3. Cryptographie Classique

Noureddine AZZOUZA Riadh MEGHATRIA

[1]Université Djilali BOUNAAMA Khemis Miliana, Algérie

Cours de Sécurité Informatique, M2GLSD

Cryptographie classique

L'essentiel des méthodes de chiffrement classique reposent sur deux principes : la substitution et la transposition.

La substitution

remplacer certaines lettres par d'autres, ou par des symboles.

La transposition

permute les lettres du message afin de le rendre incompréhensible.

Manipulation des caractères

Mot :	C	H	I	F	F	R	E
Code :	03	08	09	06	06	18	05

Clé :	5	7	2	3	6	1	4
Mot :	C	H	I	F	F	R	E

	1	2	3	4	5	6	7
Code:	R	I	F	E	C	F	H

- Ordre respecté
- Message altéré

- Ordre non respecté
- Message non altéré

Chiffrement par substitution mono-alphabétique

Définitions

remplace chaque lettre par une autre lettre de l'alphabet et toujours la même lettre.

Exemples

- Le chiffrement de **César** (décalage de k lettres).
- Le chiffrement par substitution mon-alphabétique à **clé**.
- Le chiffrement **AtBash** (alphabet en sens contraire).
- Le chiffrement **ROT13** (décalage de k=13 lettres).

Chiffrement de César

Chaque lettre du texte en clair est remplacée par une autre lettre a distance fixe dans l'alphabet.

Principe

- décaler les lettres de l'alphabet de k
- Chiffrement : lettre codée = (lettre claire + k) mod 26
- Déchiffrement : lettre claire = (lettre codée - k) mod 26

Exemples

- Utiliser le code de César avec k=3
- Message à chiffrer : "MASTER GLSD"
- Solution : PDVWHU JOVG

Chiffrement par substitution mono-alphabétique à clé

Utiliser un mot pour que le cryptogramme soit déchiffré (Des millions de mots clé possibles).

Principe

1. Choisir un mot clé
2. Le "nettoyer" en enlevant tout les doubles et les accents
3. Reporter ce mot dans le tableau de correspondance
4. Compléter l'alphabet (à partir de la dernière lettre)

Chiffrement par substitution mono-alphabétique à clé

Exemples

- Mot clé : "informatique"
- Mot clé nettoyé : "INFORMATQUE"
- tableau de correspondance :

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
I	N	F	O	R	M	A	T	Q	U	E															

- tableau de correspondance complété :

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

Chiffrement par substitution poly-alphabétique

Définitions

remplacer une lettre par une autre lettre qui n'est pas toujours la même(plusieurs symboles possibles).

Exemples

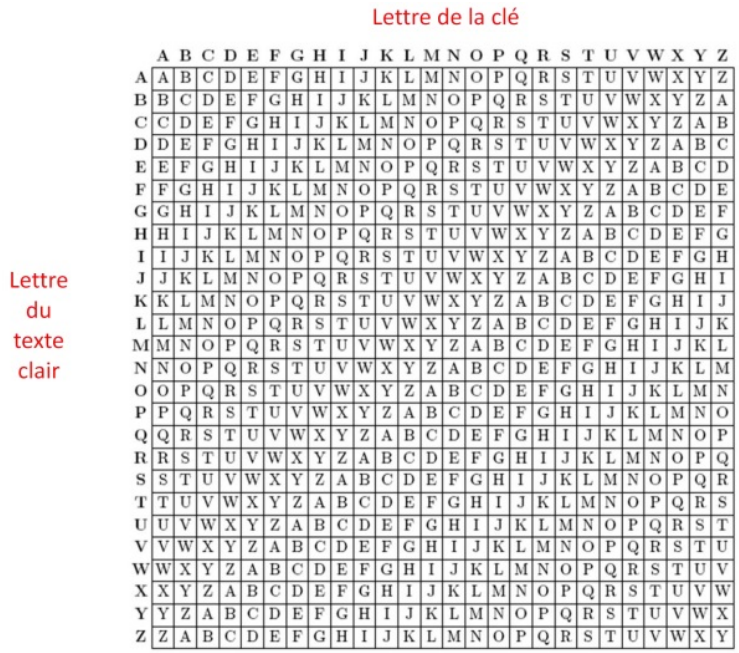
- Le chiffrement de **Vigenère**.
- Le chiffrement de **Venam**.
- Le chiffrement **Jefferson**.
- Le chiffrement **Enigma**.

Chiffrement de Vigenère

Utiliser un chiffre de César, mais avec une table composée de 26 alphabets, écrits dans l'ordre, et décalée à gauche d'un caractère. (Carré de Vigenère).

Principe

- Choisir un mot clé
- écrit la clé sous le message à coder (avec répétition)
- regarde dans le tableau l'intersection de la ligne de la lettre à coder avec la colonne de la lettre de la clé



Chiffrement de Vigenère

Exemple

- Message à codé : "MASTER GLSD"
- Mot clé nettoyé : "CUAT"
- tableau de correspondance :

Texte Clair	M	A	S	T	E	R	G	L	S	D
Clé	C	U	A	T	C	U	A	T	C	U
Texte Chiffré										

- tableau de correspondance complété :

Texte Clair	M	A	S	T	E	R	G	L	S	D
Clé	C	U	A	T	C	U	A	T	C	U
Texte Chiffré	O	U	S	M	G	L	G	E	U	X

Chiffrement de Venam

Appelé également masque jetable est défini comme un chiffrement de Vigenère avec la caractéristique que la clé de chiffrement a la même longueur que le message clair.

Propriétés

- Choisir une clé aussi longue que le texte à chiffrer
- utiliser une clé formée d'une suite de caractères aléatoires
- ne jamais réutiliser une clé

Chiffrement par transposition

Définitions

Le chiffrement par transposition ou permutation consiste à changer uniquement l'ordre des lettres sans faire de substitution.

Exemples

- La méthode **Simple** : Permutation (2, 4, 1, 3).
- La méthode de **ZigZag**.
- La méthode de **la grille** avec clé.

La méthode Zig Zag

Principe

- Écrire : sur 2 ou plusieurs lignes
- Lire : ligne par ligne

Exemples

- Message à chiffrer : "MASTER GLSD"
- Profondeur égale à 2 (2 lignes)

M	S	E	G	S
A	T	R	L	D

- Message chiffré : MSEGSATRLD

Méthode de la grille avec clé

Principe

- écrire : dans une grille rectangulaire ligne par ligne
- Lire : colonne par colonne
- l'ordre : défini par la clé

Exemples

- Message à chiffrer : "MASTER GLSD"
- Clé = TEST (4 lettres ——> 4 colonnes)
- Prendre l'ordre alphabétique définit par la clé
- Message chiffré : ARDSGMESTL

M	A	S	T
E	R	G	L
S	D		

T	E	S	T
3	1	2	4