

Cours de Cryptographie

Enseignante: **Bouzara Reguia Lamia**

Niveau: Première année Master

Université Yahia Fares de Médéa

Chapitre I: Cryptographie Conventionnelle

- Introduction
- Chiffrement de César/Chiffrement affine
- Chiffrement par substitution
- Chiffrement de Vignère/Chiffrement de Hill
- Masque jetable (One-pad time)
- Chiffrement par transposition
- Mode opératoires

Outlines of this talk

1 Introduction

Introduction

Les gens ont toujours l'habitude de garder leurs secrets et leurs informations loin des étrangers. Plusieurs gens utilisent des messages codés entre eux pour garder leurs secrets loin de leurs parents, amies, connaissances.

L'histoire a connu plusieurs rois et généraux qui ont utilisé la cryptographie et ses méthodes pour éviter que leurs ennemies accèdent à leurs informations sensibles (par exemple la deuxième guerre mondiale).

Lorsque on parle de ce sujet on parle de trois termes: Cryptologie, Cryptographie et Cryptanalyse.

Cryptographie : C'est l'étude des méthodes et techniques servant à crypter du texte pour le protéger et assurer sa confidentialité, authenticité et intégrité en s'aidant de données secrètes ou clés.

Cryptanalyse : Opposée à la Cryptographie, elle a pour but de déchiffrer le texte chiffrer.

Cryptologie : La science du secret, il s'agit d'une scène englobant deux branches: la cryptographie i.e l'écriture secrète et la cryptanalyse i.e l'analyse de cette dernière.

Cryptographie conventionnelle

La cryptographie conventionnelle est liée principalement aux services de confidentialité.
Un cryptosystème est un 5-uplet (P, C, K, E, D) ou:

P : est l'ensemble des messages clairs (plain text)

C : est l'ensemble des messages cryptés ou chiffrés (ciphertext)

K : est l'ensemble des clés (key).

$E: \{E_e : P \rightarrow C\}$

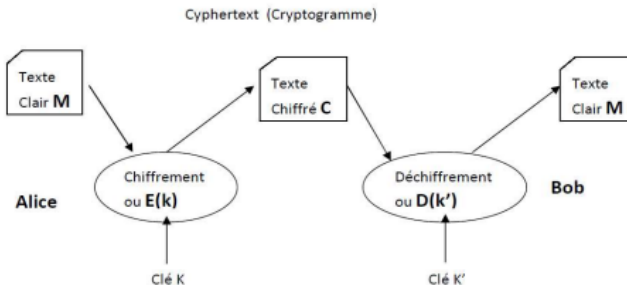
E_e fonction de chiffrement.

$D: \{D_k : C \rightarrow P\}$

D_k fonction de déchiffrement.

A chaque clé $e \in K$ est associée une clé $d \in K$ telle que: $D_d(E_e(p)) = p$ et $E_e(D_d(x)) = x$. Le chiffrement d'un message en clair m se fait par un algorithme de chiffrement ou une fonction de chiffrement noté E_k , l'entrée de cet algorithme est m (plain text) et on obtient comme sortie le message chiffré $c = E_k(m)$ (ciphertext).

Le déchiffrement à partir du chiffré ou cryptogramme se fait en utilisant un algorithme de déchiffrement D_k , prenant en entrée le message chiffré c et la même clé k ;
 $D_k(E_k(m)) = m$ et $E_k(D_k(c)) = c$.



Remarque

On parle de la cryptographie à clé secrète ou symétrique si les clés de chiffrement et les clés de déchiffrement sont égaux, on se déduit l'une à l'autre;

$k = e$ Cryptographie symétrique où à clé secrète.

$k \neq e$ Cryptographie asymétrique où à clé publique.

L'émission de la cryptographie:

La cryptographie doit résoudre les problèmes suivants:

Confidentialité: Ceux qui ne sont pas destinataires d'une information ne doivent pas avoir l'accès à ce message.

Authentification Il doit être possible pour le récepteur du message de garantir son origine, une tierce personne ne doit pas pouvoir se faire passer pour quelqu'un d'autre. Ce service assure que l'information soit non déchiffirable à des personnes autres que les acteurs de la communication.

Intégrité Le récepteur doit pouvoir s'assurer que le message n'a pas été modifié durant la transmission.

Non répudiation: Un émetteur ne doit pas pouvoir nier l'envoi d'un message. Ce service doit assurer que l'auteur d'une action ne peut ensuite nier de l'avoir effectuée.

Disponibilité Ce service doit assurer aux utilisateurs la continuité de l'accès à tout moment à l'information.

Alphabet et mots:

Pour écrire des textes, nous avons besoin des symboles ou un alphabet noté Σ (fini et non vide) tel que:

- $|\Sigma|$ = longueur de Σ .
- Les éléments de Σ sont appelés symboles ou lettres.

Exemple

l'alphabet $\Sigma = \{A, B, C, \dots, Z\}$ est de longueur 26.

Definition

Soit Σ un alphabet, alors:

- Un mot sur Σ est une suite de symboles de Σ .
- La longueur d'un mot w est le nombre de composante de w .
- Si $n \geq 0$, Σ^n est l'ensemble des mots de longueur n .

$|\Sigma| = n \in \mathbb{N}^*$, alors un symbole peut être identifier avec des entiers naturels.

Les symboles de Σ sont identifiées aux nombres de $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$

Chiffrement de César

Definition

On peut définir le chiffrement de César simplement par une addition dans \mathbb{Z}_{26} .
Fixons un entier k qui est le décalage, la fonction de chiffrement de César de décalage k qui va de \mathbb{Z}_{26} à \mathbb{Z}_{26} est donnée par:

- (1) $E_k : \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}$
- (2) $x \mapsto x + k[26]$

Chiffrement de César

exemple

Pour $k = 3$ la fonction de chiffrement est notée E_3 et on chiffre modulo 26: $E_3(0) = 3$, $E_3(1) = 4 \dots$

Pour déchiffrer, il suffit d'aller dans le sens contraire:

$$(3) \quad D_k : \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}$$

$$(4) \quad x \mapsto x - k[26]$$

Pour $k = 3$:

$$(5) \quad D_3 : \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}$$

$$(6) \quad x \mapsto x - 3[26]$$

Si 1 est chiffré par 4 par la fonction de chiffrement E_3 le déchiffrement est

$$D_3(4) = 4 - 3 = 1.$$

Chiffrement de César

Exemple

Pour chiffrer le mot "ELECTRON" par le chiffrement de César avec la fonction de chiffrement E_3 , on utilise le tableau suivant pour identifier les symboles de l'alphabet aux nombres de \mathbb{Z}_{26}

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
				q	r	s	t	u	v	w	x	y	z		
				16	17	18	19	20	21	22	23	24	25		

Et puis on applique la fonction de chiffrement E_3 , on obtient le chiffré:

7 14 7 5 22 11 17 16

Le cryptogramme est : HOHFWURQ

Chiffrement affine

Le chiffrement affine est une généralisation naturelle du chiffrement de César.

Fonction de chiffrement:

$$(7) \quad E_{(a,b)} : \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}$$

$$(8) \quad x \mapsto ax + b[26]$$

Si a est inversible dans \mathbb{Z}_{26} càd $(a, 26) = 1$, alors:

$$a \in \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\} = \mathbb{Z}_{26}^*.$$

$\mathbb{Z}_{26}^* \neq \mathbb{Z}_{26} \setminus \{0\}$, on a:

$$a \in \mathbb{Z}_{26}^* \Rightarrow a \text{ est inversible.}$$

Chiffrement affine

On a:

$$c \equiv ax + b[26] \Leftrightarrow c - b \equiv ax[26] \Leftrightarrow ax \equiv c - b[26]$$

Alors la fonction de déchiffrement est donnée par:

Fonction de déchiffrement:

$$(9) \quad D_{a,b} : \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}$$

$$(10) \quad c \mapsto a^{-1}(c - b)[26] = x$$

Chiffrement par substitution

Il est facile de remarquer que le chiffrement de César n'est pas efficace car on peut l'attaquer facilement, c'est pourquoi il est amélioré au lieu de faire un décalage, on peut remplacer chaque lettre par une autre lettre d'une manière aléatoire. Cette méthode de chiffrement est appelée chiffrement par substitution

Exemple

Crypter le message " être ou ne pas être telle est la question ". En utilisant le tableau de correspondance suivant:

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

Le message crypté est: XGKX DR SX OFV XGKX GXWWX XVG WF ZRXVGPDS
Pour déchiffrer le message, il suffit d'utiliser le tableau et faire l'opération inverse.

Chiffrement par substitution

Attaque statistique: Pour faire l'attaque on utilise l'analyse des fréquences. Dans les textes longs les lettres n'apparaissent pas avec la même fréquence (la fréquence d'une lettre varie d'une langue à une autre).

Pour trouver le message en clair nous remplaçons le symbole le plus fréquent par la lettre la plus fréquente du message en clair, le suivant par la deuxième et on continue par la même façon les autres lettres pour avoir tous les symboles du cryptogramme.

Par exemple les fréquences des lettres les plus utilisées dans la langue française sont par ordre:

E	S	A	I	N	T	R	U	L	O	D
14.69%	8.01%	7.54%	7.18%	6.89%	6.88%	6.49%	6.12%	5.63%	5.29%	3.66%

Chiffrement de Vigenère

Le principe de ce chiffrement est de regrouper le message en blocs de la même longueur que la clé k . Après on chiffre par la fonction de chiffrement.

On a: $P = C = K = \mathbb{Z}_{26}$.

Fonction de chiffrement:

$$(11) \quad D_k : \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}$$

$$(12) \quad (x_1, \dots, x_n) \mapsto (x_1 + k_1[26], \dots, x_n + k_n[26])$$

Pour déchiffrer on fait l'opération inverse:

Fonction de déchiffrement:

$$(13) \quad E_k : \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}$$

$$(14) \quad (x_1, \dots, x_n) \mapsto (x_1 - k_1[26], \dots, x_n - k_n[26])$$

Exemple:

On veut chiffrer le message: "DEMAINONPART" en utilisant le chiffrement de Vigenère avec la clé $k = \text{CRYPTO}$: Pour chiffrer le message on regroupe les lettres de notre texte par blocs de longueur 6, après on identifie les lettres aux nombres de \mathbb{Z}_{26} et en utilisant le tableau:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
				q	r	s	t	u	v	w	x	y	z		
				16	17	18	19	20	21	22	23	24	25		

et on chiffre en utilisant la fonction de chiffrement E_k . On obtient le cryptogramme: FVKPBBQENPKH

Chiffrement de Hill

Ce chiffrement est un autre cryptosystème inventé en 1929 par Lester-S-Hill, l'espace de clés est l'ensemble de toutes les matrices carrées d'ordre n à coefficients dans \mathbb{Z}_m tel que:

$$\det(A ; m) = 1 (A \text{ est inversible})$$

Fonction de chiffrement:

$$(15) \quad E_A : \mathbb{Z}_m^n \rightarrow \mathbb{Z}_m^n$$

$$(16) \quad x \mapsto A \cdot X$$

Supposons qu'on a une matrice carrée d'ordre 2:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Chiffrement de Hill

le chiffrement d'un message en clair (x_k, x_{k+1}) se fait de la manière suivante:

$$\begin{pmatrix} y_k \\ y_{k+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_k \\ x_{k+1} \end{pmatrix}$$

(y_k, y_{k+1}) est le message chiffré. Cela veut dire que les premières lettres du message en clair $(x_1 \text{ et } x_2)$ seront chiffrées en $(y_1 \text{ et } y_2)$ selon les deux équations suivantes:

$$(17) \quad y_1 = ax_1 + bx_2 [26]$$

$$(18) \quad y_2 = cx_1 + dx_2 [26]$$

Pour déchiffrer le message (x_1, x_2) la matrice

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

doit être inversible dans \mathbb{Z}_{26} , et on déchiffre de la manière suivante:

$$\begin{pmatrix} x_k \\ x_{k+1} \end{pmatrix} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} y_k \\ y_{k+1} \end{pmatrix}$$

où:

$$\det(A) = \frac{1}{ad - bc}$$

$$\text{et } A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Masque jetable

Le plus célèbre cryptosystème à secret parfait est la technique du masque jetable (one-pad time).

Méthode de chiffrement:

Principe:

- La clé doit être une suite de caractère doit être de la même longueur ou d'une longueur plus grande que les message qu'on veut chiffrer.
- Le choix de la clé est aléatoire et puis on jette la clé. Si on respecte ces règles d'une manière stricte, on obtient un système avec sécurité théorique absolue.

Déchiffrement:

Pour déchiffrer, on procède de la même manière mais avec soustraction du masque du message chiffré.

Masque jetable

Exemple

Chiffrer le mot "TEST" en utilisant la méthode du masque jetable avec clé k=FVEB:

	T	19	+	F	5	=	24	
	E	4	+	V	21	=	25	
Plaintext	S	18	+	E	4	=	22	Ciphertext YZWU
	T	19	+	B	1	=	20	

Chiffrement par transposition

le principe de ce chiffrement est de faire une transposition (un réarrangement) de l'ensemble des caractères pour cacher le sens initial du message. Cette méthode est très peu résistante aux attaques statistiques. il y a plusieurs types de transpositions, par exemple:

Transposition rectangulaire:

- le plaintext est écrit dans un tableau.
- la clé est le tableau.
- La technique de transposition de base consiste à lire le tableau en colonne.

On veut chiffrer le message "Une tortue était, à la tête légère", on choisie par exemple une matrice à 9×3 :

U	N	E	T	O	R	T	U	E
E	T	A	I	T	A	L	A	T
E	T	E	L	E	G	E	R	E

On obtient le cryptogramme: "UEENTTEAETILOTERAGTLEUARETE"

Chiffrement par transposition

Chiffrement à transposition rectangulaire avec clé:

- On combine la transposition avec une substitution simple.
- on réarrange les colonnes selon une permutation (on la considère comme clé).

Exemple

On veut chiffrer le message: "Qui lasse de son trou voulut voir le pays", on choisit un tableau avec 5 lignes et 7 colonnes:

Q	U	I	L	A	S	S
E	D	E	S	O	N	T
R	O	U	V	O	U	L
U	T	V	O	I	R	L
E	P	A	Y	S	M	G

Chiffrement par transposition

Exemple:

On ajoute à ce tableau une clé (mot de passe) définie par le mot : VERLAINE on numérote les lettres par ordre alphabétique:

V	E	R	L	A	I	N	E
1	2	3	4	5	6	7	

et on retire les lettres doublés, la clé devient alors:

V	E	R	L	A	I	N	E
7	2	6	4	1	3	5	

7	2	6	4	1	3	5
Q	U	I	L	A	S	S
E	D	E	S	O	N	T
R	O	U	V	O	U	L
U	T	V	O	I	R	L
E	P	A	Y	S	M	G

Chiffrement par transposition

Exemple:

La dernière étape est de réécrire les colonnes du tableau par ordre alphabétique de la clé:

1	2	3	4	5	6	7
A	U	S	L	S	I	Q
O	D	N	S	T	E	E
O	O	U	V	L	U	R
I	T	R	O	L	V	U
S	P	M	Y	G	A	E

On obtient le cryptogramme: AOOISUDOTPSNURMLSV OYSTLLGIEUVAQERUE.

Mode opératoire

Definition

$$(19) \quad \oplus : \{0, 1\}^2 \rightarrow \{0, 1\}$$

$$(20) \quad (a, b) \mapsto a \oplus b$$

\oplus est appelé XOR ou exclusif.

Mode opératoire

Le mode ECB (Carnet de codage electronique/Electronic code-book

Dans ce type de chiffrement on découpe le message M en bloc m_i de taille n et on chiffre indépendamment chaque m_i avec la clé k .

Exemple

Chiffrement du message $M = 101100010100101$ en utilisant le mode *ECB*.

Avec la clé de permutation:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

Pour chiffrer le message M on découpe le message en bloc de taille 4 après on applique la clé π à chaque bloc:

$$(21) \quad m_1 = 1011 \rightarrow E_\pi(1011) = 0111$$

$$(22) \quad m_2 = 0001 \rightarrow E_\pi(0001) = 0010$$

$$(23) \quad m_3 = 0100 \rightarrow E_\pi(0100) = 1000$$

$$(24) \quad m_4 = 1010 \rightarrow E_\pi(1010) = 0101$$

On obtient le cryptogramme: 0111001010000101.

Le mode CBC (Cipher Bloc Chaining / Chiffrement par chainage de blocs)

On veut chiffrer le message:

$$m = m_1 m_2 \cdots m_t \text{ où } |m_i| = n$$

Fonction de chiffrement:

$$c_j = E_k(c_{j-1} \oplus m_j), 1 \leq j \leq t.$$

Avec $c_0 = v$ (vecteur d'initialisation).

Le cryptogramme est donné par: $c = c_1 c_2 \cdots c_t$.

Mode opératoire

Fonction de déchiffrement:

On veut savoir le m_j , on a:

$$(25) \quad c_j = E_k(c_{j-1} \oplus m_j)$$

$$(26) \quad D_k(c_j) = c_{j-1} \oplus m_j$$

Alors,

$$m_j = D_k(c_j) \oplus c_{j-1}$$

Car:

$$E_k \circ D_k = D_k \circ E_k = I$$

Mode opératoire

Exemple

Chiffrer le message en clair $m_1 m_2 m_3 m_4$ où:

$m_1 = 1011$, $m_2 = 0001$, $m_3 = 0100$, $m_4 = 1010$

avec la clé:

$$k = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

et $v = 1010$

On a: $c_0 = v \Rightarrow c_0 = 1010$ alors:

$c_1 = E_k(1010 \oplus 1011) = E_k(0001) = 0010$





$c_2 = 0110$

$c_3 = 0100$

$c_4 = 1101$

Cryptogramme: $c = 0010011001001101$

References

-  J. Hoffstein, J. Pipher and J. H. Silverman, "An Introduction to Mathematical Cryptography", Springer, Berlin, 2008.
-  D. Stinson, "Cryptography: Theory and Practice. 4th Edition", CRC Press, 2019.
-  J. A. Buchmann , "Introduction to Cryptography", Springer, 2000.
-  L. C. Washington, "Introduction to Cryptography with Coding Theory", Pearson Prentice Hall, 2006.