Sisteme generale de criptare

Prof. Dr. Adrian Atanasiu

Universitatea București

February 9, 2011

Caracteristici

1. *Confidențialitate (privacy)*: Proprietatea de a păstra secretul informației, pentru ca aceasta să fie folosită numai de persoanele autorizate.

Caracteristici

1. *Confidențialitate (privacy)*: Proprietatea de a păstra secretul informației, pentru ca aceasta să fie folosită numai de persoanele autorizate.
2. *Integritatea datelor*: Proprietatea de a evita orice modificare (inserare, ștergere, substituție) neautorizată a informației.

Caracteristici

1. *Confidențialitate (privacy)*: Proprietatea de a păstra secretul informației, pentru ca aceasta să fie folosită numai de persoanele autorizate.
2. *Integritatea datelor*: Proprietatea de a evita orice modificare (inserare, ștergere, substituție) neautorizată a informației.
3. *Non - repudiere*: Proprietatea care previne negarea unor evenimente anterioare.

Caracteristici

1. *Confidențialitate (privacy)*: Proprietatea de a păstra secretul informației, pentru ca aceasta să fie folosită numai de persoanele autorizate.
2. *Integritatea datelor*: Proprietatea de a evita orice modificare (inserare, ștergere, substituție) neautorizată a informației.
3. *Non - repudiere*: Proprietatea care previne negarea unor evenimente anterioare.
4. *Autentificare*: Proprietatea de a identifica o entitate conform anumitor standarde.
   Este compusă din
   1. *Autentificarea unei entități*;

Caracteristici

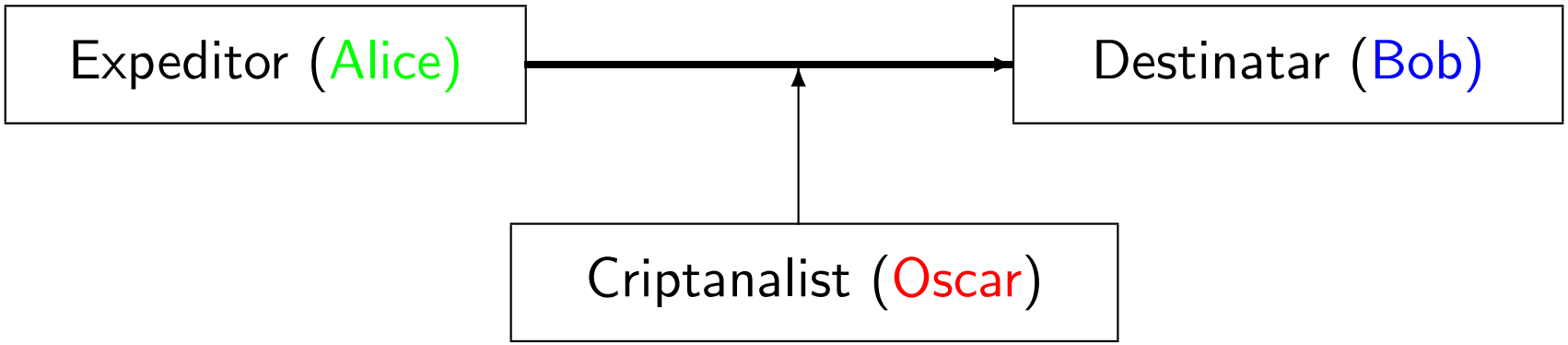
1. *Confidențialitate (privacy)*: Proprietatea de a păstra secretul informației, pentru ca aceasta să fie folosită numai de persoanele autorizate.
2. *Integritatea datelor*: Proprietatea de a evita orice modificare (inserare, ștergere, substituție) neautorizată a informației.
3. *Non - repudiere*: Proprietatea care previne negarea unor evenimente anterioare.
4. *Autentificare*: Proprietatea de a identifica o entitate conform anumitor standarde.
   Este compusă din
   1. *Autentificarea unei entități*;
   2. *Autentificarea sursei informației*.

Definiție

Criptografia este studiul metodelor matematice legate de securitatea informației, capabile să asigure confidențialitatea, autentificarea și non-repudierea mesajelor, precum și integritatea datelor vehiculate.

Cuvântul **criptografie** este inventat în 1658 de fizicianul englez Thomas Browne; este format din cuvintele greceți *cryptos* – ascuns și *grafie* – scriere.

Schema de lucru în criptografie:



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

- **Pasiv**: se mulțumește să intercepteze mesajele și să le citească, folosindu-le în scop personal;

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

- **Pasiv**: se mulțumește să intercepteze mesajele și să le citească, folosindu-le în scop personal;
- **Activ**: dorește să modifice mesajele, să le schimbe ordinea sau să introducă propriile sale mesaje, în intenția de a fi acceptat de *Bob* drept *Alice*.

În acest caz, mesajul va trebui să verifice – înafară de condiția de confidențialitate – și pe cea de autenticitate: *Bob* trebuie să fie sigur că mesajul primit a fost de la *Alice*.

Non-repudiere

În unele cazuri, problema se complică prin faptul că există anumite mesaje pe care *Alice* neagă că îi aparțin, deși le-a trimis chiar ea.

În acest caz trebuie prevăzute anumite protocoale care să întărească proprietățile de autentificare; proprietăți care să o silească pe *Alice* să își recunoască propriile mesaje (non-repudiere).

Terminologie:

Un mesaj în forma sa originară este numit **text clar**.

Expeditorul rescrie acest mesaj folosind o metodă cunoscută numai de el (eventual și de destinatar); spunem că el **criptează** (sau **cifrează**) mesajul, obținând un **text criptat**.

Terminologie:

Un mesaj în forma sa originară este numit **text clar**.

Expeditorul rescrie acest mesaj folosind o metodă cunoscută numai de el (eventual și de destinatar); spunem că el **criptează** (sau **cifrează**) mesajul, obținând un **text criptat**.

Destinatarul primește textul cifrat și îl **descriptează**, știind metoda folosită pentru criptare.

Deci *Alice* și *Bob* trebuie să stabilească într-o etapă preliminară toate detaliile de criptare și de decriptare.

Sistem de criptare:

Definiție

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

$$d_K(e_K(w)) = w, \ \forall w \in \mathcal{P}$$

Sistem de criptare simetric

În general se consideră

$$\mathcal{C} = \{\alpha \mid \exists a \in \mathcal{P},\ \exists k \in \mathcal{K},\ \alpha = e_K(a)\}$$

Funcția e_K este evident injectivă (condiția de injectivitate nu este obligatorie pentru funcția de decriptare d_K).

Sistem de criptare simetric

În general se consideră

$$\mathcal{C} = \{\alpha \mid \exists a \in \mathcal{P},\ \exists k \in \mathcal{K},\ \alpha = e_K(a)\}$$

Funcția e_K este evident injectivă (condiția de injectivitate nu este obligatorie pentru funcția de decriptare d_K).
Dacă e_K este bijectivă (și deci $d_K = e_K^{-1}$), sistemul de criptare se numește "*simetric*" sau sistem de criptare *bloc*.

Blocuri de criptare

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 $K \in \mathcal{K}$.

Blocuri de criptare

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 $y_i = e_K(x_i)$ $(1 \leq i \leq n)$ și obține textul criptat

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

pe care îl trimite prin canalul de comunicație. *Bob* primește mesajul $y = y_1 y_2 \dots y_n$, pe care îl decriptează folosind funcția d_K :

$$x_i = d_K(y_i) \quad (1 \leq i \leq n)$$

Criterii de securitate

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

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

Criterii de securitate

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

1. Fiind date e_K și $\alpha \in \mathcal{P}$, este ușor de determinat $e_K(\alpha)$;
2. Fiind date d_K și $w \in \mathcal{C}$, este ușor de determinat $d_K(w)$;

Criterii de securitate

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

1. Fiind date e_K și $\alpha \in \mathcal{P}$, este ușor de determinat $e_K(\alpha)$;
2. Fiind date d_K și $w \in \mathcal{C}$, este ușor de determinat $d_K(w)$;
3. α este imposibil de determinat din w, fără a cunoaște d_K.

Criterii de securitate

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

1. Fiind date e_K și $\alpha \in \mathcal{P}$, este ușor de determinat $e_K(\alpha)$;
2. Fiind date d_K și $w \in \mathcal{C}$, este ușor de determinat $d_K(w)$;
3. α este imposibil de determinat din w, fără a cunoaște d_K.

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

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

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

$\mathcal{P}$ versus $\mathcal{NP}$

Întreaga disciplină numită "criptografie" se bazează pe conjectura

$$\mathcal{P} \neq \mathcal{NP}.$$

$\mathcal{P}$ reprezintă clasa problemelor rezolvabile prin algoritmi a căror complexitate este mărginită superior de o funcție polinomială în lungimea datelor de intrare.
Modelul standard de calculabilitate este mașina Turing.

$\mathcal{NP}$ este clasa problemelor rezolvabile prin algoritmi nedeterministic polinomiali (incluși în algoritmii de complexitate cel puțin exponențială).

Evident, $\mathcal{P} \subseteq \mathcal{NP}$, dar se pare că problema egalității este nedecidabilă (în termeni matematici).

Cezar

Exemplu

Unul din primele sisteme de criptare cunoscute este sistemul de criptare Cezar.

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 $[0, 25]$.
Rescriem alfabetul latin permutat ciclic, începând însă cu litera având numărul de ordine k (litera A are numărul de ordine 0).

Cezar

Exemplu

Unul din primele sisteme de criptare cunoscute este sistemul de criptare Cezar.

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 $[0, 25]$.
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 așezăm sub prima scriere, astfel (am presupus $k = 2$):

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

continuare

Exemplu

$$NIMIC \;\; NOU \Longrightarrow PKOKEPQW$$

(din motive suplimentare de securitate, spațiile dintre cuvinte se ignoră de obicei).

Bob cunoaște (fiind destinatar legal) cheia de criptare e_k.
Cheia sa de decriptare este $d_k = e_{26-k}$.

continuare

Exemplu

$$NIMIC\ \ NOU \Longrightarrow PKOKEPQW$$

(din motive suplimentare de securitate, spațiile dintre cuvinte se ignoră de obicei).

Bob cunoaște (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:

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

$$PKOKEPQW \Longrightarrow NIMICNOU$$

continuare

Exemplu

Codificare:

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 pe inelul finit $\mathbb{Z}_{26}$.

$$\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$$

Pentru $K \in \mathcal{K}$ *ales arbitrar (și* $m \in \mathcal{P}$, $\alpha \in \mathcal{C}$*):*

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

și

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

Criteriile lui Shannon

Există două tehnici de construcție a sistemelor de criptare (Claude Shannon, 1949):

Criteriile lui Shannon

Există două tehnici de construcție a sistemelor de criptare (Claude Shannon, 1949):

- **Confuzie**: Scopul este de a bloca orice informație obținută prin analize statistice sau redondanțe ale textului criptat.
  O modalitate simplă de a obține un grad ridicat de confuzie se bazează pe utilizarea de substituții.

Criteriile lui Shannon

Există două tehnici de construcție a sistemelor de criptare (Claude Shannon, 1949):

- **Confuzie**: Scopul este de a bloca orice informație obținută prin analize statistice sau redondanțe ale textului criptat.
  O modalitate simplă de a obține un grad ridicat de confuzie se bazează pe utilizarea de substituții.
- **Difuzie**: Disipează redondanța specifică textului clar.
  Practic, o modificare a unui singur caracter din textul clar provoacă multiple modificări în textul criptat.
  Pentru distingerea unei redondanțe din textul clar este necesară studierea unei cantități apreciabile de text criptat.

Secret perfect (perfect secrecy)

Un sistem de criptare are proprietatea de "secret perfect" dacă din textul criptat, *Oscar* nu poate obține nici o informație referitoare la textul clar.

Secret perfect (perfect secrecy)

Un sistem de criptare are proprietatea de "secret perfect" dacă din textul criptat, *Oscar* nu poate obține nici o informație referitoare la textul clar.

Definiție

Un sistem de criptare este perfect secret dacă

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

pentru orice $x \in \mathcal{P}$, $y \in \mathcal{C}$.
Probabilitatea aposteriori ca textul clar x *să fie criptat în textul recepționat* y *este identică cu probabilitatea apriori ca textul clar să fie* x.

Teoremă

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 și numai dacă toate cheile sunt utilizate cu probabilități egale și $\forall x \in \mathcal{P}$, $\forall y \in \mathcal{C}$ *există o cheie unică* $K \in \mathcal{K}$ *cu* $y = e_K(x)$.

Criptanaliza

Definiție

Procesul de determinare a unei chei K folosind un text criptat α (asociat eventual cu alte informații auxiliare) se numește "criptanaliză".

Decriptarea și *criptanaliza* au în final același scop: aflarea textului clar.
Diferența constă în faptul că în criptanaliză acesta trebuie aflat *fără a ști cheia de decriptare*.

Nu subestimați niciodată pe criptanalist.

Regula este verificată 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 intrușilor.

Principiul lui Kerkoff

Oscar are la dispoziție facilități de calcul excelente, adesea superioare celor de care dispun cei doi parteneri *Alice* și *Bob*.

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

Principiul lui Kerkoff

Oscar are la dispoziție facilități de calcul excelente, adesea superioare celor de care dispun cei doi parteneri *Alice* și *Bob*.

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

Criptanalistul știe toate detaliile sistemului de criptare folosit, inclusiv algoritmii utilizați precum și implementările lor.

Principiul lui Kerkoff

Oscar are la dispoziție facilități de calcul excelente, adesea superioare celor de care dispun cei doi parteneri *Alice* și *Bob*.

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

Criptanalistul știe toate detaliile sistemului de criptare folosit, inclusiv algoritmii utilizați precum și implementările lor.

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

Definiție

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

Definiție

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

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

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

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

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

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

Criptanaliza examinează cu atenție toate slăbiciunile (faliile) unui sistem și încearcă să construiască atacuri bazate pe aceste slăbiciuni, pentru a demonstra că sistemul nu este sigur (și 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.

În general un sistem de criptare poate fi:

- necondiționat sigur,

În general un sistem de criptare poate fi:

- necondiționat sigur,
- condiționat sigur.

Un sistem necondiționat 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.

Cazul I de atac:

1. *Oscar* știe numai textul criptat w;

în acest caz atacurile sunt direct legate de lungimea textului.

Cazul I de atac:

1. *Oscar* știe 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 și verificarea textului criptat, până se găsește cheia corectă.
Este atacul prin *forță brută* și el reușește totdeauna.

Teoremă

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 găsește cheia corectă.

Teoremă

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 găsește cheia corectă.

În cazul când numărul cheilor posibile este mic, această cheie se poate afla foarte ușor 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 biți sunt necesare în medie 2^{n-1} încercări (dacă nu există nici o informație suplimentară).

Teoremă

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 găsește cheia corectă.

În cazul când numărul cheilor posibile este mic, această cheie se poate afla foarte ușor 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 biți sunt necesare în medie 2^{n-1} încercări (dacă nu există nici o informație suplimentară).
O extindere a lungimii cheii la $n+1$ biți dublează deci spațiul de căutare.

Tehnica actuală de calcul permite atacuri prin forță brută eficiente pentru cheile de lungimi mai mici de 128 biți; de aceea sistemele de criptare actuale folosesc în general chei de cel puțin 1024 biți (excepție: sistemele bazate pe curbe eliptice).

Tehnica actuală de calcul permite atacuri prin forță brută eficiente pentru cheile de lungimi mai mici de 128 biți; de aceea sistemele de criptare actuale folosesc în general chei de cel puțin 1024 biți (excepție: sistemele bazate pe curbe eliptice).

Atacul prin forță brută poate fi îmbunătățit semnificativ cu alte informații legate de sistem, informații care pot reduce numărul cheilor posibile.
Multe atacuri folosesc diverse strategii pentru a reduce cât se poate de mult spațiul posibil al cheilor, după care se folosește un atac prin forță brută.

Cazul II de atac:

2. *Oscar* știe cel puțin o pereche de caractere *(text clar, text criptat)*.

Din cunoașterea câtorva perechi $(x, e_K(x))$ cu $x \in \mathcal{P}$ *Oscar* va încearca să decripteze întregul text criptat interceptat.

Exemple:

Exemplu

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

Exemple:

Exemplu

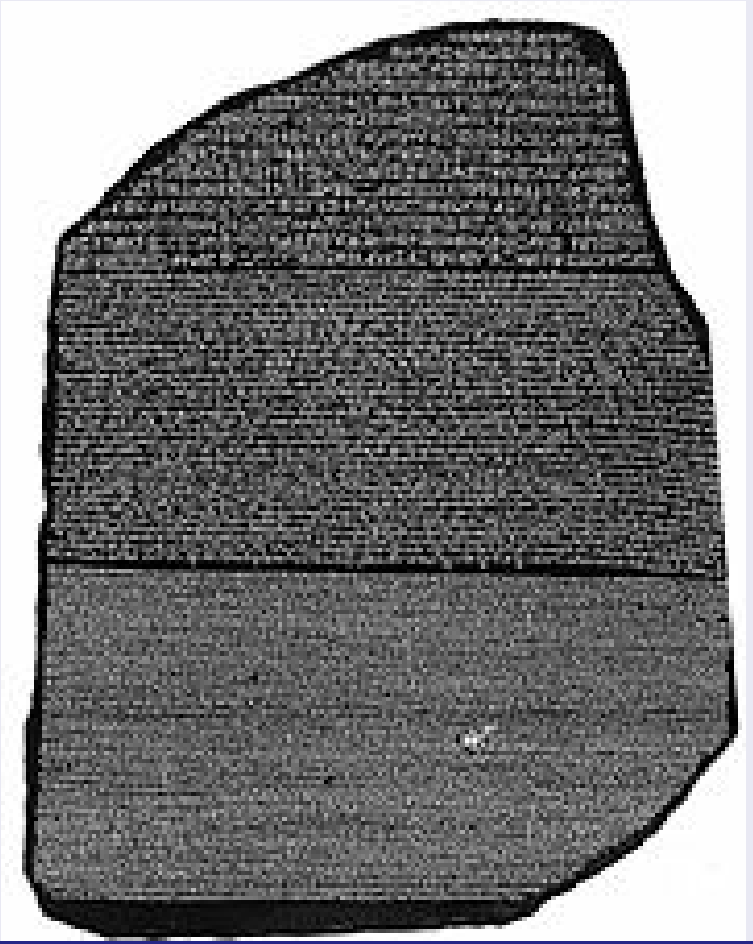
La sistemul de criptare Cezar, o singură pereche $(a, e_K(a))$, dezvăluie imediat cheia și – implicit duce la decriptare.

Exemplu

Aceasta a fost situația în care s-a aflat orientalistul francez Jean François Champollion, când a descifrat hieroglifele, folosind piatra de la Rosetta.

Piatra de la Rosetta

Exemplu



Cazul III de atac:

3. *Oscar* cunoaște criptarea unor texte clare selectate de el.

Acesta este *atacul cu text clar ales*, luat în considerare de majoritatea studiilor de criptanaliză.

Sistemul Hill:

Exemplu

Sistemul de criptare Hill (creat în 1929 de Lester Hill).
Definim un număr întreg fixat d ($d \geq 2$). Se construiesc mulțimile

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

Sistemul Hill:

Exemplu

Sistemul de criptare Hill (creat în 1929 de Lester Hill).
Definim un număr întreg fixat d ($d \geq 2$). Se construiesc mulțimile

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

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).

Sistemul Hill:

Exemplu

Sistemul de criptare Hill (creat în 1929 de Lester Hill).
Definim un număr întreg fixat d ($d \geq 2$). Se construiesc mulțimile

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

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

$$\beta_i = e_M(\alpha_i) = \alpha_i \cdot M \ (mod\ 26), \qquad (1 \leq i \leq n)$$

Sistemul Hill:

Exemplu

Sistemul de criptare Hill (creat în 1929 de Lester Hill).
Definim un număr întreg fixat d ($d \geq 2$). Se construiesc mulțimile

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

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

$$\beta_i = e_M(\alpha_i) = \alpha_i \cdot M \ (mod\ 26), \qquad (1 \leq i \leq n)$$

Pentru decriptare se folosește relația

$$d_M(\beta_i) = \beta_i \cdot M^{-1} \ (mod\ 26)$$

Continuare I:

Exemplu

Să luăm $d = 2$ și 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

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

Continuare II:

Exemplu

Din relațiile

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

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

se obține textul criptat $x = XWEK$.

Continuare III:

Exemplu

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

Continuare III:

Exemplu

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

Care este matricea
$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *cu* $a, b, c, d \in \{0, 1, \ldots, 25\}$, *astfel ca*

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

Continuare IV:

Exemplu

Oscar află întâi inversa lui $A = \begin{pmatrix} 5 & 17 \\ 0 & 2 \end{pmatrix}$.

Continuare IV:

Exemplu

Oscar află întâi inversa lui $A = \begin{pmatrix} 5 & 17 \\ 0 & 2 \end{pmatrix}$.

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

Continuare V:

Exemplu

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

Continuare V:

Exemplu

Să presupunem că Oscar lucrează în ipoteza (3)*; alege un text clar a cărui matrice este inversabilă și îi află criptarea.*
Fie BRAD acest text clar, a cărui matrice asociată este

$$A = \begin{pmatrix} 1 & 17 \\ 0 & 3 \end{pmatrix}$$

Continuare V:

Exemplu

Să presupunem că Oscar lucrează în ipoteza (3); alege un text clar a cărui matrice este inversabilă și 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 și primește LKGP, de matrice

$$B = \begin{pmatrix} 11 & 10 \\ 6 & 15 \end{pmatrix}$$

Continuare V:

Exemplu

Să presupunem că Oscar lucrează în ipoteza (3); alege un text clar a cărui matrice este inversabilă și 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 și primește LKGP, de matrice

$$B = \begin{pmatrix} 11 & 10 \\ 6 & 15 \end{pmatrix}$$

Deci el dispune de perechea (BRAD, LKGP).

Continuare VI:

Exemplu

Oscar determină întâi

$$A^{-1} = \begin{pmatrix} 1 & 3 \\ 0 & 9 \end{pmatrix}$$

Continuare VI:

Exemplu

Oscar determină întâi

$$A^{-1} = \begin{pmatrix} 1 & 3 \\ 0 & 9 \end{pmatrix}$$

Apoi, din ecuația $A \cdot M = B$, *va găsi soluția*

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

Cazul IV de atac:

Oscar știe cheia de criptare e_K. Pe baza ei încearcă să determine d_K înainte de interceptarea mesajelor criptate.

Cazul IV de atac:

Oscar știe cheia de criptare e_K. Pe baza ei încearcă să determine d_K înainte de interceptarea mesajelor criptate.

Este situația tipică sistemelor de criptare cu cheie publică: cheia de criptare e_K este cunoscută public cu mult înainte de a fi folosită pentru criptare.

Cazul IV de atac:

Oscar știe cheia de criptare e_K. Pe baza ei încearcă să determine d_K înainte de interceptarea mesajelor criptate.

Este situația 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 dispoziție destul de mult timp pentru prelucrarea ei și orice clarificare în perioada când timpul este "**ieftin**" are o valoare deosebită; după ce se primesc mesaje criptate, timpul devine "**scump**", și el trebuie să fie scurtat cât mai mult.

Clasificare:

În general, sistemele de criptare clasice se numesc și *sisteme simetrice*.
Motive:

Clasificare:

În general, sistemele de criptare clasice se numesc și *sisteme simetrice*.
Motive:

- Odată cu aflarea cheii de criptare e_K, cheia de decriptare d_K se obține imediat, fiind funcția inversă.

Clasificare:

În general, sistemele de criptare clasice se numesc și *sisteme simetrice*.
Motive:

- Odată cu aflarea cheii de criptare e_K, cheia de decriptare d_K se obține imediat, fiind funcția inversă.
- *Alice* și *Bob* dispun de aceeași informație relativ la sistemul de criptare.

Clasificare:

În general, sistemele de criptare clasice se numesc și *sisteme simetrice*.
Motive:

- Odată cu aflarea cheii de criptare e_K, cheia de decriptare d_K se obține imediat, fiind funcția inversă.
- *Alice* și *Bob* dispun de aceeași informație relativ la sistemul de criptare.

Sistemele de criptare simetrice se împart în: *cifruri de permutare*

Clasificare:

În general, sistemele de criptare clasice se numesc și *sisteme simetrice*.
Motive:

- Odată cu aflarea cheii de criptare e_K, cheia de decriptare d_K se obține imediat, fiind funcția inversă.
- *Alice* și *Bob* dispun de aceeași informație relativ la sistemul de criptare.

Sistemele de criptare simetrice se împart în: *cifruri de permutare* și *cifruri de substituție*.

Cifru de permutare

Textul clar se împarte în blocuri de n ($n \geq 2$) caractere, după care fiecărui bloc i se aplică o permutare $\pi \in S_n$ (mulțimea permutărilor de n elemente).

Elementele n și π sunt fixate.

π este cheia de criptare, iar π^{-1} va fi cheia de decriptare.

Exemplu

Cheie de criptare $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.

Un text clar, de exemplu

FLOARE ALBASTRA

se împarte în grupuri de câte trei caractere (s-a considerat și caracterul spațiu, notat _)

FLO ARE _AL BAS TRA

Exemplu

Cheie de criptare $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.

Un text clar, de exemplu

FLOARE ALBASTRA

se împarte în grupuri de câte trei caractere (s-a considerat și caracterul spațiu, notat _)

FLO ARE _AL BAS TRA

Textul criptat va fi

LFO RAE A_L ABS RTA

Exemplu

Cheie de criptare $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.

Un text clar, de exemplu

FLOARE ALBASTRA

se împarte în grupuri de câte trei caractere (s-a considerat și caracterul spațiu, notat _)

FLO ARE _AL BAS TRA

Textul criptat va fi

LFO RAE A_L ABS RTA

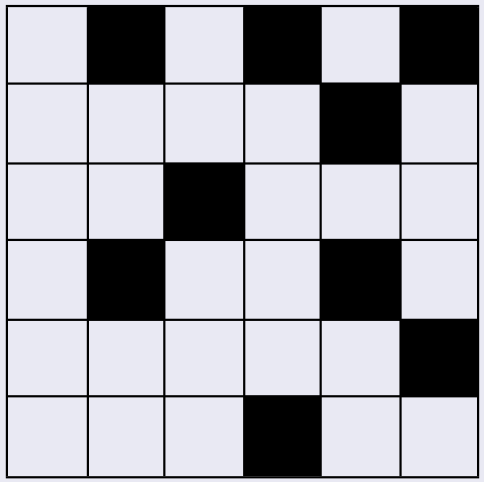
sau – eliminând grupările,

LFORAEA LABSRTA.

Sistemul Richelieu

Exemplu

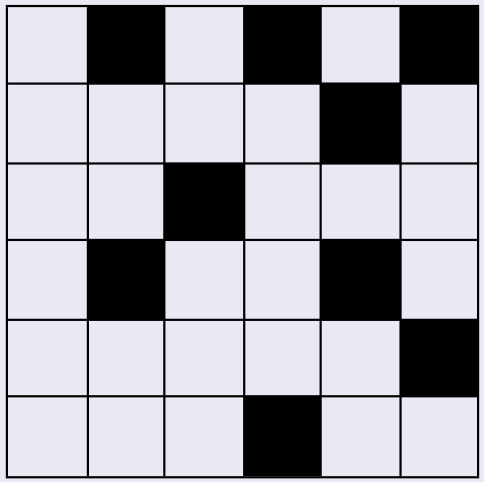
Fie cartonul 6×6, *în care zonele haşurate constituie găuri.*



Sistemul Richelieu

Exemplu

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



Vrem să criptăm textul

EMINESCU A FOST UN MARE POET NATIONAL

Richelieu II:

Exemplu

Vom scrie acest text sub forma unui tabel:

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*

Richelieu II:

Exemplu

Vom scrie acest text sub forma unui tabel:

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*

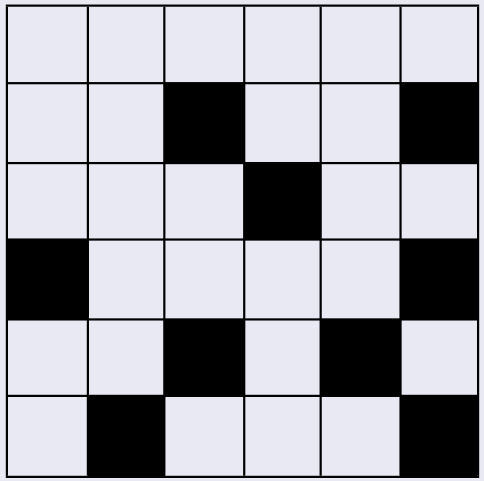
Aplicând cartonul peste acest text, vor rămâne vizibile 9 caractere:

MNS TA AN

Richelieu III:

Exemplu

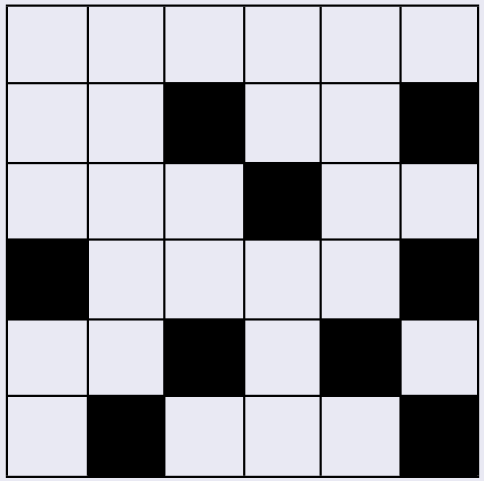
Rotim acum cartonul cu 90° în sensul acelor de ceasornic:



Richelieu III:

Exemplu

Rotim acum cartonul cu 90° în sensul acelor de ceasornic:



Așezând acum peste text, rămân vizibile caracterele

_F MPTNIL

Richelieu IV:

Exemplu

La a treia rotire a cartonului se obține

ICSUEETOA,

Richelieu IV:

Exemplu

La a treia rotire a cartonului se obține

ICSUEETOA,

iar la a patra

*EEUAOURO_*

Richelieu IV:

Exemplu

La a treia rotire a cartonului se obține

ICSUEETOA,

iar la a patra

*EEUAOURO_*

Deci textul criptat este

MNS TA AN F MPTNILICSUEETOAEEUAOURO

Richelieu IV:

Exemplu

La a treia rotire a cartonului se obține

ICSUEETOA,

iar la a patra

*EEUAOURO_*

Deci textul criptat este

MNS TA AN F MPTNILICSUEETOAEEUAOURO

Operația de decriptare se realizează similar.

Definiție

Fie n un număr natural nenul. Un cifru de permutare este un sistem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *unde* $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^n$, $\mathcal{K} = S_n$.
Pentru o cheie (permutare) $\pi \in S_n$

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

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

Lemă

Un cifru de permutare este un sistem de criptare Hill.

Lemă

Un cifru de permutare este un sistem de criptare Hill.

Proof.

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 ușor faptul că sistemul de criptare Hill cu matricea M_π este echivalent cu un cifru de permutare bazat pe cheia π.

Lemă

Un cifru de permutare este un sistem de criptare Hill.

Proof.

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

Cifruri de substituție

Sunt cele mai utilizate sisteme de criptare simetrice.
Cifrul constă în înlocuirea fiecărui caracter din V cu alt caracter (din W).

Cifruri de substituție

Sunt cele mai utilizate sisteme de criptare simetrice.
Cifrul constă în înlocuirea fiecărui caracter din V cu alt caracter (din W).

- *sisteme monoalfabetice;*

Cifruri de substituție

Sunt cele mai utilizate sisteme de criptare simetrice.
Cifrul constă în înlocuirea fiecărui caracter din V cu alt caracter (din W).

- *sisteme monoalfabetice;*
- *sisteme polialfabetice*.

Sisteme monoalfabetice

Substituie fiecare caracter cu alt caracter – totdeauna același, indiferent de poziție.

Sisteme monoalfabetice

Substituie fiecare caracter cu alt caracter – totdeauna același, indiferent de poziție.
Când cele două alfabete coincid ($V = W$), sistemele monoalfabetice sunt cazuri particulare de cifruri de permutare.

Sistemul de criptare Cezar

Odată stabilită cheia de criptare e_K, fiecare caracter x se înlocuiește prin caracterul

$$e_K(x) = x + k \ (mod\ 26)$$

Sistemul de criptare Cezar

Odată stabilită cheia de criptare e_K, fiecare caracter x se înlocuiește prin caracterul

$$e_K(x) = x + k \ (mod\ 26)$$

Decriptarea se realizează după formula

$$d_K(x) = x - k \ (mod\ 26)$$

Sistem Cezar cu cheie

Sistemul Cezar are numai 26 chei;deci este vulnerabil la atacul prin forță brută.
Pentru a-i mări rezistența, se poate utiliza o variantă, numită *sistem Cezar cu cheie*.

Sistem Cezar cu cheie

Sistemul Cezar are numai 26 chei;deci este vulnerabil la atacul prin forță brută.
Pentru a-i mări rezistența, se poate utiliza o variantă, numită *sistem Cezar cu cheie*.
Se definește un cuvânt (cheie), care se așează la începutul alfabetului.

Sistem Cezar cu cheie

Sistemul Cezar are numai 26 chei;deci este vulnerabil la atacul prin forță brută.
Pentru a-i mări rezistența, se poate utiliza o variantă, numită *sistem Cezar cu cheie*.
Se definește un cuvânt (cheie), care se așează la începutul alfabetului.
După ce se termină, șirul de completează cu literele care nu existau în cuvântul cheie, în ordine alfabetică.

Exemplu

Să presupunem că s-a ales cuvântul cheie MARTOR.

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.

Exemplu

Să presupunem că s-a ales cuvântul cheie MARTOR.

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.

$$STUDENT \longrightarrow QSUTOJS,$$

$$ARGINT \longrightarrow MPCEJS$$

Exemplu

Să presupunem că s-a ales cuvântul cheie MARTOR.

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.

$$STUDENT \longrightarrow QSUTOJS,$$

$$ARGINT \longrightarrow MPCEJS$$

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

Sistemul de criptare afin

Este o generalizare a sistemului Cezar.

$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}, \quad \mathcal{K} = \{(a, b) \mid a, b \in \mathbb{Z}_{26},\ cmmdc(a, 26) = 1\},$

Sistemul de criptare afin

Este o generalizare a sistemului Cezar.
$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}, \quad \mathcal{K} = \{(a, b) \mid a, b \in \mathbb{Z}_{26},\ cmmdc(a, 26) = 1\},$
Pentru o cheie $K = (a, b)$ fixată:

$$e_K(x) = ax + b \ (mod\ 26)$$

$$d_K(y) = a^{-1}y + a^{-1}(26 - b) \ (mod\ 26)$$

Sistemul de criptare afin

Este o generalizare a sistemului Cezar.
$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}, \quad \mathcal{K} = \{(a, b) \mid a, b \in \mathbb{Z}_{26},\ cmmdc(a, 26) = 1\}$,
Pentru o cheie $K = (a, b)$ fixată:

$$e_K(x) = ax + b\ (mod\ 26)$$

$$d_K(y) = a^{-1}y + a^{-1}(26 - b)\ (mod\ 26)$$

Condiția $cmmdc(a, 26) = 1$ asigură existența lui a^{-1} în $\mathbb{Z}_{26}$.

Exemplu

Exemplu

Funcția de criptare

$$e_K(x) = 3x + 5$$

0	1	2	3	4	5	6	7	8	9	10	11	12
5	8	11	14	17	20	23	0	3	6	9	12	15

13	14	15	16	17	18	19	20	21	22	23	24	25
18	21	24	1	4	7	10	13	16	19	22	25	2

Exemplu

Exemplu

Funcția de criptare

$$e_K(x) = 3x + 5$$

0	1	2	3	4	5	6	7	8	9	10	11	12
5	8	11	14	17	20	23	0	3	6	9	12	15

13	14	15	16	17	18	19	20	21	22	23	24	25
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

PRIMAVARA TARZIE $\longrightarrow$ *YEDPFQFEF KDECDR.*

Exemplu

Deoarece $3^{-1} = 9 \ (mod\ 26)$, *decriptarea se realizează folosind funcția* $d_K(x) = 9x + 7$.

Exemplu

Deoarece $3^{-1} = 9 \ (mod\ 26)$, *decriptarea se realizează folosind funcția* $d_K(x) = 9x + 7$.

Condiția $cmmdc(a, 26) = 1$ *asigură injectivitatea aplicației* e_K.

Pentru $e_K(x) = 10x + 1$, *A și N se transformă ambele în B, iar O nu apare ca imagine în alfabetul substituției.*

Spațiul cheilor într-un sistem de criptare afin

Orice cheie $K \in \mathcal{K}$ este determinată complet de valorile întregi (a, b) cu $cmmdc(a, 26) = 1$.

Spațiul cheilor într-un sistem de criptare afin

Orice cheie $K \in \mathcal{K}$ este determinată complet de valorile întregi (a, b) cu $cmmdc(a, 26) = 1$.
Sunt posibile 12 valori 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 excepție

$$a = 1, \ b = 0.$$

Spațiul cheilor într-un sistem de criptare afin

Orice cheie $K \in \mathcal{K}$ este determinată complet de valorile întregi (a, b) cu $cmmdc(a, 26) = 1$.
Sunt posibile 12 valori 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 excepție

$$a = 1,\ b = 0.$$

Deci $card(\mathcal{K}) = 311$, număr suficient de mic pentru reușita unui atac prin forță brută.

Sistemul de criptare Polybios

Alfabetul latin, din care se elimină o literă de frecvență cât mai redusă; fie aceasta W.

	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

Sistemul de criptare Polybios

Alfabetul latin, din care se elimină o literă de frecvență cât mai redusă; fie aceasta W.

	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

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

Variante ale sistemului Polybios

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 rusești, iar ulterior de către prizonierii americani din Vietnam.

Variante ale sistemului Polybios

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 rusești, iar ulterior de către prizonierii americani din Vietnam.
Este foarte simplu de învățat și poate fi aplicat folosind diverse semne drept coordonate (cifre, puncte, figuri, bătăi de tobă etc).

Variante ale sistemului Polybios

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 rusești, iar ulterior de către prizonierii americani din Vietnam.
Este foarte simplu de învățat și poate fi aplicat folosind diverse semne drept coordonate (cifre, puncte, figuri, bătăi 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.

Sistemul cavalerilor de Malta

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

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

S	T	U
V	W	X
Y	Z	

Liniile care încadrează fiecare caracter (inclusiv spațiul), împreună cu punctele (două, unul sau zero) indică substituția caracterului respectiv.

DUPA DOUAZECI DE ANI

Criptanaliza sistemelor de criptare monoalfabetice

Frecvența de apariție a caracterelor în text.

Dacă un text criptat este suficient de lung și se cunoaște limba în care este scris textul clar, sistemul poate fi spart printr-un atac bazat pe frecvența apariției literelor într-o limbă.

Criptanaliza sistemelor de criptare monoalfabetice

Frecvența de apariție a caracterelor în text.

Dacă un text criptat este suficient de lung și se cunoaște limba în care este scris textul clar, sistemul poate fi spart printr-un atac bazat pe frecvența apariției literelor într-o limbă.

Cu cât un text criptat este mai lung, cu atât frecvența literelor folosite în text este mai apropiată de frecvența literelor utilizate în limba în care este scris mesajul.

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

Literă	Frecvență
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	Frecvență
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 frecvență de apariție sub $1\ \%$).

Studiu de caz

Exemplu

S-a interceptat următorul text, criptat cu un sistem monoalfabetic.

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 gks gq gcxk fkpkcq sp gepbcgb

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

Continuare I:

Exemplu

Caracterele cele mai frecvente sunt c și k.
Pe de-altă parte, cele mai frecvente caractere din limba română sunt A, I și E. În mod cert, $A \in \{c, k\}$.

Continuare I:

Exemplu

Caracterele cele mai frecvente sunt c și k.
Pe de-altă parte, cele mai frecvente caractere din limba română sunt A, I și E. În mod cert, $A \in \{c, k\}$.
Sunt patru opțiuni posibile, din care trei se elimină rapid. Rămân

$$c \longleftarrow A, \ k \longleftarrow E$$

Continuare I:

Exemplu

Caracterele cele mai frecvente sunt c și k.
Pe de-altă parte, cele mai frecvente caractere din limba română sunt A, I și E. În mod cert, $A \in \{c, k\}$.
Sunt patru opțiuni posibile, din care trei se elimină rapid. Rămân

$$c \longleftarrow A, \; k \longleftarrow E$$

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

Exemplu

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

Continuare III:

Exemplu

Cuvântul REtREnEpbAq are corespondent în limba română numai pe REPREZENTA$\{I, M, U\}$
Se obțin decriptările

$$t \longleftarrow P,\ n \longleftarrow Z,\ p \longleftarrow N,\ b \longleftarrow T$$

lqaEA sp gARE aAa NAmgqT Eq ERA NEersmNqsT vE vsmgRETA mEaANA PAaANTqlqs vE Agele AmPRq ms ZoARgsT mTRAsN vE eRsgE oRATqsTATE PeRTslE sNAITE 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

Continuare IV:

Exemplu

Apoi NASgUT dă $g \longleftarrow C$, *SUPARATeR dă* $e \longleftarrow O$, *iar din fENEAU deducem* $f \longleftarrow V$.

Continuare IV:

Exemplu

Apoi NASgUT dă g ⟵ C, SUPARATeR dă e ⟵ O, iar din fENEAU deducem f ⟵ V.

lUaEA sp CARE MAM NASCUT EU ERA NEOrsSNUsT DE vsSCRETA SEaANA PAaANTUlUs DE ACOlO ASPRU Ss ZoARCsT STRAsN vE ORsCE oRATUsTATE PORTslE sNAITE 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

Continuare V:

Exemplu

Ultimele caractere:

$$l \longleftarrow L,\ a \longleftarrow M,\ r \longleftarrow B, s \longleftarrow I,\ v \longleftarrow D$$

Textul clar final este:

Continuare V:

Exemplu

Ultimele caractere:

$$I \longleftarrow L,\ a \longleftarrow M,\ r \longleftarrow B, s \longleftarrow I,\ v \longleftarrow D$$

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 IUCRU DE LA CEI CU CARE VENEAU IN CONTACT

(”Viața ca o coridă” de Octavian Paler).

Tabelele de frecvență a literelor pentru principalele limbi europene (din fiecare limbă sunt numai cele mai frecvente 9 litere):

Engleză	Frecvență
E	12,31 %
T	9,59 %
A	8,05 %
O	7,94 %
N	7,19 %
I	7,18 %
S	6,59 %
R	6,03 %
H	5,14 %

Germană	Frecvență
E	18,46 %
N	11,42 %
I	8,02 %
R	7,14 %
S	7,04 %
A	5,38 %
T	5,22%
U	5,01%
D	4,94%

Franceză	Frecvență
E	15,87 %
A	9,42 %
I	8,41 %
S	7,90 %
T	7,26 %
N	7,15 %
R	6,46 %
U	6,24 %
L	5,34 %

Mulțumesc pentru atenție !