UNIVERSITÉ LAVAL

Cryptographie classique

MOHAMED MEJRI

Groupe LSFM

Département d'informatique et de génie logiciel

Université LAVAL

Québec, Canada

UNIVERSITÉ LAVAL

Plan

- Introduction
  - Cryptologie
  - Cryptographie
  - Stéganographie
- Cryptographie classique
  - Cryptographie monoalphabétique
    - Chiffrement affine, chiffrement par substitution, le carré de Polybe
  - Cryptographie polyalphabétique
    - Chiffrement par permutation, chiffrement de Vigenere, chiffrement de Hill
- Instruments de (dé)cryptage

Cryptologie

- La cryptologie comprend :
  - Cryptographie (crypto=secret, graphy=writing)
    - La cryptographie peut être vue comme la science de déguisement de l'information.
    - Un ensemble de techniques, de manipulation et de transformation de données dans le but de satisfaire certains buts sécuritaires.
    - Elle consiste à chiffrer ou crypter des messages en clair et de déchiffrer ou décrypter des messages codés en connaissant la clé.

  - Cryptanalyse : C'est l'art de décrypter des messages codés sans connaître la clé ("code breaking").

Cryptographie

- Un système cryptographique ou cryptosystème est composé essentiellement d'un algorithme de cryptage (chiffrement) et d'un algorithme de décryptage (déchiffrement).
- Définition formelle : Un cryptosystème est un quintuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$

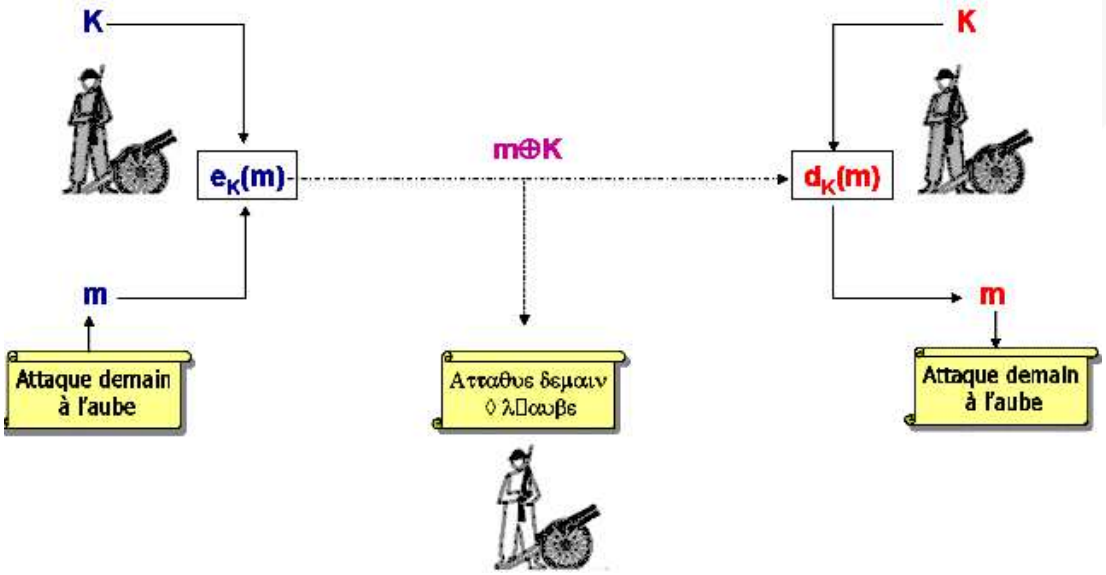
$$
\begin{aligned}
\mathcal{P} &= \{\text{messages clairs}\} \\
\mathcal{C} &= \{\text{messages chiffrés}\} \\
\mathcal{K} &= \{\text{ clefs}\} \\
\mathcal{E} &= \{e_k : \mathcal{P} \to \mathcal{C} | k \in \mathcal{K}\} \\
\mathcal{D} &= \{d_k : \mathcal{C} \to \mathcal{P} | k \in \mathcal{K}\}
\end{aligned}
$$

$$\forall\, k \in \mathcal{K},\ \forall\, x \in \mathcal{P},\ \exists\, k^{-1} \in \mathcal{K} \mid d_{k^{-1}}(e_k(x)) = x$$

Cryptographie

➪ Exemple :

$$\begin{cases} \mathcal{P} = \mathcal{C} = \mathcal{K} = \{0,1\}^n \\ e_k \in \mathcal{E} \Rightarrow e_k(m) = m \oplus k \\ d_k \in \mathcal{D} \Rightarrow d_k(m) = m \oplus k \\ k^{-1} = k \end{cases} \Rightarrow \begin{cases} d_k(e_k(m)) &= (m \oplus k) \oplus k \\ &= m \oplus (k \oplus k) \\ &= m \end{cases}$$



Cryptographie

- Motivations : La cryptographie est partout.
  - Protéger la communication – trafic : HTTPS, FTPS, SSH, etc.
    - trafic sur un réseau sans fil : WPA2, WEP, Bluetooth
    - trafic GSM : A5/1, 2
  - Protéger des données sur un disque dur : TrueCrypt, MD5, BitLocker Drive Encryption, Encrypting File System (EFS).
  - Authentification : Kerberos, TLS/SSL, NTLM2, etc.
  - Vote électronique
  - Argent numérique
  - Navigation anonyme : TOR (The Onion Router)
  - Sécurité dans l'infonuagique (*cloud*) : chiffrement homomorphique $f(a \odot b) = f(a) \otimes f(b)$
  - Etc.

Cryptographie

⇨ Motivations :

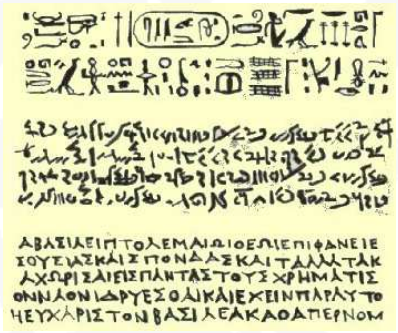
- Confidentialité : comment coder des données de telle sorte qu'elles ne soient compréhensibles (accessibles) que par certaines personnes ?
- Intégrité : comment coder des données de telle sorte que toute modification que s'y rapporte sera détectée ?
- Authentification de message : comment coder des données de telle sorte qu'il serait possible de déterminer leurs origines ?
- Non répudiation, authentification des agents, anonymat, etc.

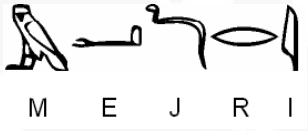
. . . . . *Elle donne des briques de base pour construire des systèmes sécuritaires.*

Cryptographie

Historique rapide :

- Existe depuis l'invention de l'écriture (Égyptiens, Jules Cesare).

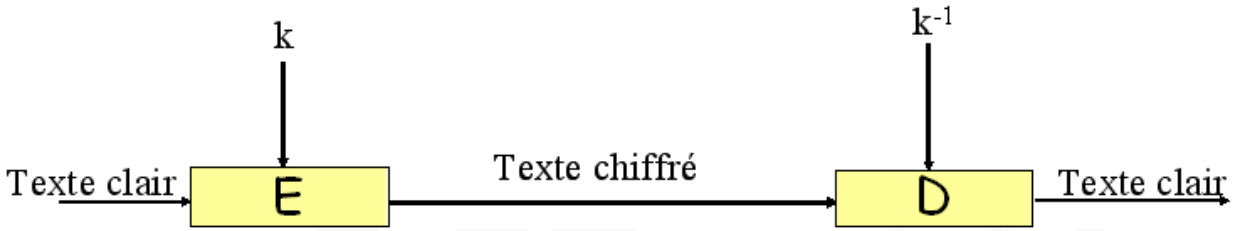




- Jusqu'à 1970 inconnue en dehors des milieux militaires et diplomatiques.

- Ordinateurs + Réseaux informatique $\Rightarrow$ utilisation de la cryptographie dans le domaine civil $\Rightarrow$ plus de recherche en cryptographie $\Rightarrow$ des systèmes cryptographiques plus sécuritaires (RSA, DES, etc.)

Cryptographie



- Types de cryptosystèmes :
  - Systèmes à usage restreint : les algorithmes de chiffrement et de déchiffrement sont secrets. La sécurité repose sur leur confidentialité.
  - Systèmes à usage général : la confidentialité ne repose pas sur l'algorithme, mais sur une clé. Tout le monde peut utiliser le même système.
- Caractérisation : trois dimentions indépendantes
  - Types d'opérations : substitution, permutation (transposition), etc.
  - Types de clés : symétrique (1 clé), asymétrique (2 clés)
  - Modes d'opérations : par bloc ou à la volée (*stream cipher*)

Stéganographie

- Définition : Ensemble de techniques qui consistent à cacher l'existence même d'un message.
- Remarque : Généralement, le message à transmettre est caché à l'intérieur d'un texte beaucoup plus grand.
- Exemples historiques : Encre invisible, la première lettre de chaque mot, le premier mot de chaque phrase, etc.
- Exemples plus récents : On cache un message dans une image graphique en modifiant le dernier bit de la couleur de chaque pixel.

Stéganographie

Quelques outils

- Image Hide : cacher du texte dans une image
- Stealth files : cacher des fichiers exécutables dans des fichiers Word, Excel, PDF, etc.
- Masker Steganography Tool : Crypte des fichiers et des répertoires et les cache dans d'autres fichiers image, vidéo, son
- Hermetic Stego : permet de crypter des fichiers, de les éclater en morceaux et de les cacher dans plusieurs fichiers BMP
- Snow.exe : cache un message dans un fichier texte en ajoutant des espaces à la fin de ligne
- Steghide : permet de crypter et de cacher des fichiers dans une variété de formats : JPEG, BPM, WAV, AU
- SpamMimic : Le site web comme www.spammimic.com : on lui donne un texte à cacher et il génère un message qui cache le texte donné

Plan

- Introduction
  - Cryptologie
  - Cryptographie
  - Stéganographie
- Cryptographie classique
  - Cryptographie monoalphabétique
    - Chiffrement affine, chiffrement par substitution, le carré de Polybe
  - Cryptographie polyalphabétique
    - Chiffrement par permutation, chiffrement de Vigenere, chiffrement de Hill
- Instruments de (dé)cryptage

Cryptographie classique

- Des techniques très simples à comprendre.
- On n'a pas besoin d'ordinateurs pour les utiliser.
- Ils ne sont pas sécuritaires.
- Pourquoi les étudier ?
  - Découvrir les origines de leurs faiblesses pour les éviter lors de la conception d'autres systèmes.
  - Profiter de leurs avantages lors de la conception de nouveaux cryptosystèmes.

Cryptographie classique

- Plusieurs types de systèmes cryptographiques classiques :
  - Monoalphabétique : Pour une clé donnée, une lettre du texte clair est toujours mappée à une même lettre du texte chiffré indépendamment de sa position dans le texte.
  - Polyalphabétique : Pour une clé donnée, une lettre du texte clair peut être mappée à plusieurs lettre du texte chiffré dépendamment de sa position dans le texte.
  - Etc.

Un peu de la théorie de nombres

- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$
- $a \; mod \; n$ est le reste de la division de a sur n.
- $(a + b) \; mod \; n = [(a \; mod \; n) + (b \; mod \; n)] \; mod \; n$.
- $(a * b) \; mod \; n = [(a \; mod \; n) * (b \; mod \; n)] \; mod \; n$.
- $a \equiv b \; mod \; n \Leftrightarrow a \; mod \; n = b \; mod \; n$.
- $\forall \; a \in \mathbb{Z}_n, \; pgcd(a, n) = 1 \Leftrightarrow \exists \; a^{-1} \in \mathbb{Z}_n \mid aa^{-1} \equiv 1 \; mod \; n$. L'élément a^{-1} est unique et il est appelé l'inverse de a dans $\mathbb{Z}_n$. Exemple : l'inverse de 7 dans $\mathbb{Z}_{20}$ est 3 puisque $7 * 3 = 21 \equiv 1 \; mod \; 20$.

Cryptographie monoalphabétique

➪ Chiffrement affine :

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

$$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} \mid pgcd(a, 26) = 1\}$$

Pour tout $k = (a, b) \in \mathcal{K}$ et $x,\ y\ \in \mathbb{Z}_{26}$, on a :

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

et

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

Cryptographie monoalphabétique

- Chiffrement affine (suite) :
  - Remarque : $a = 1 \Rightarrow$ chiffrement par décalage (code de César a=1 et b=3).
  - Exemple : $k = (1, 5)$

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

$$e_k(\text{CRYPTOGRAPHIE})$$
$$= e_k(\text{C})e_k(\text{R})\ e_k(\text{Y})e_k(\text{P})e_k(\text{T})\ e_k(\text{O})e_k(\text{G})e_k(\text{R})\ e_k(\text{A})e_k(\text{P})e_k(\text{H})\ e_k(\text{I})\ e_k(\text{E})$$
$$= \text{H}\quad \text{W}\quad \text{D}\quad \text{U}\quad \text{Y}\quad \text{T}\quad \text{L}\quad \text{W}\quad \text{F}\quad \text{U}\quad \text{M}\quad \text{N}\quad \text{J}$$

Cryptographie monoalphabétique

➪ Chiffrement par substitution :

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

$\mathcal{K} = \{\pi \mid \pi \text{ est une permutation des élements } 0, 1, \ldots, 25\}$

Pour tout $\pi \in \mathcal{K}$ et $x,\ y\ \in \mathbb{Z}_{26}$, on a :

$$e_\pi(x) = \pi(x)$$

et

$$d_k(y) = \pi^{-1}(y)$$

Cryptographie monoalphabétique

- Chiffrement par substitution (suite) :
  - Exemple :

$$\begin{aligned}\pi \quad = \quad & [0 \mapsto 20, 1 \mapsto 13, 2 \mapsto 21, 3 \mapsto 0, 4 \mapsto 1, 5 \mapsto 2, 6 \mapsto 3, 7 \mapsto 4, 8 \mapsto 5,\\ & 9 \mapsto 6, 10 \mapsto 7, 11 \mapsto 8, 12 \mapsto 9, 13 \mapsto 10, 14 \mapsto 11, 15 \mapsto 12, 16 \mapsto 14,\\ & 17 \mapsto 15, 18 \mapsto 16, 19 \mapsto 17, 20 \mapsto 18, 21 \mapsto 19, 22 \mapsto 22,\\ & 23 \mapsto 23, 24 \mapsto 24, 25 \mapsto 25]\end{aligned}$$

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

$e_k(\text{ABC}) = e_k(\text{A})e_k(\text{B})\ e_k(\text{C}) = \text{UNV}$

Cryptographie monoalphabétique

- Le carré de Polybe :
  - Principe :
    - C'est un système basé sur un carré de 25 cases.
    - Une clé est arrangement de lettres dans le tableau.
      - k_1=abcdefghijklmnopqrstuvxyz
      - k_2=maclebdfghijklnopqrstuvxyz

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i	j
3	k	l	m	n	o
4	p	q	r	s	t
5	u	v	x	y	z

	1	2	3	4	5
1	m	a	c	l	e
2	b	d	f	g	h
3	i	j	k	n	o
4	p	q	r	s	t
5	u	v	x	y	z

    - La lettre W sera supprimé du texte clair ou remplacée par une autre (V).
    - Chaque lettre est remplacée (cryptée) par deux chiffres (celui de sa ligne, celui de sa colonne) : e=15, v=52, o=35, . . .

Cryptographie monoalphabétique

Le carré de Polybe (Suite) :

- Exemple : M=On attaque demain

M	O	n	a	t	t	a	q	u	e	d	e	m	a	i	n
$e_{k_1}(M)$	35	34	11	45	45	11	42	51	15	14	15	33	11	24	34

M	O	n	a	t	t	a	q	u	e	d	e	m	a	i	n
$e_{k_2}(M)$	35	34	12	51	51	12	42	51	15	22	15	11	12	31	34

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i	j
3	k	l	m	n	o
4	p	q	r	s	t
5	u	v	x	y	z

	1	2	3	4	5
1	m	a	c	l	e
2	b	d	f	g	h
3	i	j	k	n	o
4	p	q	r	s	t
5	u	v	x	y	z

- Remarque : On peut agrandir ce carré (36 cases par exemple) afin de pouvoir ajouter les chiffres ou de tenir compte des langages qui manipulent plus de caractères

Cryptographie Polyalphabétique

➪ Chiffrement par permutation (appelé aussi chiffrement par transposition) :

Soit n un entier strictement positif.

$\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^n$

$\mathcal{K} = \{\pi \mid \pi \text{ est une permutation des élements } 1, \ldots, n\}$

Pour tout $\pi \in \mathcal{K}$ et $x = x_1 \ldots x_n,\ y = y_1 \ldots y_n \ \in \mathbb{Z}_{26}^n$, on a :

$$e_\pi(x_1 \ldots x_n) = x_{\pi(1)} \ldots x_{\pi(n)}$$

et

$$d_k(y_1 \ldots y_n) = y_{\pi^{-1}(1)} \ldots y_{\pi^{-1}(n)}$$

Cryptographie polyalphabétique

- Chiffrement par permutation (suite) :
  - Remarque : Si le message a une taille supérieure à n alors on fait son découpage.
  - Exemple : Soient $n = 6$ et $\pi = 3, 5, 1, 6, 4, 2$, i.e., $\pi(1) = 3,\ \pi(2) = 5, \ldots$

    e_π(CRYPTOGRAPHY)= ?

    C=1,R=2,Y=3,P=4,T=5,O=6

    G=1,R=2,A=3,P=4,H=5,Y=6

    e_π(CRYPTOGRAPHY)=YTCOPRAHGYPR

Cryptographie polyalphabétique

⇨ Chiffrement par permutation (suite) :

↦ Exercice : Crypter le message suivant :

Attaque demain à l'aube

Sachant que :

- $n = 3$
- $\pi = 3, 1, 2$

Cryptographie Polyalphabétique

➪ Chiffrement de Vigenere : Amélioration du code de CÉSAR !

Soit $n \in \mathbb{Z}_{26}$.

$\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{26})^n$

Pour tout $k = (k_1, \ldots, k_n) \in \mathcal{K}$ et $x = x_1 \ldots x_n,\ y = y_1 \ldots y_n\ \in \mathbb{Z}_{26}^n$, on a :

$$e_k(x_1 \ldots x_n) = (x_1 + k_1\ mod\ 26) \ldots (x_n + k_n\ mod\ 26)$$

et

$$d_k(y_1 \ldots y_n) = (y_1 - k_1\ mod\ 26) \ldots (y_n - k_n\ mod\ 26)$$

Cryptographie polyalphabétique

➪ Chiffrement de Vigenere (suite) :

➻ Exercice : Crypter le message suivant :

chiffrement de vigenere

Sachant que :

- $n = 9$
- $k = (1, 0, 2, 4, 7, 11, 8, 4, 17)$

Cryptographie polyalphabétique

- Chiffrement de VERNAM (masque jetable) :
  - même chose que Vigenère.
  - sauf que la clé doit toujours avoir la même longueur que le texte clair (pas de découpage).
  - Remarque : si la clé n'est utilisée qu'une seule fois, on l'appelle dans ce cas "one-time pad".

- Exercice : Crypter le message suivant :

Masque Jetable

Sachant que : $k = (23, 2, 0, 0, 19, 4, 11, 15, 17, 21, 6, 25, 2)$

Cryptographie Polyalphabétique

➪ Chiffrement de Hill :

Soit n un entier strictement positif.

$\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^n$

$\mathcal{K} = \{\text{matrices de dimension } n \times n \text{ inversibles dans } \mathbb{Z}_{26}\}$

Pour tout $k = \in \mathcal{K}$ et $x = x_1 \dots x_n,\ y = y_1 \dots y_n\ \in \mathbb{Z}_{26}^n$, on a :

$$(1)\begin{cases} e_k(x_1 \dots x_n) = (x_1 \dots x_n)k \\ et \\ d_k(y_1 \dots y_n) = (y_1 \dots y_n)k^{-1} \end{cases} \quad ou \quad (2)\begin{cases} e_k(x_1 \dots x_n) = k(x_1 \dots x_n)^t \\ et \\ d_k(y_1 \dots y_n) = k^{-1}(y_1 \dots y_n)^t \end{cases}$$

Remarque : En absence d'indications explicites, on suppose qu'on utilise le système (1).

Cryptographie Polyalphabétique

➪ Chiffrement de Hill (suite) :

➻ Exemple : $m = DBUDTA, k = \begin{pmatrix} 18 & 17 \\ 17 & 18 \end{pmatrix} : e_k(m) = c_1c_2c_3c_4c_5c_6$ avec

$$\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} 18 & 17 \\ 17 & 18 \end{pmatrix} * \begin{pmatrix} 3(D) \\ 1(B) \end{pmatrix} mod\ 26 = \begin{pmatrix} 19(T) \\ 17(R) \end{pmatrix}$$

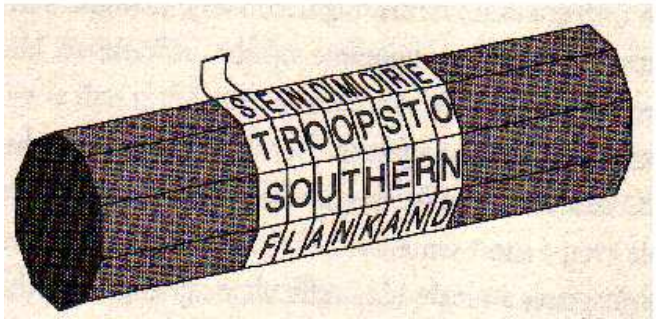
$$\begin{pmatrix} c_3 \\ c_4 \end{pmatrix} = \begin{pmatrix} 18 & 17 \\ 17 & 18 \end{pmatrix} * \begin{pmatrix} 20(U) \\ 3(D) \end{pmatrix} mod\ 26 = \begin{pmatrix} 21(V) \\ 4(E) \end{pmatrix}$$

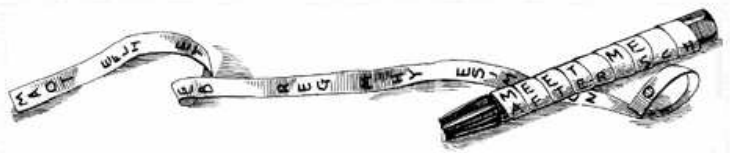
$$\begin{pmatrix} c_5 \\ c_6 \end{pmatrix} = \begin{pmatrix} 18 & 17 \\ 17 & 18 \end{pmatrix} * \begin{pmatrix} 19(U) \\ 0(D) \end{pmatrix} mod\ 26 = \begin{pmatrix} 4(E) \\ 11(L) \end{pmatrix}$$

Plan

- Introduction
  - Cryptologie
  - Cryptographie
  - Stéganographie
- Cryptographie classique
  - Cryptographie monoalphabétique
    - Chiffrement affine, chiffrement par substitution, le carré de Polybe
  - Cryptographie polyalphabétique
    - Chiffrement par permutation, chiffrement de Vigenere, chiffrement de Hill
- Instruments de (dé)cryptage

Instruments de (dé)cryptage





Instruments de (dé)cryptage

Disque à chiffrer
(XV siècle)

Machine Enigma
XX^{e} siècle

Instruments de (dé)cryptage

➪ Enigma simplifiée : Principe de fonctionnement.