Capitolul 1

Sisteme de criptare

1.1 Caracteristicile unui sistem de criptare

Criptografia este o componentă a unui domeniu mult mai larg, numit **securitatea informaţiei**. Obiectivele pe care le are în vedere un serviciu de securitate a informaţiei pot fi sumarizate în:

1. *Confidenţialitate (privacy)*: proprietatea de a păstra secretul informaţiei, pentru ca aceasta să fie folosită numai de persoanele autorizate.

2. *Integritatea datelor*: proprietatea de a evita orice modificare (inserare, ştergere, substituţie) neautorizată a informaţiei.

3. *Autentificare*: Proprietatea de a identifica o entitate conform anumitor standarde. Este compusă din

   (a) *Autentificarea unei entităţi*;

   (b) *Autentificarea sursei informaţiei*;

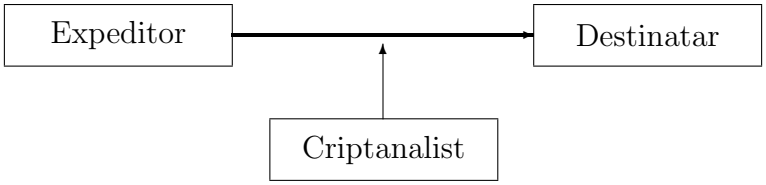
4. *Non - repudierea*: Proprietatea care previne negarea unor evenimente anterioare.

Celelalte obiective legate de securitatea informaţiei (autentificarea mesajelor, semnături, autorizare, validare, controlul accesului, certificare, timestamping, confirmarea recepţiei, anonimitate, revocare) pot fi derivate din acestea.

Definiţia 1.1. *Criptografia este studiul metodelor matematice legate de securitatea informaţiei, capabile să asigure confidenţialitatea, autentificarea şi non-repudierea mesajelor, precum şi integritatea datelor vehiculate ([39].*

Termenul *criptografie* înseamnă *scriere secretă*[1]. Domeniul cuprinde atât operaţia de criptare (cifrare) a unui text, cât şi eventualele încercări de descifrare şi de aflare a cheii de criptare. În unele lucrări, cadrul general de lucru este numit *criptologie*, termenul de *criptografie* desemnând numai operaţia de cifrare şi descifrare legală.

Situaţia generală de care se ocupă criptografia este următoarea:



Expeditorul (personalizat în majoritatea lucrărilor cu apelativul *Alice*) doreşte să trimită destinatarului (numit *Bob*) un mesaj printr-un canal de comunicaţie, canal cu un grad ridicat de nesiguranţă[2]. Această insecuritate o prezintă un adversar criptanalist (*Oscar*) care doreşte – din diverse motive – să cunoască şi – eventual – să modifice conţinutul mesajului, deşi acesta nu îi este destinat.

Această *confidenţialitate* solicitată de *Alice* şi *Bob* se rezolvă de obicei prin rescrierea mesajului sub o formă care să nu poată fi înţeleasă de nici o persoană care l-ar putea intercepta. Transformarea respectivă se numeşte **criptare**.

În general, hackerul *Oscar* poate avea două tipuri de comportament:

- *Pasiv*: el se mulţumeşte să intercepteze mesajele şi să le citească, folosindu-le în scop personal;

- *Activ*: doreşte să modifice mesajele, să le schimbe ordinea sau să introducă propriile sale mesaje, în intenţia de a fi acceptat de *Bob* drept *Alice*. În acest caz, mesajul va trebui să verifice – înafară de condiţia de confidenţialitate – şi pe cea de autenticitate: *Bob* trebuie să fie sigur că mesajul primit a fost de la *Alice*.

  În unele cazuri, problema se poate complica prin faptul că există anumite mesaje pe care *Alice* neagă că îi aparţin, deşi le-a trimis chiar ea. În acest caz trebuie prevăzute anumite protocoale care să întărească proprietăţile de autentificare; proprietăţi care să o silească pe *Alice* să îşi recunoască propriile mesaje (non-repudiere).

În toate aceste scenarii nu există personaje pozitive sau negative. Orice serviciu de criptare/decriptare are şi o secţie de criptanaliză. Se pot da numeroase exemple din istorie care să arate rolul pozitiv al lui *Oscar* în anumite situaţii. În general, într-un

[1] Cuvântul – inventat în 1658 de fizicianul englez Thomas Browne – este format din cuvintele greceşti *cryptos* – ascuns şi *grafie* – scriere.

[2] Canalul de comunicaţie poate suferi şi perturbări de ordin fizic: zgomote, ştergeri, demodulări etc; studiul detectării şi corectării erorilor de de transmitere a informaţiei constituie tema altui domeniu al securităţii informaţiei, numit *Teoria Codurilor*.

triplet (expeditor, destinatar, criptanalist) nimeni nu are încredere în nimeni. Variantele studiate în care *Alice* are încredere în *Bob* sau invers, sunt mult mai simple şi – de aceea – extrem de rare.

Pentru a începe un studiu sistematic al domeniului, să stabilim întâi terminologia folosită uzual:

Un mesaj în forma sa originară este numit *text clar*. Expeditorul rescrie acest mesaj folosind o metodă cunoscută numai de el (eventual şi de destinatar); spunem că el *criptează* (sau *cifrează*) mesajul, obţinând un *text criptat*. Destinatarul primeşte textul cifrat şi îl decriptează ştiind metoda folosită pentru criptare; deci *Alice* şi *Bob* trebuie să stabilească într-o etapă preliminară detaliile modalităţii de criptare şi de decriptare.

Algoritmul care realizează operaţiile descrise se numeşte *sistem de criptare*. Formal,

Definiţia 1.2. *Un sistem de criptare este o structură* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$*, unde:*

- $\mathcal{P}= \{w \mid w \in V^*\}$ *este mulţimea "textelor clare", scrise peste un alfabet nevid* V *(uzual* $V = \{0, 1\}$*).*
- $\mathcal{C}= \{w \mid w \in W^*\}$ *este mulţimea "textelor criptate", scrise peste un alfabet nevid* W *(uzual* $W = V$*).*
- $\mathcal{K}$ *este o mulţime de elemente numite chei.*
- *Fiecare cheie* $K \in \mathcal{K}$ *determină o metodă de criptare* $e_K \in \mathcal{E}$ *şi o metodă de decriptare* $d_K \in \mathcal{D}$*.* $e_K : \mathcal{P} \longrightarrow \mathcal{C}$ *şi* $d_K : \mathcal{C} \longrightarrow \mathcal{P}$ *sunt funcţii cu proprietatea* $d_K(e_K(w)) = w,\ \forall w \in \mathcal{P}$*.*

În general se consideră $\mathcal{C}= \{\alpha \mid \exists a \in \mathcal{P},\ \exists k \in \mathcal{K},\ \alpha = e_K(a)\}$.

Funcţia e_K este evident injectivă (de remarcat că această condiţie de injectivitate nu este obligatorie pentru funcţia de decriptare d_K).

Dacă e_K este bijectivă (şi deci $d_K = e_K^{-1}$), sistemul de criptare se numeşte "*simetric*" sau sistem de criptare *bloc*.

Observaţia 1.1. *Într-un sistem de criptare simetric cu* $\mathcal{P} = \mathcal{C}$*, funcţia de criptare este o permutare. Altfel spus, dacă mulţimea textelor clare coincide cu cea a textelor criptate, o criptare cu un sistem simetric nu face altceva decât o rearanjare (permutare) a textelor.*

Un mesaj de intrare x este descompus în

$$x = x_1 x_2 \dots x_n, \quad x_i \in \mathcal{P}.$$

Apoi fiecare x_i este criptat folosind regula de criptare e_K, specificată de o cheie fixată $K \in \mathcal{K}$.

Deci *Alice* calculează $y_i = e_K(x_i)$ $(1 \le i \le n)$ şi obţine textul criptat

$$y = y_1 y_2 \dots y_n, \quad y_i \in \mathcal{C}$$

pe care îl trimite prin canalul de comunicaţie. *Bob* primeşte mesajul $y = y_1 y_2 \dots y_n$, pe care îl decriptează folosind funcţia d_K : $x_i = d_K(y_i)$ $(1 \le i \le n)$.

Pentru ca un sistem de criptare să fie considerat **bun**, trebuie îndeplinite trei criterii (enunţate de Francis Bacon în sec. $XVII$):

1. Fiind date e_K şi $\alpha \in \mathcal{P}$, este uşor de determinat $e_K(\alpha)$;

2. Fiind date d_K şi $w \in \mathcal{C}$, este uşor de determinat $d_K(w)$;

3. α este imposibil de determinat din w, fără a cunoaşte d_K.

Ultimul criteriu defineşte – sub o formă vagă – ideea de "securitate" a sistemului.

La aceste criterii, Bacon adăuga şi o a patra regulă:

4 Textul criptat trebuie să fie un text banal, fără suspiciuni.

Această ultimă condiţie este utilizată astăzi doar de unele subdomenii al criptografiei, cum ar fi *steganografie* sau *watermarking*.

În termeni de complexitate, prin "uşor" se înţelege folosirea unui algoritm polinomial de grad mic – preferabil algoritm liniar; o problemă se consideră "imposibilă" dacă pentru rezolvarea ei nu se cunosc decât algoritmi de complexitate exponenţială.

Observaţia 1.2. *Întreaga disciplină numită "criptografie" se bazează pe o conjectură notată prescurtat $\mathcal{P} \neq \mathcal{NP}$* [3] *(pentru detalii a se vedea [14]). $\mathcal{P}$ reprezintă clasa problemelor rezolvabile prin algoritmi a căror complexitate este mărginită superior de o funcţie polinomială în lungimea datelor de intrare. Modelul standard de calculabilitate este maşina Turing. $\mathcal{NP}$ este clasa problemelor rezolvabile prin algoritmi nedeterministic polinomiali (care sunt incluşi în algoritmii de complexitate cel puţin exponenţială). Evident, $\mathcal{P} \subseteq \mathcal{NP}$, dar se pare că problema egalităţii este nedecidabilă (în termeni matematici). Oricum, pentru cei interesaţi, site-ul [66] este dedicat unei informări actualizate permanent a rezultatelor şi încercărilor de rezolvare a acestei probleme.*

Exemplul 1.1. *Unul din primele sisteme de criptare cunoscute este sistemul de criptare Cezar. Conform istoricului Suetoniu, el a fost folosit de Cezar în corespondenţa sa.*

Să considerăm alfabetul latin scris, în ordine

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

Fie k un număr întreg din intervalul $[0, 25]$. El se va numi "cheie de criptare". Rescriem alfabetul latin permutat ciclic, începând însă cu litera având numărul de ordine k (litera A are numărul de ordine 0). Această nouă scriere o aşezăm sub prima scriere, astfel (am presupus $k = 2$):

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

[3] Aceasta este prima din cele cinci probleme ale mileniului, pentru rezolvarea cărora se acordă premii de câte un milion dolari.

Dacă Alice are un text clar pe care vrea să-l cripteze cu sistemul Cezar, ea va proceda astfel:

Să presupunem că acest text clar este NIMIC NOU. Alice va aşeza sub fiecare literă a acestui text, litera aflată pe linia a doua din tabelul de sus, astfel:

$$N\ I\ M\ I\ C\ N\ O\ U$$
$$P\ K\ O\ K\ E\ P\ Q\ W$$

Textul criptat obţinut este PKOKEPQW (din motive suplimentare de securitate, spaţiile dintre cuvinte se ignoră de obicei).

La primirea textului, Bob – care ştie că este vorba de sistemul de criptare Cezar – va proceda astfel: el cunoaşte (fiind destinatar legal) cheia de criptare e_k. Cheia sa de decriptare este $d_k = e_{26-k}$. Pe baza ei Bob va putea construi cele două linii ale tabelului, după care va proceda ca Alice: scrie textul criptat pe prima linie, iar pe a doua linie determină literele corespunzătoare, conform tabelului.

În cazul $k = 2$, Bob va folosi drept cheie numărul $e_{26-2} = e_{24}$, iar tabelul (litera 24 corespunde lui Y) este

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

Literele PKOKEPQW determină pe a doua linie textul NIMICNOU.

Să rescriem sistemul Cezar în termenii Definiţiei 1.2. Deoarece textele clare şi cele criptate folosesc alfabetul latin, vom efectua în prima etapă o operaţie de "codificare": asociem literelor numere întregi din intervalul $[0, 25]$*:*

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

În acest fel putem opera matematic pe un inel finit foarte simplu: Z_{26}. Vom avea
$\mathcal{P} = \mathcal{C} = \mathcal{K} = Z_{26}$. Pentru un $K \in \mathcal{K}$ ales arbitrar (şi $m \in \mathcal{P}$, $\alpha \in \mathcal{C}$) ,

$$e_K(m) = m + K \ (mod\ 26)$$

şi

$$d_K(\alpha) = \alpha - K \ (mod\ 26)$$

La nivel conceptual, există două tehnici de construcţie a sistemelor de criptare, definite de Claude Shannon în 1949:

- **Confuzie**: Scopul este de a bloca orice informaţie obţinută prin analize statistice sau redondanţe ale textului criptat.

  O modalitate simplă de a obţine un grad ridicat de confuzie se bazează pe utilizarea de substituţii. De exemplu, în cazul secvenţelor binare, putem complementa unele subsecvenţe folosind anumite formule predefinite.

- **Difuzie**: Această tehnică disipează redondanţa specifică textului clar prin generalizarea ei la tot textul criptat. Practic, o modificare a unui singur caracter din textul clar provoacă multiple modificări în textul criptat. Deci pentru distingerea unei redondanţe din textul clar este necesară studierea unei cantităţi apreciabile de text criptat.

O rafinare a conceptelor de confuzie şi difuzie conduce la ideea de *secret perfect (perfect secrecy)*. Un sistem de criptare are proprietatea de secret perfect dacă din textul criptat, *Oscar* nu poate obţine nici o informaţie referitoare la textul clar.

Această idee poate fi formulată matematic astfel:

Definiţia 1.3. *Un sistem de criptare este perfect secret dacă*

$$Pr[x|y] = Pr[x]$$

pentru orice $x \in \mathcal{P}$, $y \in \mathcal{C}$.

Altfel spus, probabilitatea aposteriori ca textul clar x *să fie criptat în textul recepţionat* y *este identică cu probabilitatea apriori ca textul clar să fie* x.

Următoarea teoremă caracterizează proprietatea de secret perfect pentru majoritatea sistemelor de criptare simetrice:

Teorema 1.1. *Fie* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *un sistem de criptare cu* $card(\mathcal{K}) = card(\mathcal{C}) = card(\mathcal{P})$. *El asigură un secret perfect dacă şi numai dacă toate cheile sunt utilizate cu probabilităţi egale şi* $\forall x \in \mathcal{P}$, $\forall y \in \mathcal{C}$ *există o cheie unică* $K \in \mathcal{K}$ *cu* $y = e_K(x)$.

Demonstraţia acestei teoreme poate fi găsită detaliat în [9].

1.2 Criptanaliza sistemelor de criptare

Definiţia 1.4. *Procesul de determinare a unei chei* K *folosind un text criptat* α *(asociat eventual cu alte informaţii auxiliare) se numeşte "criptanaliză".*

Deci *decriptarea* şi *criptanaliza* au în final acelaşi scop: aflarea textului clar. Diferenţa constă în faptul că în criptanaliză acesta trebuie aflat *fără a şti cheia de decriptare.*

Există o "regulă de aur" a creatorilor de sisteme de criptare:

Nu subestimaţi niciodată pe criptanalist.

care s-a verificat din punct de vedere istoric pentru toate sistemele create până în prezent: acestea sau au fost sparte sau trebuie să se revizuiască periodic pentru a rezista atacurilor permanente ale intruşilor.

Să studiem puţin poziţia unui criptanalist (*Oscar*). Se presupune întotdeauna că el are la dispoziţie facilităţi de calcul excelente, adesea superioare celor de care dispun cei doi parteneri *Alice* şi *Bob*.

În secolul XIX Kirkoff lansează o ipoteză fundamentală (numită *"Principiul lui Kirkoff"*):

Criptanalistul ştie toate detaliile sistemului de criptare folosit, inclusiv algoritmii şi implementările lor.

Ca o consecinţă, securitatea unui sistem de criptare se bazează în totalitate pe cheie.

Definiţia 1.5. *Un atac este un algoritm eficient care – pentru un sistem de criptare fixat – găseşte elemente protejate care pot fi determinate (mult mai) rapid decât au fost specificate de autori.*

Evident, unele atacuri pot să nu contrazică securitatea sistemului ci doar să prevadă anumite slăbiciuni posibile, de care utilizatorii trebuie să ţină cont.

În general, scopul criptografiei este desemnarea de algoritmi (protocoale, scheme, servicii) de criptare siguri (din punct de vedere al complexităţii), în timp ce criptanaliza se concentrează pe construirea de atacuri asupra sistemelor de criptare, având ca scop determinarea cheilor de criptare.

Ulterior, atacurile potenţial reuşite furnizează *criterii de construcţie* a sistemelor de criptare, şi vor face parte implicit din criptografie.

Criteriile de construcţie obţinute dintr-un atac permit realizarea de sisteme de criptare imune (rezistente) la atacul respectiv.

Criptografia încearcă să demonstreze că produsele obţinute sunt sigure, folosind toată informaţia cunoscută despre atacurile posibile.

Criptanaliza examinează cu atenţie toate slăbiciunile (faliile) unui sistem şi încearcă să construiască atacuri bazate pe aceste slăbiciuni, pentru a demonstra că sistemul nu este sigur (şi deci poate fi spart de *Oscar*).

În general este imposibil de demonstrat că un sistem rezistă la orice fel de atac, în timp ce opusul său este totdeauna posibil: este suficient de descris un atac.

Se consideră că metodele de atac (cum ar fi furtul, mituirea, presiuni fizice şi psihice asupra persoanelor implicate în construirea şi utilizarea sistemului de criptare) care nu sunt legate direct de slăbiciunile sistemului de criptare, nu intră în domeniul criptanalizei.

În general un sistem de criptare poate fi *necondiţionat sigur* sau *condiţionat sigur*.

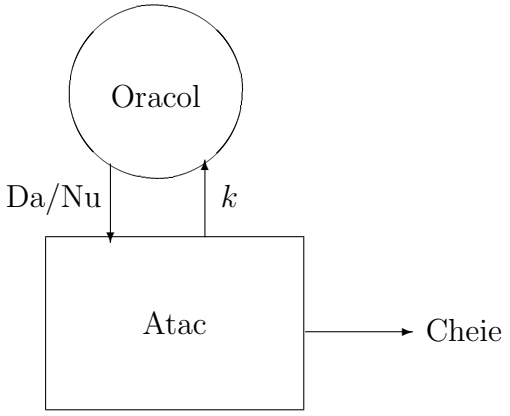
Un sistem necondiţionat sigur este imun la orice tip de atac. În acest caz, securitatea sa depinde de dificultatea de a rezolva problema matematică pe care se bazează construirea cheii (de criptare/decriptare).

În general, un criptanalist este pus în faţa următoarelor situaţii, care îi solicită strategii diverse de urmat:

1. Ştie numai textul criptat w; în acest caz atacurile sunt direct legate de lungimea textului.

   Cel mai simplu atac în acest caz constă în parcurgerea tuturor cheilor posibile şi verificarea textului criptat, până se găseşte cheia corectă. Este atacul prin *forţă brută* şi el reuşeşte totdeauna, pentru că există întotdeauna o cheie în $\mathcal{K}$, care a fost folosită la criptare.

   Un atac prin forţă brută poate fi modelat foarte simplu sub forma unui oracol, care pentru orice cheie $K \in \mathcal{K}$, răspunde dacă este corectă sau nu.



   Principala întrebare care se pune în aceasta situaţie este: dacă încercăm să "ghicim" una din n chei posibile, care este numărul mediu de încercări până găsim cheia ?

   Teorema 1.2. *Pentru a ghici o cheie din n variante posibile sunt necesare în medie $(n+1)/2$ încercări.*

   De exemplu, pentru un sistem de criptare cu $card(\mathcal{K}) = 2^{56}$, se folosesc aproximativ 2^{55} încercări până se găseşte cheia corectă.

   Demonstraţie. Dacă sistemul are n chei posibile, atunci probabilitatea de a ghici corect din prima încercare este $1/n$. Pentru a ghici din două încercări trebuie să fi dat greş cu prima încercare şi apoi – eliminând cheia care nu este corectă – să încercăm altă cheie din restul de $n-1$ chei posibile. Deci probabilitatea de a ghici din două încercări este $\left(1-\frac{1}{n}\right)\frac{1}{n-1} = \frac{1}{n}$. Similar, probabilitatea de a ghici cheia corectă în exact $3, 4, \ldots, n$ încercări este $1/n$.

Numărul mediu de încercări se obţine prin înmulţirea numărului k de încercări cu probabilitatea de ghicire a cheii corecte în k încercări şi apoi sumarea după k. Deci

$$1 \cdot \frac{1}{n} + 2 \cdot \frac{1}{n} \ldots + (n-1) \cdot \frac{1}{n} + n \cdot \frac{1}{n} = \frac{n(n+1)}{2} \cdot \frac{1}{n} = \frac{n+1}{2}$$

□

Deci, în cazul când numărul cheilor posibile este mic (în Exemplul 1.1 sunt numai 26 chei), această cheie se poate afla foarte uşor după un număr mic de încercări. De aceea sunt folosite obligatoriu sisteme de criptare cu $card(\mathcal{K})$ foarte mare. Pentru o cheie care ocupă n biţi sunt necesare în medie 2^{n-1} încercări (dacă nu există nici o informaţie suplimentară). O extindere a lungimii cheii la $n+1$ biţi dublează deci spaţiul de căutare. În momentul de faţă, tehnica de calcul oferă atacuri prin forţă brută eficiente pentru cheile de lungimi mai mici de 128 biţi; aşa că sistemele de criptare actuale folosesc în general chei de 1024 biţi sau chiar mai mult[4].

Atacul prin forţă brută poate fi îmbunătăţit semnificativ cu alte informaţii legate de sistem, informaţii care pot reduce numărul cheilor posibile.

Multe atacuri folosesc diverse strategii pentru a reduce semnificativ spaţiul cheilor posibile, după care se foloseşte atacul prin forţă brută.

2. Ştie cel puţin o pereche de caractere *(text clar, text criptat)*; din cunoaşterea câtorva perechi $(x, e_K(x))$ cu $x \in \mathcal{P}$ *Oscar* va încearca să decripteze întregul text criptat interceptat.

   Exemplul 1.2. *La sistemul de criptare Cezar, o singură pereche $(a, e_K(a))$, dezvăluie imediat cheia şi – implicit duce la decriptare.*

   Exemplul 1.3. *Aceasta a fost situaţia în care s-a aflat orientalistul francez Jean François Champollion, când a descifrat hieroglifele folosind piatra de la Rosetta (vezi [44]).*

3. *Oscar* cunoaşte criptarea unor texte clare selectate de el; este *atacul cu text clar ales*, luat în considerare de majoritatea studiilor de criptanaliză. Această situaţie este adesea superioară celei din cazul precedent; să exemplificăm acest lucru.

   Exemplul 1.4. *Fie sistemul de criptare Hill, creat în* 1929 *de Lester Hill.*

   Definim un număr întreg fixat d ($d \geq 2$). Se construiesc mulţimile

   $$\mathcal{P} = \mathcal{C} = (Z_{26})^d, \quad \mathcal{K} = \{M \mid M \in \mathcal{M}_d(Z_{26}),\ det(M) \neq 0\}.$$

[4] O excepţie o constituie sistemele bazate pe curbe eliptice, datorită aparatului matematic special folosit.

Deci o cheie de criptare este o matrice M pătrată nesingulară de dimensiune d, cu elemente din Z_{26}, iar M^{-1} formează cheia de decriptare.

Textul clar w se împarte în blocuri de lungime d : $w = \alpha_1\alpha_2\ldots\alpha_n$, $|\alpha_i| = d$ (ultimul bloc se completează eventual până ajunge la lungimea d). Textul criptat va fi $x = \beta_1\beta_2\ldots\beta_n$ unde $\beta_i = e_M(\alpha_i) = \alpha_i \cdot M \ (mod\ 26)$, $(1 \le i \le n)$.

Pentru decriptare se foloseşte relaţia $d_M(\beta_i) = \beta_i \cdot M^{-1} \ (mod\ 26)$.

Să luăm de exemplu $d = 2$ şi cheia $M = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$, cu inversa $M^{-1} = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix}$.

Dacă textul clar este $w = FRAC$, vom avea

$$\alpha_1 = (F\ R) = (5\ 17), \qquad \alpha_2 = (A\ C) = (0\ 2)$$

Din relaţiile

$$\beta_1 = \alpha_1 \cdot M \ (mod\ 26) = (5\ 17) \cdot \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} = (23\ 22) = (X\ W)$$

$$\beta_2 = \alpha_2 \cdot M \ (mod\ 26) = (0\ 2) \cdot \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} = (4\ 10) = (E\ K)$$

se obţine textul criptat $x = XWEK$.

Să ne situăm acum pe poziţia lui Oscar: presupunem că am găsit dimensiunea $d = 2$ şi încercăm să aflăm matricea M (sau – echivalent – M^{-1}), ştiind perechea (text clar, text criptat)= $(FRAC,\ XWEG)$.

Deci Oscar se află acum în faţa următoarei probleme: care este matricea $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ cu $a, b, c, d \in \{0, 1, \ldots, 25\}$, astfel ca

$$\begin{pmatrix} 5 & 17 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 23 & 22 \\ 4 & 10 \end{pmatrix}.$$

Pentru a putea afla această matrice, Oscar trebuie să afle inversa lui $A = \begin{pmatrix} 5 & 17 \\ 0 & 2 \end{pmatrix}$.

Cum $det(A) = 10$ şi $cmmdc(10, 26) > 1$, rezultă că $10^{-1}\ (mod\ 26)$ nu există; deci A nu este inversabilă.

Să presupunem acum că Oscar lucrează în ipoteza (3); alege un text clar a cărui matrice este inversabilă şi îi află criptarea.

Fie $BRAD$ acest text clar, a cărui matrice asociată este $A = \begin{pmatrix} 1 & 17 \\ 0 & 3 \end{pmatrix}$.

Oscar solicită criptarea lui $BRAD$ şi primeşte $LKGP$, de matrice $B = \begin{pmatrix} 11 & 10 \\ 6 & 15 \end{pmatrix}$.

Deci el dispune de perechea $(BRAD, LKGP)$.

Oscar determină întâi $A^{-1} = \begin{pmatrix} 1 & 3 \\ 0 & 9 \end{pmatrix}$. *Apoi, din ecuaţia* $A \cdot M = B$, *va găsi soluţia*

$$M = A^{-1} \cdot B = \begin{pmatrix} 1 & 3 \\ 0 & 9 \end{pmatrix} \cdot \begin{pmatrix} 11 & 10 \\ 6 & 15 \end{pmatrix} = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$$

4. Ştie cheia de criptare; acum *Oscar* va cunoaşte cheia e_K şi încearcă să determine d_K înainte de interceptarea mesajelor criptate.

   Aceasta este situaţia tipică sistemelor de criptare cu cheie publică: cheia de criptare e_K este cunoscută public cu mult înainte de a fi folosită pentru criptare. Deci criptanalistul are la dispoziţie destul de mult timp pentru prelucrarea ei şi orice clarificare în perioada când timpul este "ieftin" are o valoare deosebită; după ce se primesc mesaje criptate, timpul devine *scump*, şi el trebuie să fie scurtat cât mai mult.

1.3 Exerciţii

1.1. *Textul clar NUMAR este criptat în "Orice vânt nu bate seara". Să se descrie sistemul de criptare.*

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

1.3. *Să presupunem că Cezar trimite un mesaj criptat unuia din generalii săi, iar acest mesaj este format dintr-o singură literă. Ce puteţi spune despre securitatea mesajului ?*

1.4. *Fie* p *un număr prim. Arătăţi că numărul matricilor* 2×2 *inversabile peste* Z_p *este* $(p^2 - 1)(p^2 - p)$.

1.5. *Câte matrici* 2×2 *sunt inversabile peste* Z_n *pentru* $n = 6,\ 9,\ 26$ *?*

1.6. *Să se cripteze textul clar INAINTE SI LA DREAPTA folosind sistemul de xriptare Hill cu matricea*

$$M = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \qquad \textit{sau} \qquad M = \begin{pmatrix} 11 & 2 & 19 \\ 5 & 23 & 25 \\ 20 & 7 & 1 \end{pmatrix}$$

1.7. *Câte auto-chei sunt într-un sistem de criptare Hill cu* $d = 2$ *?*

1.8. *Determinaţi inversele matricilor (modulo* 26*):*

$$\begin{pmatrix} 2 & 5 \\ 9 & 5 \end{pmatrix}, \quad \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}, \quad \begin{pmatrix} 10 & 5 & 12 \\ 3 & 14 & 21 \\ 8 & 9 & 11 \end{pmatrix}, \quad \begin{pmatrix} 1 & 11 & 12 \\ 4 & 23 & 2 \\ 17 & 15 & 9 \end{pmatrix}$$

1.9. *Textul clar "conversation" este criptat în "HIARRTNUYTUS" folosind un sistem de criptare Hill bazat pe o matrice neinversabilă* $n \times n$*.*

Determinaţi n *şi apoi matricile de criptare şi decriptare.*

1.10. *Fie* n $(n \geq 2)$ *un număr întreg. Un pătrat latin de ordin* n *este un tablou* L *de dimensiune* $n \times n$*, cu elemente din mulţimea* $\{1, 2, \ldots, n\}$*, astfel că fiecare număr apare o singură dată pe fiecare linie şi fiecare coloană din* L*. Arătaţi că el defineşte un sistem de criptare cu* $\mathcal{P} = \mathcal{C} = \mathcal{K}$*, în care criptarea lui* x *cu cheia* k *este* $L(k, x)$*.*

Asigură un astfel de sistem de criptare un secret perfect ?

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