
Textul criptat va fi

LFO RAE A_L ABS RTA

sau – eliminând grupările, LFORAEA LABSRTA.

Exemplul 2.2. *Un sistem celebru de criptare cu permutări este sistemul Richelieu (prezentat şi în literatură de Jules Verne, în romanul Mathias Sandorf). Dăm un exemplu de utilizare a unui astfel de sistem.*

Fie cartonul 6×6*, în care zonele haşurate constituie găuri.*



Vrem să criptăm textul

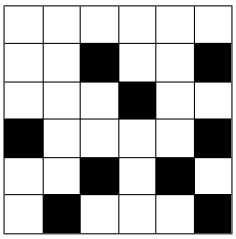
EMINESCU A FOST UN MARE POET NATIONAL

Vom scrie acest text sub forma unui tabel cu şase linii şi şase coloane, astfel:

E	*M*	*I*	*N*	*E*	*S*
C	*U*		*A*		*F*
O	*S*	*T*		*U*	*N*
M	*A*	*R*	*E*		*P*
O	*E*	*T*		*N*	*A*
T	*I*	*O*	*N*	*A*	*L*

Aplicând cartonul peste acest text, vor rămâne vizibile 9 *caractere: MNS TA AN (citite de la stânga la dreapta şi de sus în jos).*

Vom roti acum cartonul cu 90^o *în sensul acelor de ceasornic. El va arăta*



Aşezând acum peste text, rămân vizibile caracterele _F MPTNIL (primul caracter a fost un spaţiu şi l-am marcat cu _ pentru a-l face vizibil).

*La a treia rotire a cartonului se obţine similar textul ICSUEETOA, iar la a patra – EEUAOURO_*

Deci textul criptat este

MNS TA AN F MPTNILICSUEETOAEEUAOURO

Operaţia de decriptare se realizează similar.

Să dăm o definiţie matematică acestei clase de sisteme de criptare.

Definiţia 2.1. *Fie* n *un număr natural nenul. Un cifru de permutare este un sistem* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *unde* $\mathcal{P} = \mathcal{C} = (Z_{26})^n$, $\mathcal{K} = S_n$.

Pentru o cheie (permutare) $\pi \in S_n$

$$e_\pi(a_1 a_2 \dots a_n) = a_{\pi(1)} a_{\pi(2)} \dots a_{\pi(n)}$$

$$d_\pi(b_1 b_2 \dots b_n) = b_{\pi^{-1}(1)} b_{\pi^{-1}(2)} \dots b_{\pi^{-1}(n)}$$

Lema 2.1. *Un cifru de permutare este un sistem de criptare Hill.*

Demonstraţie. Pentru fiecare permutare $\pi \in S_n$ putem construi o matrice de permutare $M_\pi = (m_{i,j})$ definită

$$m_{i,j} = 1 \quad \Longleftrightarrow \quad i = \pi(j)$$

Se verifică uşor faptul că sistemul de criptare Hill cu matricea M_π este echivalent cu un cifru de permutare bazat pe cheia π. Mai mult, $M_\pi^{-1} = M_{\pi^{-1}}$. □

Exemplul 2.3. *Să reluăm Exemplul 2.1. Permutării* $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ *îi corespunde matricea de permutare* $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Operaţia de criptare este imediată. De exemplu, criptarea textului FLO este

$$(5\ 11\ 14) \cdot \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (11\ 5\ 14)$$

adică LFO.

2.2 Cifruri de substituţie

Cifrurile de substituţie sunt cele mai utilizate sisteme de criptare simetrice; ele se întâlnesc şi azi, exemple standard fiind sistemele DES şi AES.

Un astfel de cifru constă în înlocuirea fiecărui caracter din V cu alt caracter (din W). Există două clase mari de cifruri de substituţie: *sisteme monoalfabetice* şi *polialfabetice*.

2.2.1 Sisteme de criptare monoalfabetice

Un astfel de sistem substituie fiecare caracter cu alt caracter – totdeauna acelaşi, indiferent de poziţie. Atunci când cele două alfabete coincid ($V = W$), sistemele monoalfabetice sunt cazuri particulare de cifruri de permutare.

Vom trece în revistă câteva astfel de sisteme.

Sistemul de criptare Cezar

Sistemul de criptare Cezar este un sistem monoalfabetic: odată stabilită cheia de criptare e_K, fiecare caracter cod x se înlocuieşte prin caracterul cod $x + k \ (mod\ 26)$ (a se vedea Capitolul I). Decriptarea se realizează după formula $d_K(x) = x - k \ (mod\ 26)$.

Observaţia 2.1. *În cartea sa "De bello gallico", Cezar aminteşte de un sistem de criptare, fără să dea detalii. Mai tarziu, Suetoniu – în "Viata lui Iuliu Cezar" descrie sistemul. Cezar folosea sistemul înlocuind literele romane cu cele greceşti şi aplica deplasarea* $k = 3$*. Nepotul lui Cezar, împăratul Augustus a folosit acelaşi sistem, bazat pe deplasarea* $k = 1$*. Sistemul Cezar a fost utilizat mult timp. Armata rusă apela frecvent la el în* 1915*, ca înlocuitor pentru sistemele sale proprii de criptare, prea sofisticate la nivelul trupelor de câmp. Un sistem Cezar cu* $k = 13$ *este sistemul ROT*13*, apărut în comunitatea Internet în* 1984 *sau* 1985 *şi implementat pe sistemele UNIX ([45],[47],[60])*

Evident, Cezar este un sistem generat de permutările ciclice din S_{26}. Fiind numai 26 chei posibile, el este extrem de vulnerabil la atacul prin forţă brută. Pentru a-i mări rezistenţa, s-a utilizat şi o variantă, numită *sistem Cezar cu cheie*, definită astfel:

Se consideră un cuvânt (cheie), preferabil cu toate caracterele distincte (în caz contrar, literele identice se folosesc doar la prima apariţie). Acest cuvânt se aşează la începutul alfabetului. După ce se termină, şirul de completează cu literele care nu existau în cuvântul cheie, în ordine alfabetică.

Exemplul 2.4. *Să presupunem că s-a ales cuvântul cheie MARTOR. Scriem*

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

Pentru textul clar se vor folosi caracterele de pe primul rând, iar pentru criptare – caracterele corespondente de pe rândul al doilea. Astfel, STUDENT se criptează în QSUTOJS, ARGINT în MPCEJS etc.

Sistemul Cezar cu cheie rezistă mai bine la atacul cu forţă brută, numărul cheilor fiind acum $card(S_{26}) = 26!$.

Sistemul de criptare afin

Sistemul de criptare afin este o generalizare a sistemului Cezar. Vom avea $\mathcal{P} = \mathcal{C} = Z_{26}$, $\mathcal{K} = \{(a, b) \mid a, b \in Z_{26},\ cmmdc(a, 26) = 1\}$, iar funcţiile de criptare şi decriptare (pentru o cheie $K = (a, b)$) sunt

$$e_K(x) = ax + b\ (mod\ 26), \qquad d_K(y) = a^{-1}y + a^{-1}(26 - b)\ (mod\ 26)$$

Condiţia ca a să fie prim cu 26 asigură existenţa lui a^{-1} în Z_{26}.

Exemplul 2.5. *De exemplu, pentru* $a = 3,\ b = 5$ *funcţia de criptare este* $e_K(x) = 3x + 5$*, care poate fi reprezentată prin tabelul:*

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

sau – scris direct pentru caractere

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

Astfel, textul clar PRIMAVARA TARZIE se criptează în YEDPFQFEF KDECDR.

Deoarece $3^{-1} = 9 \pmod{26}$*, decriptarea se realizează matematic folosind funcţia* $d_K(x) = 9x + 7$ *(sau – practic – inversând cele două linii ale tabelului de mai sus).*

Condiţia $cmmdc(a, 26) = 1$ *asigură de asemenea injectivitatea aplicaţiei* e_K*.*
De exemplu, pentru $e_K(x) = 10x + 1$*, A şi N se transformă ambele în B, iar O nu apare ca imagine în alfabetul substituţiei.*

Să studiem spaţiul cheilor $\mathcal{K}$. Orice cheie $K \in \mathcal{K}$ este determinată complet de valorile întregi (a, b) cu $(a, 26) = 1$. Sunt posibile 12 valori[1] pentru $a : 1, 3, 5, 7, 9, 11, 15, 19, 21, 23, 25$. Pentru b sunt posibile 26 valori, care se iau independent de a, cu singura excepţie $a = 1,\ b = 0$ (care se exclude deoarece nu conduce la nici o criptare). Deci $card(\mathcal{K}) = 311$, număr suficient de mic pentru reuşita unui atac prin forţă brută.

Sistemul de criptare Polybios

Sistemul Cezar nu este cel mai vechi de criptare. Se pare că primul astfel de sistem a fost Polybios (istoric grec mort cu 30 ani înaintea naşterii lui Cezar). Iniţial acesta a fost doar un sistem maritim de semnalizare cu torţe; ulterior i s-a dat o semnificaţie criptografică.

Să considerăm alfabetul latin, din care eliminam o literă de frecvenţă cât mai redusă[2]; fie aceasta W. Cele 25 litere rămase le aşezăm într-un pătrat 5×5 (numit careu Polybios) în felul următor:

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

În operaţia de criptare, fiecare caracter a va fi reprezentat printr-o pereche $(x, y) \quad (x, y \in \{A, B, C, D, E\})$ care dau linia respectiv coloana pe care se află a.

Astfel, textul clar MERGEM ACASA este criptat în

CCAEDCBBAECCAAACAADDAA.

Deci sistemul de criptare Polybios este o substituţie monoalfabetică cu alfabetul $W = \{AA, AB, AC, \ldots, EE\}$ de 25 caractere.

Sunt diverse variante ale sistemului Polybios. Astfel, dacă se folosesc drept coordonate cifrele $1, 2, 3, 4, 5$ în loc de A, B, C, D, E, sistemul a fost folosit în penitenciarele ruseşti[3], iar ulterior de către prizonierii americani din Vietnam. Este foarte simplu de învăţat şi poate fi aplicat folosind diverse semne drept coordonate (cifre, puncte, figuri, bătăi

[1] Pentru un număr dat n există $\phi(n)$ numere mai mici decât n şi prime cu n, unde *phi* este funcţia Euler. În particular $\phi(26) = 12$.

[2] În limba engleză litera eliminată este de obicei J.

[3] Alfabetul cirilic are 33 litere, deci în acest caz s-a utilizat un careu 6×6.

de tobă etc). A fost utilizat de asemenea în cadrul altor sisteme de criptare, cum ar fi sistemul nihilist, cifrul ADFGVX (utilizat de armata germană în primul război mondial) sau sistemul Bifid, inventat de Dellastell în 1901 (pentru detalii, se vedea [61]).

Sistemul cavalerilor de Malta

Ordinul cavalerilor de Malta folosea un sistem de criptare monoalfabetic bazat pe stilizarea unei cruci. Astfel, să considerăm careurile:

$A:$	$B:$	$C:$
$D:$	$E:$	$F:$
$G:$	$H:$	$I:$

$J.$	$K.$	$L.$
$M.$	$N.$	$O.$
$P.$	$Q.$	$R.$

S	T	U
V	W	X
Y	Z	

Liniile care încadrează fiecare caracter (inclusiv spaţiul), împreună cu punctele (două, unul sau zero) indică substituţia caracterului respectiv. Astfel, textul clar DUPA DOUAZECI DE ANI se criptează în

2.2.2 Criptanaliza sistemelor de criptare monoalfabetice

Punctul slab al sistemelor de criptare monoalfabetice constă în frecvenţa de apariţie a caracterelor în text. Dacă un text criptat este suficient de lung şi se cunoaşte limba în care este scris textul clar, sistemul poate fi spart printr-un atac bazat pe frecvenţa apariţiei literelor într-o limbă.

Sunt construite diverse structuri de ordine relative la frecvenţa apariţiei literelor în fiecare limbă europeană. De obicei, cu cât un text criptat este mai lung, cu atât frecvenţa literelor folosite se apropie de această ordonare generală. O comparare între cele două relaţii de ordine (cea a caracterelor din textul criptat şi cea a lterelor din alfabetul limbii curente) conduce la realizarea câtorva corespondenţe (literă text clar – literă text criptat), ceea ce stabileşte în mod univoc cheia de criptare. Pentru sistemul Cezar este suficientă stabilirea unei singure perechi; pentru sistemul afin trebuiesc două perechi etc.

Pentru limba română, un tabel al literelor cele mai frecvent întâlnite este

Literă	Frecvenţă
A	$13,04\ \%$
I	$12,89\ \%$
E	$11,75\ \%$
R	$7,39\ \%$
T	$6,62\ \%$
N	$6,44\ \%$
U	$6,44\ \%$
S	$5,50\ \%$
C	$5,47\ \%$

Literă	Frecvenţă
L	$4,58\ \%$
O	$3,85\ \%$
D	$3,68\ \%$
M	$3,33\ \%$
P	$2,91\ \%$
F	$1,50\ \%$
V	$1,26\%$

(restul caracterelor au o în mod normal o frecvenţă de apariţie sub 1 %).

Exemplul 2.6. *Să considerăm că s-a interceptat următorul text, criptat cu un sistem monoalfabetic (nu se ştie exact ce sistem a fost utilizat).*

```
lqakc sp gcxk aca pcmgqb kq kxc pkersmpqsb vk vsmgxkbc mkacpc tcacpbqlqs
vk cgele cmtxq ms nocxgsb mbxcsp vk exsgk oxcbqsbcbk texbslk spclbk gcxk
cmgqpvkcq bxkgcbexslk gqxbslk xktxknkpbcq tkpbxq mbxcsps qp cfkxbsmakpb
mqtcxcbex vcx lsatkvk pq bxkrqscq mc zsk txkc gqxsems psgs mc mk cmbktbk
mc czlk acxk lqgxq vk lc gkl gq gcxk fkpkcq sp gepbcgb
```

În prima etapă, vom număra de câte ori apare în text fiecare caracter. se obţine tabelul

Caracter	*c*	*k*	*x*	*b*	*s*	*q*	*g*	*p*	*m*	*l*	*e*	*p*	*a*	*v*	*b*	*n*	*o*	*f*	*z*
Frecvenţă	*39*	*38*	*27*	*25*	*23*	*20*	*19*	*18*	*18*	*11*	*9*	*8*	*7*	*7*	*2*	*2*	*2*	*2*	*2*

Deci caracterele cele mai frecvente sunt c şi k. Pe de-altă parte, cele mai frecvente caractere din limba română sunt A, I şi E (textul nu este suficient de mare pentru a putea face o distincţie netă). În mod cert, $A \in \{c, k\}$. Sunt patru opţiuni posibile, din care trei se elimină rapid. Rămâne de abordat $c \longleftarrow A$, $k \longleftarrow E$.

Vom nota cu litere mari caracterele din textul clar; prin înlocuirea lui c cu A, a lui k cu E, textul devine

```
lqaEA sp gAxE aAa pAmgqb Eq ExA pEersmpqsb vE vsmgxEbA mEaApA tAaApbqlqs
vE Agele Amtxq ms noAxgsb mbxAsp vE exsgE oxAbqsbAbE texbslE spAlbE gAxE
AmgqpvEAq bxEgAbexslk gqxbslE xEtxEnEpbAq tEpbxq mbxAsps qp AfExbsmaEpb
mqtAxAbex vAx lsatEvE pq bxErqsAq mA zsE txEA gqxsems psgs mA mE AmbEtbE
mA AzlE aAxE lqgxq vE lA gEs gq gAxE fEpEAq sp gepbAgb
```

*Cuvântul ExA de pe primul rând are caracterul din mijloc (x) de frecvenţă ridicată (*27 *apariţii); deci el trebuie să corespundă unei litere frecvente din limba română şi – în plus – să aibă semnificaţie semantică. Concluzie: acest cuvânt este ERA. Deci $x \longleftarrow R$. Facem substituţia şi se obţine textul*

```
lqaEA sp gARE aAa pAmgqb Eq ERA pEersmpqsb vE vsmgREbA mEaApA tAaApbqlqs
vE Agele AmtRq ms noARgsb mbRAsp vE eRsgE oRAbqsbAbE teRbslE spAlbE gARE
AmgqpvEAq bREgAbeRsleR gqRbslE REtREnEpbAq tEpbRq mbRAsps qp AfERbsmaEpb
mqtARAbeR vAR lsatEvE pq bRErqsAq mA zsE tREA gqRsems psgs mA mE AmbEtbE
mA AzlE aARE lqgRq vE lA gEs gq gARE fEpEAq sp gepbAgb
```

În acest text, cuvântul REtREnEpbAq are corespondent în limba română numai pe $REPREZENTA\{I, M, U\}$. *De aici se obţin decriptările* $t \longleftarrow P$, $n \longleftarrow Z$, $p \longleftarrow N$ *şi* $b \longleftarrow T$ *(pentru ultimul caracter - q, nu facem deocamdată nici o opţiune). Noul text va fi*

```
lqaEA sp gARE aAa NAmgqT Eq ERA NEersmNqsT vE vsmgRETA mEaANA PAaANTqlqs
vE Agele AmPRq ms ZoARgsT mTRAsN vE eRsgE oRATqsTATE PeRTslE sNAlTE gARE
AmgqNvEAq TREgATeRsleR gqRTslE REPREZENTAq PENTRq mTRAsNs qN AfERTsmaENT
mqPARATeR vAR lsaPEvE Nq bRErqsAq mA zsE PREA gqRsems Nsgs mA mE AmTEPTE
mA AzlE aARE lqgRq vE lA gEs gq gARE fENEAq sN geNTAgT
```

Lucrurile încep acum să se simplifice: $PENTRq$ *este corect numai pentru* $q \longleftarrow U$, $AmTEPTE$ *pentru* $m \longleftarrow S$. *Apoi* $NASgUT$ *dă* $g \longleftarrow C$, $SUPARATeR$ *dă* $e \longleftarrow O$, *iar din* $fENEAU$ *deducem* $f \longleftarrow V$. *Făcând aceste înlcuiri, se obţine textul*

```
lUaEA sp CARE MAM NASCUT EU ERA NEOrsSNUsT DE vsSCRETA SEaANA PAaANTUlUs
DE ACOlO ASPRU Ss ZoARCsT STRAsN vE ORsCE oRATUsTATE PORTslE sNAlTE CARE
ASCUNvEAU TRECATORslOR CURTslE REPREZENTAU PENTRU STRAsNs UN AfERTsSaENT
SUPARATOR vAR lsaPEvE NU bRErqsAU SA zsE PREA CURsOms NsCs SA SE ASTEPTE
mA AzlE aARE lUCRU vE lA CEs CU CARE VENEAU sN CONTACT
```

Ultimele caractere se deduc imediat: $l \longleftarrow L$, $a \longleftarrow M$, $r \longleftarrow B, s \longleftarrow I$, $v \longleftarrow D$. *Textul clar final este:*

```
LUMEA IN CARE MAM NASCUT EU ERA NEOBISNUIT DE DISCRETA SEMANA PAMANTULUI
DE ACOLO ASPRU SI ZGARCIT STRAIN DE ORICE GRATUITATE PORTILE INALTE CARE
ASCUNDEAU TRECATORILOR CURTILE REPREZENTAU PENTRU STRAINI UN AVERTISMENT
SUPARATOR DAR LIMPEDE NU TREBUIAU SA FIE PREA CURIOSI NICI SA SE ASTEPTE
SA AFLE MARE lUCRU DE LA CEI CU CARE VENEAU IN CONTACT
```

(textul provine din romanul "Viaţa ca o coridă" de Octavian Paler).

Evident, dacă se ştia sistemul de criptare (afin, Cezar etc) criptanaliza se simplifică mult.

Pentru alte aplicaţii, oferim tabelele de frecvenţă a literelor pentru principalele limbi europene[4] (am reţinut din fiecare limba numai cele mai frecvente nouă litere):

Engleză	Frecvenţă	Germană	Frecvenţă	Franceză	Frecvenţă	Spaniolă	Frecvenţă
E	12,31 %	*E*	18,46 %	*E*	15,87 %	*E*	13,15 %
T	9,59 %	*N*	11,42 %	*A*	9,42 %	*A*	12,69 %
A	8,05 %	*I*	8,02 %	*I*	8,41 %	*O*	9,49 %
O	7,94 %	*R*	7,14 %	*S*	7,90 %	*S*	7,60 %
N	7,19 %	*S*	7,04 %	*T*	7,26 %	*N*	6,95 %
I	7,18 %	*A*	5,38 %	*N*	7,15 %	*R*	6,25 %
S	6,59 %	*T*	5,22%	*R*	6,46 %	*I*	6,25 %
R	6,03 %	*U*	5,01%	*U*	6,24 %	*L*	5,94 %
H	5,14 %	*D*	4,94%	*L*	5,34 %	*D*	5,58 %

[4]Datele statistice pentru toate tabelele – inclusiv limba română – sunt din anul 1994.

Există o situaţie ipotetică în care criptanaliza unui sistem monoalfabetic este imposibilă: atunci când $\mathcal{P}= V^*$ şi nu dispunem de nici o altă informaţie (decât eventual sistemul de criptare). Acest caz corespunde însă unei codificări; adevărata criptare a avut loc atunci când mesajele inteligibile au fost translatate în cuvinte din V^*.

2.2.3 Sisteme de criptare polialfabetice

Diferenţa dintre aceste sisteme de criptare şi cele monoalfabetice constă în faptul că substituţia unui caracter variază în text, în funcţie de diverşi parametri (poziţie, context etc.). Aceasta conduce bineînţeles la un număr mult mai mare de chei posibile. Se consideră că primul sistem de criptare polialfabetic a fost creat de Leon Battista în 1568 ([47]). Unele aplicaţii actuale folosesc încă pentru anumite secţiuni astfel de sisteme de criptare.

Sistemul homofonic

Sistemul de criptare homofonic este un sistem intermediar între sistemele mono şi cele polialfabetice. Principalul lui scop este de a evita atacul prin frecvenţa de apariţie a caracterelor. Se pare că a fost utilizat prima oară în 1401 de către ducele de Mantua.

Fiecărui caracter $a \in \mathcal{P}$ i se asociază o mulţime $H(a) \subset \mathcal{C}$ astfel încât:

1. $H(a) \cap H(b) = \emptyset \iff a \neq b$;
2. Dacă a apare mai frecvent în textele clare, atunci $card((H(a)) \geq card(H(b))$.

Criptarea unui caracter $a \in \mathcal{P}$ se face cu un element ales aleator din $H(a)$. Pentru decriptarea lui $y \in \mathcal{C}$ se caută o mulţime $H(a)$ astfel ca $y \in H(a)$.

Exemplul 2.7. *Să considerăm* $\mathcal{P}= \{a, b\}$ *şi* $H(a) = \{001, 010\}$, $H(b) = \{000, 011, 101, 111\}$. *Pentru criptarea textului ab se poate folosi oricare din secvenţele*

$$001000, 001011, 001101, 001111, 010000, 010011, 010101, 010111.$$

Sistemul homofonic este mult mai rezistent la un atac bazat numai pe textul criptat, dar cedează uşor la un atac cu text clar ales.

Sistemul de criptare Playfair

Sistemul a fost inventat 1854 de Sir Charles Wheatstone. Cel care îl promovează şi îl susţine pentru a fi adoptat ca cifru oficial al Marii Britanii este baronul Lyon Playfair de St. Andrews. Guvernul preferă altă variantă, dar acest sistem de criptare capătă numele baronului.

Ideea de bază este următoarea:

Din cele 26 litere ale alfabetului se elimină una de frecvenţă minimă; să spunem Q. Restul literelor se aranjează arbitrar sub forma unui pătrat 5×5. Să exemplificăm sistemul pentru tabloul

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

Acest tabel va forma atât cheia de criptare cât şi cea de decriptare.

Regulile de criptare/decriptare sunt:

- Textul clar este separat în blocuri de câte două caractere (ignorând spaţiile). Condiţia este ca nici un bloc să nu conţină aceiaşi literă, iar textul să fie de lungime pară. Aceste deziderate se realizează uşor modificând puţin textul clar (se introduce o literă de frecvenţă mică între cele două litere egale, respectiv ca ultim caracter).

- Fiecare bloc se criptează astfel: dacă cele două litere nu sunt plasate în tabel pe aceeaşi linie sau coloană (de exemplu A şi E), se cercetează colţurile dreptunghiului determinat de cele două litere (în cazul nostru A, F, O, E). Perechea AE este criptată în FO. Ordinea este determinată de ordinea liniilor pe care se află literele din textul clar. Astfel, EA se criptează în OF, SF în ZB etc.

  Dacă cele două litere se găsesc pe aceeaşi linie (coloană), se merge ciclic cu o poziţie la dreapta (respectiv jos). Deci CA se criptează în AX, WX în UG, CA în AX etc.

De exemplu, textul clar *AFARA PLOUA* se criptează în *XHHPPDPEPX*. Se observă că cele patru apariţii ale caracterului A au fost criptate cu X, H, P şi din nou X.

O permutare ciclică a liniilor şi coloanelor tabloului nu modifică criptarea. De exemplu, pătratul

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

obţinut prin deplasarea cu două poziţii spre stânga şi o poziţie în sus, este echivalent cu cel iniţial (ambele asigură aceiaşi cheie de criptare).

Regulile de bază pot fi modificate sau completate după necesităţi. Astfel, se poate adăuga din loc în loc câte o literă falsă (cu frecvenţă foarte redusă, cum ar fi X, Y) care să modifice textul criptat. Pătratul 5×5 poate fi înlocuit cu un dreptunghi 4×6 sau 3×8, cu schimbările corespunzătoare în alegerea literelor care se elimină.

Pentru a păstra cheia în siguranţă, se recomandă memorarea acesteia. Cum o astfel de cheie este extrem de greu de memorat, se foloseşte un cuvânt cheie sau o propoziţie cu toate literele distincte. Acesta cuvânt este scris la începutul tabloului. Spaţiile rămase sunt completate cu restul literelor alfabetului, scrise în ordinea apariţiei lor[5].

[5]În definiţia iniţială a sistemului, Wheatstone pleca de la cuvântul *Holmes*.

Astfel, în preajma primului război mondial, armata română folosea un dreptunghi 3×8 din care lipseau literele Q şi K. Cuvântul cheie era $ROMANESC$. Un astfel de tablou putea avea de exemplu forma

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

Ca şi sistemul anterior, *Playfair* rezistă la atacuri bazate pe frecvenţa apariţiei, dar nu şi la cele prin text clar ales.

Implementări actuale folosesc reprezentarea binară a literelor şi fac un pas suplimentar: după ce s-a obţinut o pereche criptată, aceasta se combină printr-un XOR (adunare modulo 2) cu perechea criptată anterior.

O variantă a sistemului de criptare Palyfair este *Playfair dublu*, sistem folosit de Germania în al doilea război mondial. Regulile sunt următoarele:

1. Se folosesc două careuri 5×5 alipite.
2. Textul clar se scrie pe două rânduri (completând eventual ultimul rând cu un caracter de frecvenţă mică). Fiecare coloană va furniza o pereche de două litere.
3. Intr-o pereche de litere (X, Y), X este un element din primul careu, iar Y – un element din al doilea careu.
4. Dacă X şi Y sunt vârfurile unui dreptunghi, se ia ca rezultat perechea formată din celelalte două vârfuri. Dacă X şi Y se află pe aceeaşi linie, se iau următoarele caractere (din fiecare careu) – similar sistemului Playfair simplu. Fie (Z, U) perechea obţinută (Z este din al doilea careu, iar U – din primul careu).
5. Se consideră perechea (U, Z) şi se reia pasul (4), obţinându-se în final textul criptat (P, Q).

Exemplul 2.8. *Să considerăm careurile Playfair definite de cuvintele ROMANESC şi respectiv PREDOMINANT (s-a eliminat litera K):*

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

Să criptăm textul clar

DOAR O VORBA SA ITI SPUN

În prima fază, el va fi scris pe două linii (Q este caracter de completare):

$$\begin{array}{cccccccccc} D & O & A & R & O & V & O & R & B & A \\ S & A & I & T & I & S & P & U & N & Q \end{array}$$

Fiecare pereche de litere este criptată în două etape:

$DS \longrightarrow AU \longrightarrow OT$, $OA \longrightarrow DS \longrightarrow AU$, $AI \longrightarrow RB \longrightarrow PF$,
$RT \longrightarrow OE \longrightarrow DM$, $OI \longrightarrow RS \longrightarrow DL$, $VS \longrightarrow YL \longrightarrow WT$,
$OP \longrightarrow RM \longrightarrow PE$, $RU \longrightarrow OL \longrightarrow RP$, $BN \longrightarrow AD \longrightarrow ON$,
$AQ \longrightarrow ET \longrightarrow MS$.

Mesajul criptat este deci

$$OAPDDWPROMTUFMLTEPNS$$

Sistemul Playfair dublu asigură o securitate sporită – comparativ cu cel simplu. Motivul: sunt folosite două careuri (în loc de unul), plus un parametru suplimentar (lungimea textului clar).

Sistemul de criptare Vigenere

Numele sistemului[6] vine de la baronul francez Blaise de Vigenere $(1523 - 1596)$ diplomat la curtea regelui Henry III. A fost considerat mult timp unul din cele mai bune sisteme de criptare.

Prezentarea sistemului

Considerăm – ca şi la sistemele anterioare – cele 26 litere ale alfabetului, numerotate de la 0 (pentru A) până la 25 (pentru Z), conform tabelului:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Definim $\mathcal{P} = \mathcal{C} = Z_{26}$, $\mathcal{K} = Z_{26}^{+}$.

O cheie $K \in \mathcal{K}$ este un cuvânt având codificarea numerică $k_0 k_1 \ldots k_{p-1}$.

Fie $\mathbf{a} = a_0 a_1 \ldots a_n$ codificarea textului clar care trebuie transmis. Textul criptat va fi $e_K(\mathbf{a}) = \mathbf{x} = x_0 x_1 \ldots x_n$, unde

$$x_i = a_i + k_{i \ (mod\ p)} \quad (mod\ 26) \qquad (*)$$

Exemplul 2.9. *Să considerăm cuvântul cheie FOCAR; deci $p = 5$ şi $K = 5\ 14\ 2\ 0\ 17$.*

Dacă vrem să criptăm cu această cheie textul clar NU POT VENI AZI, vom proceda astfel:

[6] Sursa [62] indică drept real inventator al sistemului pe Giovan Batista Belaso în 1553.

Codificarea textului este $\mathbf{a} = 13\ 20\ 15\ 14\ 19\ 21\ 4\ 13\ 8\ 0\ 25\ 8$.

Sub fiecare număr din $\mathbf{a}$ *se aşează câte un număr din* K*; când cheia se termină, ea se reia ciclic, până se termină* $\mathbf{a}$*. Deci vom avea*

13	20	15	14	19	21	4	13	8	0	25	8
5	14	2	0	17	5	14	2	0	17	5	14
18	8	17	14	10	0	18	15	8	17	4	22
S	*I*	*R*	*O*	*K*	*A*	*S*	*P*	*I*	*R*	*E*	*W*

Linia a treia conţine suma modulo 26 *a numerelor de pe primele două linii; acesta este textul criptat rezultat.*

Decriptarea se realizează similar, scăzând (modulo 26) din codul caracterului criptat, codul caracterului corespunzător din cheie.

O variantă a sistemul Vigenere este sistemul Beaufort (amiral englez, de asemenea autorul unei scale a vânturilor care îi poartă numele); aici relaţia de criptare ($*$) este înlocuită cu

$$x_i = k_{i\ (mod\ p)} - a_i \pmod{26}, \qquad (i \geq 0)$$

Avantajul sistemului Beaufort constă în faptul că ecuaţia de criptare se aplică şi la decriptare ($a_i = k_{i\ (mod\ p)} - x_i$).

Altă variantă este sistemul *Autoclave*, atribuit matematicianului Cardano (autorul formulelor de rezolvare pentru ecuaţiile de gradul 3 şi 4). Aici cheia se foloseşte o singură dată, la început, după care este utilizat drept cheie textul clar.

Exemplul 2.10. *Să luăm cuvântul cheie COVOR şi textul clar A VENIT TOAMNA. Putem aranja sistemul de criptare sub forma unui tabel (s-au trecut doar caracterele, nu şi codificările lor):*

Text clar:	*A*	*V*	*E*	*N*	*I*	*T*	*T*	*O*	*A*	*M*	*N*	*A*
Cheie:	*C*	*O*	*V*	*O*	*R*	*A*	*V*	*E*	*N*	*I*	*T*	*T*
Text criptat	*C*	*J*	*Z*	*B*	*Z*	*T*	*O*	*S*	*N*	*U*	*G*	*T*

Sistemul Vigenere a fost utilizat secole de-a rândul, fiind considerat ca fiind unul din cele mai sigure sisteme de criptare. În 1917 de exemplu, prestigioasa revistă "Scientific American" îl considera imposibil de atacat. Numai că acest sistem a fost spart de Kasiski încă din 1863 (şi independent de Babbage în 1854).

Criptanaliza sistemului Vigenere

Fie $\mathbf{x} = x_0x_1 \dots x_{n-1}$ textul criptat cu cheia $K = k_0k_1 \dots k_{p-1}$. Putem aranja acest text sub forma unei matrici cu p linii şi $\lceil n/p \rceil$ coloane, astfel

$$\begin{array}{cccc} x_0 & x_p & x_{2p} \dots & \\ x_1 & x_{p+1} & x_{2p+1} & \dots \\ & & \vdots & \\ x_{p-1} & x_{2p-1} & x_{3p-1} & \dots \end{array}$$

Elementele de pe prima linie au fost criptate după formula

$$x_{pr} = a_{pr} + k_0 \ (mod\ 26), \qquad (k \geq 0)$$

adică folosind un sistem Cezar (k_0 fiind o valoare fixată din Z_{26}). În mod similar şi celelalte linii.

Deci, dacă s-ar cunoaşte lungimea p a cheii, problema s-ar reduce la criptanaliza a p texte criptate cu Cezar – sistem de criptare monoalfabetic.

Sunt cunoscute două metode pentru aflarea lungimii cheii: *testul lui Kasiski* şi *indexul de coincidenţe*.

Prima metodă constă în studiul textului criptat şi aflarea de perechi de segmente de cel puţin 3 caractere (această lungime este propusă de Kasiski) identice. Pentru fiecare astfel de pereche, se determină distanţa dintre segmente.

După ce s-au găsit mai multe astfel de distanţe, valoarea lui p va fi cel mai mare divizor comun al lor (sau – eventual un divizor al acestuia).

Exemplul 2.11. *Oscar interceptează următorul text criptat, despre care bănuie că s-a folosit Vigenere:*

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

*Textul este destul de scurt (*146 *litere) şi nu se mai ştie nici un text trimis anterior. Folosind metoda Kasiski, Oscar găseşte secvenţa $QLNCJ$ care apare pe rândul al doilea. Distanţa dintre cele două apariţii este* 27*. De asemenea, apar două cuvinte foarte asemănătoare: $AQLN$ şi $AOLN$, având între ele distanţa* 57*.*

Deci putem bănui că avem de-a face cu un cuvânt cheie de lungime $cmmdc(27, 57) = 3$. Rescriem textul pe coloane, fiecare coloană având trei elemente. Anume:

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

Numărând frecvenţa apariţiei literelor pe fiecare linie, obţinem tabelul

	A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
Linia 1	2	0	6	1	0	1	3	2	2	1	0	0	0	0	3	1	3	2	7	0	0	1	8	0	0	0
Linia 2	0	0	1	2	4	0	3	0	1	3	6	3	0	0	0	0	0	4	0	2	0	6	2	0	1	3
Linia 3	11	0	3	0	3	0	1	0	2	0	0	2	2	3	1	1	0	3	2	3	4	0	0	0	0	1

În limba română, primele litere ca frecvenţă sunt $A-E-I$, aflate la distanţă egală una de alta. Deci vom căuta pe fiecare linie tripletele de litere situate pe poziţiile $(k, k+4, k+8)$ având frecvenţă semnificativ de mare (maximă în cazul unui text lung). Pentru linia 3*, alegerea este simplă: ea este chiar $A-E-I$ (*16 *apariţii din* 49 *posibile), deci o deplasare* 0 *în codul Cezar.*

Pentru prima linie, sunt două posibilităţi: $O-S-W$ *(deplasare* 14*) sau* $S-W-A$ *(deplasare* 18*), ambele cu câte* 18 *apariţii.*

Tot două variante apar şi pentru a doua linie: $C-G-K$ *(deplasare* 2*) cu* 10 *apariţii, sau* $R-V-Z$ *(deplasare* 14*) cu* 13 *apariţii.*

Deplasările dau exact codificările cheii. Deci trebuie luate în considerare patru variante de cuvânt cheie: OCA, ORA, SCA *sau* SRA*. Cum de obicei cuvântul cheie are o semnificaţie semantică (pentru a putea fi reţinut mental uşor), putem presupune că el este* OCA *sau* ORA*.*

O simplă verificare reţine drept cuvânt cheie ORA*, care conduce la decriptarea corectă a textului (spaţiile şi semnele de punctuaţie se pun corespunzător):*

```
PELANGAPLOPIIFARASOTADESEAAMTRECUTMACUNOSTEAUVECINIITOTITUNUMAICUNOSCUT
ACEASTAESTEPRIMASTROFAAUNEINPOEZIICELEBREDEMIHAIEMINESCU
```

A doua metodă de aflare a lungimii cheii de criptare într-un sistem Vigenere se bazează pe un concept definit în 1920 de Wolfe Friedman: *indexul de coincidenţe* ([52]).

Definiţia 2.2. *Dacă* $\mathbf{x} = x_1x_2\ldots x_n$ *este o secvenţă de* n *caractere alfabetice, se numeşte "index de coincidenţe" al lui* $\mathbf{x}$ *probabilitatea ca două caractere din* $\mathbf{x}$*, alese aleator, să fie identice. Această valoare se notează* $I_c(\mathbf{x})$*.*

Să notăm cu f_i frecvenţa de apariţie în $\mathbf{x}$ a caracterului literal codificat i $(0 \le i \le 25)$. Două litere din $\mathbf{x}$ pot fi alese în C_n^2 moduri. Din acestea, sunt $C_{f_i}^2$ moduri ca ambele să aibă aceiaşi codificare i $(0 \le i \le 25)$. De aici se poate deduce formula

$$I_c(\mathbf{x}) = \frac{\sum_{i=0}^{25} C_{f_i}^2}{C_n^2} = \frac{\sum_{i=0}^{25} f_i(f_i-1)}{n(n-1)}$$

Să presupunem că $\mathbf{x}$ este un text în limba română. Din tabelul frecvenţelor de apariţie ale literelor, notând p_i probabilitatea de apariţie a caracterului codificat cu i $(0 \le i \le 25)$, valoarea pe care o putem estima pentru indexul de coincidenţe este

$$I_c(\mathbf{x}) \approx \sum_{i=0}^{25} p_i^2 = 0,0788$$

Motivaţie: Probabilitatea ca două elemente aleatoare să fie ambele egale cu caracterul de cod i este p_i^2 $(0 \le i \le 25)$. Afirmaţia este valabilă pentru orice criptare cu un sistem monoalfabetic.

Să presupunem acum că am aranjat textul criptat $\mathbf{x} = x_0x_1\ldots x_{n-1}$ într-o matrice cu p linii şi $\lceil n/p \rceil$ coloane (unde p este un număr întreg pozitiv arbitrar), astfel

$$\begin{array}{rcccc} \mathbf{x_0} = & x_0 & x_p & x_{2p}\ldots & \\ \mathbf{x_1} = & x_1 & x_{p+1} & x_{2p+1} & \ldots \\ & & \vdots & & \\ \mathbf{x_{p-1}} = & x_{p-1} & x_{2p-1} & x_{3p-1} & \ldots \end{array}$$

Dacă p este chiar lungimea cheii, atunci fiecare valoare $I_c(\mathbf{x_i})$ trebuie să fie apropiată de $0,0788$. În caz contrar, şirul $\mathbf{x_i}$ va arăta mult mai aleator, fiind obţinut prin amestecul unei secvenţe de caractere criptate cu chei diferite. Pentru o secvenţă complet aleatoare, valoarea indexului de coincidenţe este

$$I_c \approx 26\left(\frac{1}{26}\right)^2 = \frac{1}{26} = 0,0384$$

Valorile $0,0788$ şi $0,0384$ vor constitui punctele de extrem pe care le poate lua I_c. Vom lua deci diverse valori pentru p, până vom găsi una care să se apropie cât mai mult de $0,788$ şi nu de $0,384$. Aceea poate fi considerată – cu suficientă siguranţă – că este lungimea cheii.

În etapa a doua, vom încerca să aflăm efectiv cheia $K = k_0k_1 \ldots k_{p-1}$.

Dacă notăm $n_1 = \lfloor n/p \rfloor$ lungimea secvenţei $\mathbf{x_i}$, atunci distribuţia de probabilitate ale celor 26 litere în $\mathbf{x_i}$ este

$$\frac{f_0}{n_1}, \frac{f_1}{n_1}, \ldots, \frac{f_{25}}{n_1}$$

Secvenţa $\mathbf{x_i}$ a fost obţinută printr-o criptare Cezar cu o deplasare k_i. Deci, situaţia ideală este când distribuţia de probabilitate a deplasării

$$\frac{f_{k_i}}{n_1}, \frac{f_{k_i+1 \ (mod\ 26)}}{n_1}, \ldots, \frac{f_{k_i+25 \ (mod\ 26)}}{n_1}$$

este cât mai apropiată de distribuţia de probabilitate $p_0, p_1, \ldots, p_{25}$ a limbii române.

Fie un întreg m $(0 \leq m \leq 25)$; definim expresia

$$F_m = \sum_{i=0}^{25} \frac{p_i \cdot f_{i+m}}{n_1}$$

Dacă $m = k_j$ $(0 \leq j \leq p-1)$, ne putem aştepta ca $F_m \approx \sum_{i=0}^{25} p_i^2 = 0,0788$.

Dacă $m \neq k_j$, atunci F_m va fi semnificativ mai mic decât această valoare. Deci, după cel mult 25 încercări, se poate afla deplasarea k_j şi deci a j-a literă din cheie.

2.3 Exerciţii

2.1. *Folosind atacul prin forţă brută, decriptaţi mesajul WYPTBSJBYZ criptat cu un sistem Cezar.*

2.2. *O cheie K este "auto-cheie" dacă $d_K = e_K$. Găsiţi toate auto-cheile sistemului de criptare Cezar.*

2.3. *Demonstraţi că într-un cifru de permutare, π este o auto-cheie dacă şi numai dacă*

$$(\forall i, j)\ [\pi(i) = j \quad \Longrightarrow \quad \pi(j) = i]$$

Găsiţi toate auto-cheile unui cifru de permutare cu $n = 2, 3, 4, 5, 6$.

2.4. *Considerăm următorul cifru de permutare: Se fixează numerele naturale p, q. Textul clar se împarte în blocuri de câte $p \cdot q$ caractere. Fiecare astfel de bloc se scrie pe liniile unei matrici de p linii şi q coloane. Criptarea blocului se realizează scriind aceste matrici pe coloane.*

De exemplu, pentru $p = 3,\ q = 4$, textul clar MAINI CURATE se scrie

M	A	I	N
I	C	U	R
A	T	E	X

(textul s-a completat cu litera X). Textul criptat va fi MIAACTIUENRX.

Decriptaţi următorul text DJNOUDNAINPAPANONZ criptat într-un mod similar.

2.5. *Să se decripteze mesajul*

N	T	I	N	I	I		I	D	D	N	R	I		R	T	E	E	A	D
U	M	I	I	G	R		A	D	V	O	B	E		M	C	I	I	I	E
Z	S	R	U	A	U		C	M	L	T	A	I		T	U	I	T	N	I
D	A	A	L	E	A		R	A	C	R	I	A		S	Z	T	E	E	E
I	G	P	S	A	D		E	A	P	R	E	Z		S	T	C		A	O
A	E	R	I	D	R		E	D	D	E	I	E		S	E	E	P	E	L

şiind că a fost criptat cu matricea Richelieu definită în Exemplul 2.2.

2.6. *Demonstraţi că funcţia de criptare afină $e_K(x) = ax + b\ (mod\ 26)$ este injectivă dacă şi numai dacă $cmmdc(a, 26) = 1$.*

2.7. *Textul clar este scris peste alfabetul $V = \{a, b, c, d\}$. Se foloseşte un sistem de criptare monoalfabetic dat de regulile $a \longrightarrow bb,\ b \longrightarrow aab,\ c \longrightarrow bab,\ d \longrightarrow a$. Să se arate că funcţia de criptare este injectivă.*

Dar pentru: $a \longrightarrow ab,\ b \longrightarrow ba,\ c \longrightarrow a,\ d \longrightarrow c$?

2.8. *Se definesc două sisteme de criptare cu $\mathcal{P}= \{a, b\}$, $\mathcal{C}= \{c, d\}$ şi regulile*

$a \longrightarrow ccd,\ b \longrightarrow c$ pentru primul sistem,

$a \longrightarrow c,\ b \longrightarrow dcc$ la al doilea sistem.

Ce cuvinte sunt criptate la fel în cele două sisteme ?

2.9. *S-a recepţionat mesajul*

$$ARAU\ RIRU\ ITAA\ URIR\ EESU\ URAP\ IUTE\ IRI$$

Despre el, criptanalistul are următoarele informaţii: s-a folosit un careu de criptare tip Polybios, precum şi cuvântul cheie STROP.

Să se decripteze mesajul.

2.10. *În sistemele de criptare simple, orice cheie de criptare poate fi reprezentată ca o compunere de câteva chei generatoare. La sistemul Cezar, o astfel de cheie este e_1. Arătaţi că la sistemul afin sunt necesare cel putîn două chei generatoare.*

2.11. *Decriptaţi următorul mesaj*

```
TKLCP  OCTLE  TSSZC  XCMEB  CVKMK  CCSBX  KGQBA  CGQPE  MBKCQ  FKGSP
SSBEB  SBQPQ  ACSGQ  PEMGQ  BLCOK  CAQLB  CQGKM  BXCLQ  GKCTX  SFKCA
CBCBV  KVKME  LQAKP  BXXCO  CPBKL  KOKCB  QPQAC  SSPBK  LKM
```

criptat cu un sistem afin.

2.12. *O variantă a sistemului AUTOCLAVE este utilizarea textului criptat (în loc de text clar) după prima aplicare a cheii. La care din cele două variante de AUTOCLAVE este criptanaliza mai uşoară ?*

2.13. *Câte chei are un sistem de criptare afin în care $card(V) = 30,\ 100$ sau 1225 ?*

2.14. *Să presupunem că $K = (5, 21)$ este o cheie într-un sistem de criptare afin peste Z_{29}.*

(a) Exprimaţi funcţia de decriptare sub forma $d_K(y) = ay + b$ unde $a, b \in Z_{29}$;

(b) Arătaţi că $e_K(d_K(x)) = x,\ \forall x \in Z_{29}$.

2.15. *Fie $K = (a, b)$ o cheie într-un sistem afin peste Z_n. Arătaţi că K este auto-cheie dacă şi numai dacă $a^{-1} \equiv a\ (mod\ n)$ şi $b \cdot (a + 1) \equiv 0\ (mod\ n)$.*

Aflaţi toate auto-cheile dintr-un sistem afin peste Z_{15}.

Să presupunem că $n = pq$ unde p şi q sunt numere prime distincte. Arătaţi că numărul auto-cheilor din sistemul afin peste Z_n este $n + p + q + 1$.

2.16. *Fiind dat unn număr întreg n $(n \geq 1)$, să se arate că mulţimea tuturor funcţiilor de criptare Vigenere (definite pentru toate cheile de lungime fixată n) formează o structură algebrică de grup.*

2.17. *Fiind date două sisteme de criptare $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ şi $(\mathcal{P}', \mathcal{C}', \mathcal{K}', \mathcal{E}', \mathcal{D}')$ cu $\mathcal{P}' = \mathcal{C}$, definim "produsul" lor ca fiind sistemul $(\mathcal{P}, \mathcal{C}', \mathcal{K} \times \mathcal{K}', \mathcal{E} \circ \mathcal{E}', \mathcal{D}' \circ \mathcal{D})$, unde criptarea unui text clar $m \in \mathcal{P}$ este $e_{K_2}(e_{K_1}(m))$ $(K_1 \in \mathcal{K},\ K_2 \in \mathcal{K}')$, iar decriptarea unui mesaj $y \in \mathcal{C}'$ este $d_{K_1}(d_{K_2}(y))$.*

Care este produsul a două sisteme de criptare Vigenere cu chei de lungimi diferite ?

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] E. Biham, A. Shamir, *Differential Cryptanalysis of DES - like Cryptosystems*, Journal of Cryptology, vol. 4, 1 (1991), pp. 3-72.

[5] E. Biham, A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, 1993.

[6] E. Biham, A. Shamir, *Differential Cryptanalysis of the Full 16-Round DES*, Proceedings of Crypto92, LNCS 740, Springer-Verlag.

[7] E. Biham, *On Matsuis Linear Cryptanalysis*, Advances in Cryptology - EUROCRYPT 94 (LNCS 950), Springer-Verlag, pp. 341-355, 1995.

[8] A. Biryukov, A. Shamir, D. Wagner, *Real Time Cryptanalysis of* $A5/1$ *on a PC*, Fast Software Encryption - FSE 2000, pp 118.

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

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

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

[12] 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.

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

[14] Cook S., *http* : *//www.claymath.org/millennium/P_vs_NP/Official_Problem_Description.pdf*

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

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

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

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

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

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

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

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

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

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

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

[26] H. M. Heyes, *A Tutorial on Linear and Differential Cryptanalysis.*

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

[28] P. Junod, *On the complexity of Matsuiş attack*, in SAC 01: Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography, pp 199211, London, UK, 2001. Springer-Verlag.

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

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

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

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

[33] Matsui, M, Yamagishi, A. *A new method for known plaintext attack of FEAL cipher*. Advances in Cryptology - EUROCRYPT 1992.

[34] M. Matsui, *Linear Cryptanalysis Method for DES Cipher*, Advances in Cryptology - EUROCRYPT 93, LNCS 765, Springer-Verlag, pp. 386-397, 1994.

[35] M. Matsui, *The first experimental cryptanalysis of the Data Encryption Standard*, in Y.G. Desmedt, editor, Advances in Cryptology - Crypto 4, LNCS 839, SpringerVerlag (1994), 1- 11.

[36] M. Matsui, *New Structure of Block Ciphers with Provable Security against Differential and Linear Cryptalaysis*, Fast Software Encryption, LNCS 1039, Springer-Verlag, 1996, pp. 205-218.

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

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

[39] Menezes A., Oorschot P., Vanstome S., *Handbook of Applied Cryptography*

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

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

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

[43] 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.

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

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

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

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

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

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

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

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

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

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

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

[55] 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.

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

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

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

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

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

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

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

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

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

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

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

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