Ecole Supérieure Polytechnique
Laboratoire d'Informatique,
de Télécommunications et Applications
LITA

Cryptologie Classique

Pr Gervais MENDY
gervais.mendy@esp.sn

Département Génie Informatique, École Supérieure Polytechnique ESP-UCAD

April 2, 2024

Plan

Introduction

Introduction au chiffrement classique

- Les principaux concepts du chiffrement classique sont restés essentiellement les mêmes.

Introduction

Introduction au chiffrement classique

- Les principaux concepts du chiffrement classique sont restés essentiellement les mêmes.
- Le chiffrement regroupe les techniques mises en œuvre pour brouiller la signification d'un message qui est matériellement visible.

Introduction

Introduction au chiffrement classique

- Les principaux concepts du chiffrement classique sont restés essentiellement les mêmes.
- Le chiffrement regroupe les techniques mises en œuvre pour brouiller la signification d'un message qui est matériellement visible.
- Le contenu du message ne doit alors être retrouvé que par les personnes auxquelles le message est adressé.

Introduction

Introduction au chiffrement classique

- Les principaux concepts du chiffrement classique sont restés essentiellement les mêmes.
- Le chiffrement regroupe les techniques mises en œuvre pour brouiller la signification d'un message qui est matériellement visible.
- Le contenu du message ne doit alors être retrouvé que par les personnes auxquelles le message est adressé.
- La substitution consiste à remplacer, sans en bouleverser l'ordre, les symboles d'un texte clair par d'autres symboles

Introduction

Introduction au chiffrement classique

- Les principaux concepts du chiffrement classique sont restés essentiellement les mêmes.
- Le chiffrement regroupe les techniques mises en œuvre pour brouiller la signification d'un message qui est matériellement visible.
- Le contenu du message ne doit alors être retrouvé que par les personnes auxquelles le message est adressé.
- La substitution consiste à remplacer, sans en bouleverser l'ordre, les symboles d'un texte clair par d'autres symboles
- La transposition repose sur le bouleversement de l'ordre des symboles (mais pas leur identité).

Types de base de substitution

- Le ***chiffrement à substitution simple*** est un chiffrement dans lequel chaque caractère du texte en clair est remplacé par un caractère correspondant dans le texte chiffré.

Types de base de substitution

- Le ***chiffrement à substitution simple*** est un chiffrement dans lequel chaque caractère du texte en clair est remplacé par un caractère correspondant dans le texte chiffré.
- Le ***chiffrement à substitution homophonique*** ou ***chiffrement à substitution simple à représentation multiple*** est comme un chiffrement à substitution simple, sauf qu'à un caractère du texte en clair on fait correspondre plusieurs caractères dans le texte chiffré.

Types de base de substitution

- Le ***chiffrement à substitution simple*** est un chiffrement dans lequel chaque caractère du texte en clair est remplacé par un caractère correspondant dans le texte chiffré.
- Le ***chiffrement à substitution homophonique*** ou ***chiffrement à substitution simple à représentation multiple*** est comme un chiffrement à substitution simple, sauf qu'à un caractère du texte en clair on fait correspondre plusieurs caractères dans le texte chiffré.
- Le ***chiffrement à substitution simple par polygrammes*** est un chiffrement pour lequel les caractères sont chiffrés par bloc.

Types de base de substitution

- Le ***chiffrement à substitution simple*** est un chiffrement dans lequel chaque caractère du texte en clair est remplacé par un caractère correspondant dans le texte chiffré.
- Le ***chiffrement à substitution homophonique*** ou ***chiffrement à substitution simple à représentation multiple*** est comme un chiffrement à substitution simple, sauf qu'à un caractère du texte en clair on fait correspondre plusieurs caractères dans le texte chiffré.
- Le ***chiffrement à substitution simple par polygrammes*** est un chiffrement pour lequel les caractères sont chiffrés par bloc.
- Le ***chiffrement à substitution poly-alphabétique*** est composé à partir de plusieurs chiffrements à substitution simple.

Cryptosystème

Définition

- Soit $\mathcal{A}$ un alphabet fini dont les constituants sont appelés symboles.

Cryptosystème

Définition

- Soit $\mathcal{A}$ un alphabet fini dont les constituants sont appelés symboles.
- Si x est une chaîne sur $\mathcal{A}$ alors on note $x[i]$ son i-ième symbole.

Cryptosystème

Définition

- Soit $\mathcal{A}$ un alphabet fini dont les constituants sont appelés symboles.
- Si x est une chaîne sur $\mathcal{A}$ alors on note $x[i]$ son i-ième symbole.
- Si x est une chaîne alors $|x|$ désigne la longueur de x, c'est-à-dire le nombre de symboles qu'elle contient.

Cryptosystème

Définition

- Soit $\mathcal{A}$ un alphabet fini dont les constituants sont appelés symboles.
- Si x est une chaîne sur $\mathcal{A}$ alors on note $x[i]$ son i-ième symbole.
- Si x est une chaîne alors $|x|$ désigne la longueur de x, c'est-à-dire le nombre de symboles qu'elle contient.
- Une permutation π sur un ensemble S est une application $\pi : S \longrightarrow S$ bijective.

Définition (suite)

On appelle système cryptographique ou cryptosystème un triplet $(\mathcal{P}, \mathcal{C}, \mathcal{K})$ satisfaisant les conditions suivantes :

- $\mathcal{P}$ est l'ensemble fini des textes clairs possibles (plaintexts),

Définition (suite)

On appelle système cryptographique ou cryptosystème un triplet $(\mathcal{P}, \mathcal{C}, \mathcal{K})$ satisfaisant les conditions suivantes :

- $\mathcal{P}$ est l'ensemble fini des textes clairs possibles (plaintexts),
- $\mathcal{C}$ est l'ensemble fini des textes chiffrés possibles (ciphertexts),

Définition (suite)

On appelle système cryptographique ou cryptosystème un triplet $(\mathcal{P}, \mathcal{C}, \mathcal{K})$ satisfaisant les conditions suivantes :

- $\mathcal{P}$ est l'ensemble fini des textes clairs possibles (plaintexts),
- $\mathcal{C}$ est l'ensemble fini des textes chiffrés possibles (ciphertexts),
- $\mathcal{K}$ est l'ensemble fini des clés possibles, appelé parfois espace des clés (keys),

Définition (suite)

On appelle système cryptographique ou cryptosystème un triplet $(\mathcal{P}, \mathcal{C}, \mathcal{K})$ satisfaisant les conditions suivantes :

- $\mathcal{P}$ est l'ensemble fini des textes clairs possibles (plaintexts),
- $\mathcal{C}$ est l'ensemble fini des textes chiffrés possibles (ciphertexts),
- $\mathcal{K}$ est l'ensemble fini des clés possibles, appelé parfois espace des clés (keys),
- Pour tout $k \in \mathcal{K}$, il existe une fonction de chiffrement E_k telle que

$$E_k : \mathcal{P} \longrightarrow \mathcal{C} : \quad t \longmapsto E_k(t)$$

et il existe une fonction de déchiffrement D_k telle que

$$D_k : \mathcal{C} \longrightarrow \mathcal{P} : \quad t \longmapsto D_k(t)$$

et $\quad \forall\, t \in \mathcal{P}, \quad D_k(E_k(t)) = t.$

Définition (suite 1)

Un chiffrement par substitution sur l'alphabet $\mathcal{A}$ est un cas particulier de schéma de chiffrement symétrique dans lequel la sortie de l'algorithme de génération de clé $\mathcal{K}$ est toujours une permutation sur $\mathcal{A}$ et les algorithmes de chiffrement et de déchiffrement sont les suivants:

Algorithme $E_\pi(M)$
Pour $i = 1$ jusqu'à $|M|$ faire
$C[i] \longleftarrow \pi(M[i])$
Retourner C

Algorithme $D_\pi(C)$
Pour $i = 1$ jusqu'à $|C|$ faire
$M[i] \longleftarrow \pi^{-1}(C[i])$
Retourner M

Substitution mono-alphabétique

Chiffrement de César

- Le chiffrement par substitution mono-alphabétique le plus simple est le *chiffrement par décalage*, aussi connu sous le nom de *chiffrement de César*.

Substitution mono-alphabétique

Chiffrement de César

- Le chiffrement par substitution mono-alphabétique le plus simple est le *chiffrement par décalage*, aussi connu sous le nom de *chiffrement de César*.
- Il consiste simplement à décaler les lettres de l'alphabet d'un nombre de positions constant vers la droite ou la gauche.

Substitution mono-alphabétique

Chiffrement de César

- Le chiffrement par substitution mono-alphabétique le plus simple est le *chiffrement par décalage*, aussi connu sous le nom de *chiffrement de César*.
- Il consiste simplement à décaler les lettres de l'alphabet d'un nombre de positions constant vers la droite ou la gauche.
- De façon simpliste mais formelle, le chiffrement par décalage peut être décrit en posant $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$ et pour tout $k \in \{0, \ldots, 25\}$,

Substitution mono-alphabétique

Chiffrement de César

- Le chiffrement par substitution mono-alphabétique le plus simple est le *chiffrement par décalage*, aussi connu sous le nom de *chiffrement de César*.
- Il consiste simplement à décaler les lettres de l'alphabet d'un nombre de positions constant vers la droite ou la gauche.
- De façon simpliste mais formelle, le chiffrement par décalage peut être décrit en posant $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$ et pour tout $k \in \{0, \ldots, 25\}$,
- $E_k(x) = (x + k) \mod 26$ et $D_k(y) = (y - k) \mod 26$.

Substitution mono-alphabétique

Chiffrement de César (suite)

- Pour $k = 3$, le chiffrement est appelé chiffrement de César. Dans ce cas particulier du décalage circulaire, il n'y a que 26 clés possibles.

Substitution mono-alphabétique

Chiffrement de César (suite)

- Pour $k = 3$, le chiffrement est appelé chiffrement de César. Dans ce cas particulier du décalage circulaire, il n'y a que 26 clés possibles.
- Le système n'est donc pas fiable: on peut essayer tous les décalages possibles jusqu'à obtenir un texte intelligible.

Substitution mono-alphabétique

Chiffrement de César (suite)

- Pour $k = 3$, le chiffrement est appelé chiffrement de César. Dans ce cas particulier du décalage circulaire, il n'y a que 26 clés possibles.
- Le système n'est donc pas fiable: on peut essayer tous les décalages possibles jusqu'à obtenir un texte intelligible.
- Dans le cas général, il y a 26! permutations possibles et la taille de l'espace des clés est amplement suffisante.

Substitution mono-alphabétique

Chiffrement de César (suite)

- Pour $k = 3$, le chiffrement est appelé chiffrement de César. Dans ce cas particulier du décalage circulaire, il n'y a que 26 clés possibles.
- Le système n'est donc pas fiable: on peut essayer tous les décalages possibles jusqu'à obtenir un texte intelligible.
- Dans le cas général, il y a 26! permutations possibles et la taille de l'espace des clés est amplement suffisante.
- Pourtant, ce système est cassé par la cryptanalyse statistique car dans une langue usuelle telle que le français, les lettres n'apparaissent pas toutes avec les mêmes fréquences.

Substitution mono-alphabétique

Chiffrement affine

- Le chiffrement affine est un système de chiffrement par substitution mono-alphabétique.

Substitution mono-alphabétique

Chiffrement affine

- Le chiffrement affine est un système de chiffrement par substitution mono-alphabétique.
- La clé consiste en un couple d'entiers $(a, b) \in \mathbb{Z}_{26}^* \times \mathbb{Z}_{26}$.

Substitution mono-alphabétique

Chiffrement affine

- Le chiffrement affine est un système de chiffrement par substitution mono-alphabétique.
- La clé consiste en un couple d'entiers $(a, b) \in \mathbb{Z}_{26}^* \times \mathbb{Z}_{26}$.
- Chaque lettre du texte clair de rang $i \in \{0, \ldots, 25\}$ est remplacée dans le texte chiffré par la lettre de rang $a \cdot i + b \mod 26$.

Substitution mono-alphabétique

Chiffrement affine

- Le chiffrement affine est un système de chiffrement par substitution mono-alphabétique.
- La clé consiste en un couple d'entiers $(a, b) \in \mathbb{Z}_{26}^* \times \mathbb{Z}_{26}$.
- Chaque lettre du texte clair de rang $i \in \{0, \ldots, 25\}$ est remplacée dans le texte chiffré par la lettre de rang $a \cdot i + b \mod 26$.
- Puisque a est inversible dans $\mathbb{Z}_{26}$, cette transformation est bien une permutation de $\mathbb{Z}_{26}$.

Substitution mono-alphabétique

Chiffrement affine (suite)

- De façon formelle, nous posons $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$.

Substitution mono-alphabétique

Chiffrement affine (suite)

- De façon formelle, nous posons $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$.
- Nous considérons a et b appartenant à $\mathbb{Z}_n$ avec a inversible dans $\mathbb{Z}_n$ (i.e., $pgcd(a, n) = 1$).

Substitution mono-alphabétique

Chiffrement affine (suite)

- De façon formelle, nous posons $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$.
- Nous considérons a et b appartenant à $\mathbb{Z}_n$ avec a inversible dans $\mathbb{Z}_n$ (i.e., $pgcd(a, n) = 1$).
- Ainsi, on a

$$\mathcal{K} = \{(a, b) \quad | \quad a \in \mathbb{Z}_n^*, b \in \mathbb{Z}_n\}$$

et pour une clé $k = (a, b)$ choisie dans $\mathcal{K}$, on a $E_k(x) = ax + b \mod n$ et $D_k(y) = a^{-1}(y - b) \mod n$.

Substitution mono-alphabétique

Chiffrement affine (suite)

- De façon formelle, nous posons $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$.
- Nous considérons a et b appartenant à $\mathbb{Z}_n$ avec a inversible dans $\mathbb{Z}_n$ (i.e., $pgcd(a, n) = 1$).
- Ainsi, on a

$$\mathcal{K} = \{(a, b) \quad | \quad a \in \mathbb{Z}_n^*, b \in \mathbb{Z}_n\}$$

  et pour une clé $k = (a, b)$ choisie dans $\mathcal{K}$, on a $E_k(x) = ax + b \mod n$ et $D_k(y) = a^{-1}(y - b) \mod n$.
- Le nombre de clés est bien évidemment $\phi(n)$.

Chiffrement homophonique

- Pour le chiffrement homophonique, il s'agit de remplacer une lettre non pas par un symbole ***unique***, mais par un symbole choisi au hasard parmi plusieurs.

Chiffrement homophonique

- Pour le chiffrement homophonique, il s'agit de remplacer une lettre non pas par un symbole ***unique***, mais par un symbole choisi au hasard parmi plusieurs.
- Dans sa version la plus sophistiquée, on choisira un nombre des symboles proportionnel à la fréquence d'apparition de la lettre. Ainsi, on obtient un renversement des fréquences ce qui permet de faire disparaître complètement les indications fournies par la fréquence.

Chiffrement homophonique

- Pour le chiffrement homophonique, il s'agit de remplacer une lettre non pas par un symbole ***unique***, mais par un symbole choisi au hasard parmi plusieurs.
- Dans sa version la plus sophistiquée, on choisira un nombre des symboles proportionnel à la fréquence d'apparition de la lettre. Ainsi, on obtient un renversement des fréquences ce qui permet de faire disparaître complètement les indications fournies par la fréquence.
- Dans sa version la plus sophistiquée, on choisira un nombre des symboles proportionnel à la fréquence d'apparition de la lettre. Ainsi, on obtient un renversement des fréquences ce qui permet de faire disparaître complètement les indications fournies par la fréquence.

Substitution simple et substitution polygrammique

- Les substitutions simples sont sensibles à l'analyse des fréquences, qui consiste à compter les occurrences des caractères et à comparer le résultat avec la distribution des lettres dans la langue du texte en clair.

Substitution simple et substitution polygrammique

- Les substitutions simples sont sensibles à l'analyse des fréquences, qui consiste à compter les occurrences des caractères et à comparer le résultat avec la distribution des lettres dans la langue du texte en clair.
- Une substitution polygrammique est une substitution simple sur des groupements de plusieurs lettres. Par exemple, dans une substitution bigrammique, deux lettres du texte clair sont transformées en deux lettres du cryptogramme.

Substitution simple et substitution polygrammique

- Les substitutions simples sont sensibles à l'analyse des fréquences, qui consiste à compter les occurrences des caractères et à comparer le résultat avec la distribution des lettres dans la langue du texte en clair.
- Une substitution polygrammique est une substitution simple sur des groupements de plusieurs lettres. Par exemple, dans une substitution bigrammique, deux lettres du texte clair sont transformées en deux lettres du cryptogramme.
- Cela rend plus difficile l'analyse des fréquences puisqu'il faut disposer cette fois de statistiques sur les groupements de deux lettres.

Substitution simple et substitution polygrammique

- Les substitutions simples sont sensibles à l'analyse des fréquences, qui consiste à compter les occurrences des caractères et à comparer le résultat avec la distribution des lettres dans la langue du texte en clair.
- Une substitution polygrammique est une substitution simple sur des groupements de plusieurs lettres. Par exemple, dans une substitution bigrammique, deux lettres du texte clair sont transformées en deux lettres du cryptogramme.
- Cela rend plus difficile l'analyse des fréquences puisqu'il faut disposer cette fois de statistiques sur les groupements de deux lettres.
- En générale, il s'agit ici de chiffrer un groupe de l lettres par un autre groupe de l symboles.

Chiffrement polygrammique

Chiffrement de Playfair

- Ce chiffrement utilise un carré de vingt-cinq cases rempli avec les lettres de l'alphabet.

Chiffrement polygrammique

Chiffrement de Playfair

- Ce chiffrement utilise un carré de vingt-cinq cases rempli avec les lettres de l'alphabet.
- En français, on peut omettre le *w*, ou bien en anglais fusionner le *i* et le *j*.

Chiffrement polygrammique

Chiffrement de Playfair

- Ce chiffrement utilise un carré de vingt-cinq cases rempli avec les lettres de l'alphabet.
- En français, on peut omettre le *w*, ou bien en anglais fusionner le *i* et le *j*.
- Un procédé pour remplir ce carré est par exemple de convenir d'une phrase, d'écrire les lettres de cette phrase dans le carré sans les répéter, puis de compléter le carré avec les lettres manquantes dans l'ordre alphabétique.

Chiffrement polygrammique

Exemple de chiffrement de Playfair

La phrase convenue, « **promenade cryptologique** », conduira au carré ci -dessous.

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

Figure: Chiffrement de Playfair

Deux lettres du texte clair sont transformées en deux lettres du cryptogramme selon leur disposition dans ce carré :

Chiffrement polygrammique

Exemple de chiffrement de Playfair (suite)

- les lettres doubles du texte clair sont éliminées en insérant entre elles une lettre rare comme par exemple le K ;

Chiffrement polygrammique

Exemple de chiffrement de Playfair (suite)

- les lettres doubles du texte clair sont éliminées en insérant entre elles une lettre rare comme par exemple le K ;
- si deux lettres sont sur une même ligne ou une même colonne, les lettres du cryptogramme sont les suivantes sur la ligne ou sur la colonne en convenant d'un sens, par exemple de haut en bas et de gauche à droite ;

Chiffrement polygrammique

Exemple de chiffrement de Playfair (suite)

- les lettres doubles du texte clair sont éliminées en insérant entre elles une lettre rare comme par exemple le K ;
- si deux lettres sont sur une même ligne ou une même colonne, les lettres du cryptogramme sont les suivantes sur la ligne ou sur la colonne en convenant d'un sens, par exemple de haut en bas et de gauche à droite ;
- si les deux lettres forment les diagonales d'un rectangle, les lettres du cryptogramme sont les extrémités de l'autre diagonale en convenant d'un sens de rotation, par exemple dans le sens des aiguilles d'une montre.

Chiffrement polygrammique

Exemple de chiffrement de Playfair (suite 1)

Voici illustré le chiffrement du message « *l'attente est toujours longue* » :

clair :		LA	TK	TE	NT	EK	ES	TK	TO	UJ	OU	RS
	LO	NG	UE									
cryptogramme :		BL	UP	PQ	TU	ZP	ZR	UP	PG	BU	FP	AR
	RG	DT	PJ									

Chiffrement polygrammique

Chiffrement de Hill

On présente ci-après un exemple où les lettres sont regroupées deux par deux.

- Leur codage représente des couples de nombres.

Chiffrement polygrammique

Chiffrement de Hill

On présente ci-après un exemple où les lettres sont regroupées deux par deux.

- Leur codage représente des couples de nombres.
- Le chiffrement consiste à appliquer sur ces nombres un calcul linéaire.

Chiffrement polygrammique

Chiffrement de Hill

On présente ci-après un exemple où les lettres sont regroupées deux par deux.

- Leur codage représente des couples de nombres.
- Le chiffrement consiste à appliquer sur ces nombres un calcul linéaire.
- Les correspondants conviennent de quatre paramètres a, b, c, et d.

Chiffrement polygrammique

Chiffrement de Hill

On présente ci-après un exemple où les lettres sont regroupées deux par deux.

- Leur codage représente des couples de nombres.
- Le chiffrement consiste à appliquer sur ces nombres un calcul linéaire.
- Les correspondants conviennent de quatre paramètres a, b, c, et d.
- Le couple de nombres (x, y) est transformé en un couple de nombres (u, v) en appliquant les formules suivantes:

$$\begin{cases} u = ax + by \pmod{26} \\ v = cx + dy \pmod{26} \end{cases} \quad (1)$$

Chiffrement polygrammique

Chiffrement de Hill (suite)

$$\begin{cases} u = ax + by \pmod{26} \\ v = cx + dy \pmod{26} \end{cases} \tag{2}$$

La traduction matricielle du système d'équations 2 sera:

$$\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{26}$$

- La matrice doit être inversible dans $\mathbb{Z}_{26}$.

Chiffrement polygrammique

Chiffrement de Hill (suite)

$$\begin{cases} u = ax + by \pmod{26} \\ v = cx + dy \pmod{26} \end{cases} \tag{2}$$

La traduction matricielle du système d'équations 2 sera:

$$\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{26}$$

- La matrice doit être inversible dans $\mathbb{Z}_{26}$.
- Sa taille n'est pas fixée à 2.

Chiffrement polygrammique

Chiffrement de Hill (suite)

$$\begin{cases} u = ax + by \pmod{26} \\ v = cx + dy \pmod{26} \end{cases} \tag{2}$$

La traduction matricielle du système d'équations 2 sera:

$$\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{26}$$

- La matrice doit être inversible dans $\mathbb{Z}_{26}$.
- Sa taille n'est pas fixée à 2.
- Elle grandira selon le nombre de lettres à chiffrer simultanément.

Polyalphabétisme

Contexte

- Inconvénient majeur des substitutions simples: la grande sensibilité à l'analyse des fréquences.

Polyalphabétisme

Contexte

- Inconvénient majeur des substitutions simples: la grande sensibilité à l'analyse des fréquences.
- Les chiffrements homophoniques et les substitutions polygrammiques sont des tentatives pour contrer cette faiblesse.

Polyalphabétisme

Contexte

- Inconvénient majeur des substitutions simples: la grande sensibilité à l'analyse des fréquences.
- Les chiffrements homophoniques et les substitutions polygrammiques sont des tentatives pour contrer cette faiblesse.
- Mais le progrès essentiel a été le polyalphabétisme.

Polyalphabétisme

Contexte

- Inconvénient majeur des substitutions simples: la grande sensibilité à l'analyse des fréquences.
- Les chiffrements homophoniques et les substitutions polygrammiques sont des tentatives pour contrer cette faiblesse.
- Mais le progrès essentiel a été le polyalphabétisme.
- Il met en œuvre plusieurs alphabets.

Polyalphabétisme

Contexte

- Inconvénient majeur des substitutions simples: la grande sensibilité à l'analyse des fréquences.
- Les chiffrements homophoniques et les substitutions polygrammiques sont des tentatives pour contrer cette faiblesse.
- Mais le progrès essentiel a été le polyalphabétisme.
- Il met en œuvre plusieurs alphabets.
- Une même lettre du message sera codée par des lettres différentes dans le cryptogramme.

Polyalphabétisme

Contexte (suite)

- L'utilisation de plusieurs alphabets pour effectuer le chiffrement entraîne des chiffrements différents pour une même lettre et des occurrences différentes d'une même lettre dans le texte chiffré.

Polyalphabétisme

Contexte (suite)

- L'utilisation de plusieurs alphabets pour effectuer le chiffrement entraîne des chiffrements différents pour une même lettre et des occurrences différentes d'une même lettre dans le texte chiffré.
- En particulier, une cryptanalyse par analyse fréquentielle d'un chiffrement par substitution poly-alphabétique doit utiliser des techniques plus évoluées que pour des substitutions mono-alphabétiques.

Polyalphabétisme

Chiffrement de Vigenère

- Le *chiffrement de Vigenère* repose sur l'utilisation périodique de plusieurs alphabets de substitution déterminés par la clé (en général un mot).

Polyalphabétisme

Chiffrement de Vigenère

- Le *chiffrement de Vigenère* repose sur l'utilisation périodique de plusieurs alphabets de substitution déterminés par la clé (en général un mot).
- Pour pouvoir chiffrer un texte clair, à chaque caractère on associe une lettre de la clé pour effectuer le décalage correspondant comme dans le chiffrement de César.

Polyalphabétisme

Chiffrement de Vigenère

- Le *chiffrement de Vigenère* repose sur l'utilisation périodique de plusieurs alphabets de substitution déterminés par la clé (en général un mot).
- Pour pouvoir chiffrer un texte clair, à chaque caractère on associe une lettre de la clé pour effectuer le décalage correspondant comme dans le chiffrement de César.
- Ainsi le texte clair « *vigenere* » chiffré avec la clé « *cle* » devient le chiffré « *xtkgyitp* ».

Polyalphabétisme

Chiffrement de Vigenère

- Le *chiffrement de Vigenère* repose sur l'utilisation périodique de plusieurs alphabets de substitution déterminés par la clé (en général un mot).
- Pour pouvoir chiffrer un texte clair, à chaque caractère on associe une lettre de la clé pour effectuer le décalage correspondant comme dans le chiffrement de César.
- Ainsi le texte clair « *vigenere* » chiffré avec la clé « *cle* » devient le chiffré « *xtkgyitp* ».
- En effet, la lettre *v* chiffrée avec la lettre *c* est décalée de deux positions, la lettre *i* est chiffrée avec la lettre *l* et la lettre *g* chiffrée avec la lettre *e*. Ensuite, la lettre *e* est chiffrée avec la lettre *c* et ainsi de suite de façon périodique.

Polyalphabétisme

Chiffrement de Vigenère (suite)

En particulier, si la longueur de la clé l est connue, retrouver le texte clair à partir du texte chiffré c peut se faire en appliquant une cryptanalyse du chiffrement de César pour chaque sous-chiffré c_i de c formé uniquement des lettres dont les positions sont congrues à i modulo l (pour $i \in \{0, \ldots, l-1\}$).

La difficulté pour le cryptanalyste consiste donc à retrouver la longueur de la clé.

Cryptanalyse du chiffrement de Vigenère

Méthode de Kasiski

- Elle repose sur le fait que si deux groupes de lettres (ou polygrammes) du chiffré sont égaux alors il s'agit probablement du même polygramme dans le texte clair chiffré avec la même partie de la clé.

Cryptanalyse du chiffrement de Vigenère

Méthode de Kasiski

- Elle repose sur le fait que si deux groupes de lettres (ou polygrammes) du chiffré sont égaux alors il s'agit probablement du même polygramme dans le texte clair chiffré avec la même partie de la clé.
- La taille de l'intervalle qui sépare ces deux polygrammes identiques dans le chiffré sera donc, dans la majorité des cas, un multiple du nombre de la longueur de la clé.

Cryptanalyse du chiffrement de Vigenère

Méthode de Kasiski

- Elle repose sur le fait que si deux groupes de lettres (ou polygrammes) du chiffré sont égaux alors il s'agit probablement du même polygramme dans le texte clair chiffré avec la même partie de la clé.
- La taille de l'intervalle qui sépare ces deux polygrammes identiques dans le chiffré sera donc, dans la majorité des cas, un multiple du nombre de la longueur de la clé.
- S'il y a plusieurs répétitions de polygrammes, le plus grand commun diviseur (*pgcd*) des distances les séparant est très probablement la taille de clé.

Chiffrement de Vigenère

Méthode générale

Elle repose sur le calcul de l'indice de coïncidence qui détermine la probabilité de répétition des lettres dans un message chiffré. L'indice se calcule par la formule suivante:

$$I = \sum_{i=0}^{25} \frac{n_i(n_i - 1)}{n(n-1)}$$

où n_i est le nombre de lettres de rang i dans le texte chiffré (pour $i \in \{0, \ldots, 25\}$) et n la longueur du texte chiffré. Dans le cas d'un texte aléatoire (i.e. où les lettres sont tirées uniformément aléatoires dans l'alphabet $\{a, b, \ldots, z\}$), l'indice de coïncidence est égal à $0,0385$.

Chiffrement de Vigenère

Méthode formelle

Le chiffrement de Vigenère traite m symboles simultanément. Il s'agit en quelque sorte de m chiffrements par substitution. Ici,
$\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{26})^m$,
si $k = (k_1, \ldots, k_m) \in (\mathbb{Z}_{26})^m$, alors

$$E_k(x_1, \ldots, x_m) = (x_1 + k_1, \ldots, x_m + k_m) \mod 26,$$

$$D_k(y_1, \ldots, y_m) = (y_1 - k_1, \ldots, y_m - k_m) \mod 26.$$

On peut convenir que pour chiffrer une suite de longueur $rm + s$ constituée de r $m-uples$ d'éléments de $\mathbb{Z}_{26}$ suivie d'un $s-uple$ d'éléments de $\mathbb{Z}_{26}$ avec $0 \leq s < m$,

$$x = x_1 \cdots x_m | \cdots | x_{(r-1)m+1} \cdots x_{rm} | x_{rm+1} \cdots x_{rm+s},$$

Chiffrement de Vigenère

Méthode formelle (suite)

on calculera

$$y = (x_1 + k_1) \cdots (x_m + k_m) | \cdots | (x_{(r-1)m+1} + k_1) \cdots (x_{rm} + k_m) | \\ (x_{rm+1} + k_1) \cdots (x_{rm+s} + k_s) \mod 26.$$

Dans le chiffrement de Vigenère, un même symbole peut être transformé en m symboles distincts suivant la position qu'occupe ce symbole dans un $m - uplet$ donné. La cryptanalyse du chiffrement de Vigenere peut être réalisée assez facilement par le test de Kasiski ou l'utilisation d'un indice de coïncidence.

Chiffrement par transposition

Définition

C'est un système de chiffrement qui consiste à bouleverser l'ordre des données à chiffrer (de façon à les rendre incompréhensibles) sans pour autant remplacer les lettres du message par d'autres lettres ou symboles.

- Il s'agit généralement de réordonner géométriquement les données pour les rendre visuellement inexploitables.

Chiffrement par transposition

Définition

C'est un système de chiffrement qui consiste à bouleverser l'ordre des données à chiffrer (de façon à les rendre incompréhensibles) sans pour autant remplacer les lettres du message par d'autres lettres ou symboles.

- Il s'agit généralement de réordonner géométriquement les données pour les rendre visuellement inexploitables.
- Il ne modifie pas les lettres du message clair.

Chiffrement par transposition

Définition

C'est un système de chiffrement qui consiste à bouleverser l'ordre des données à chiffrer (de façon à les rendre incompréhensibles) sans pour autant remplacer les lettres du message par d'autres lettres ou symboles.

- Il s'agit généralement de réordonner géométriquement les données pour les rendre visuellement inexploitables.
- Il ne modifie pas les lettres du message clair.
- Le texte chiffré aura exactement la même fréquence de lettres que le texte clair original.

Chiffrement par transposition

Définition

C'est un système de chiffrement qui consiste à bouleverser l'ordre des données à chiffrer (de façon à les rendre incompréhensibles) sans pour autant remplacer les lettres du message par d'autres lettres ou symboles.

- Il s'agit généralement de réordonner géométriquement les données pour les rendre visuellement inexploitables.
- Il ne modifie pas les lettres du message clair.
- Le texte chiffré aura exactement la même fréquence de lettres que le texte clair original.
- Le système est simple, mais peu sûre pour de très brefs messages car il y a peu de variantes.

Chiffrement par transposition

Définition (suite)

- Ainsi, un mot de trois lettres ne pourra être transposé que dans $6 (= 3!)$ positions différentes.

Chiffrement par transposition

Définition (suite)

- Ainsi, un mot de trois lettres ne pourra être transposé que dans $6 (= 3!)$ positions différentes.
- Par exemple, "col" ne peut se transformer qu'en "col", "clo", "ocl", "olc", "lco" et "loc".

Chiffrement par transposition

Définition (suite)

- Ainsi, un mot de trois lettres ne pourra être transposé que dans $6 (= 3!)$ positions différentes.
- Par exemple, "col" ne peut se transformer qu'en "col", "clo", "ocl", "olc", "lco" et "loc".
- Lorsque le nombre de lettres croît, il devient de plus en plus difficile de retrouver le texte original sans connaître le procédé de brouillage.

Chiffrement par transposition

Définition (suite)

- Ainsi, un mot de trois lettres ne pourra être transposé que dans $6 (= 3!)$ positions différentes.
- Par exemple, "col" ne peut se transformer qu'en "col", "clo", "ocl", "olc", "lco" et "loc".
- Lorsque le nombre de lettres croît, il devient de plus en plus difficile de retrouver le texte original sans connaître le procédé de brouillage.
- Ainsi, une phrase de 35 lettres peut être disposée de $35! = 10^{40}$ manières différentes.

Chiffrement par transposition

Définition (suite)

- Ainsi, un mot de trois lettres ne pourra être transposé que dans $6 (= 3!)$ positions différentes.
- Par exemple, "col" ne peut se transformer qu'en "col", "clo", "ocl", "olc", "lco" et "loc".
- Lorsque le nombre de lettres croît, il devient de plus en plus difficile de retrouver le texte original sans connaître le procédé de brouillage.
- Ainsi, une phrase de 35 lettres peut être disposée de $35! = 10^{40}$ manières différentes.
- Ce chiffrement nécessite un procédé rigoureux convenu auparavant entre les parties.

Cryptosystème à clef secrète

Longueur des clefs

- La sécurité d'un cryptosystème à clef secrète dépend de deux choses:

Cryptosystème à clef secrète

Longueur des clefs

- La sécurité d'un cryptosystème à clef secrète dépend de deux choses:
- la solidité de l'algorithme

Cryptosystème à clef secrète

Longueur des clefs

- La sécurité d'un cryptosystème à clef secrète dépend de deux choses:
- la solidité de l'algorithme
- la longueur de la clef

Cryptosystème à clef secrète

Longueur des clefs

- La sécurité d'un cryptosystème à clef secrète dépend de deux choses:
- la solidité de l'algorithme
- la longueur de la clef
- La première caractéristique est plus importante mais la deuxième est plus facile à illustrer.

Longueur des clefs

Solidité de l'algorithme

- **Hypothèse forte**: la solidité de l'algorithme est parfaite.

Longueur des clefs

Solidité de l'algorithme

- **Hypothèse forte**: la solidité de l'algorithme est parfaite.
- C'est-à-dire le seul moyen de casser le cryptosystème est d'essayer toutes les clefs possibles.

Longueur des clefs

Solidité de l'algorithme

- **Hypothèse forte**: la solidité de l'algorithme est parfaite.
- C'est-à-dire le seul moyen de casser le cryptosystème est d'essayer toutes les clefs possibles.
- On parlera alors d'**attaque exhaustive**.

Longueur des clefs

Solidité de l'algorithme

- **Hypothèse forte**: la solidité de l'algorithme est parfaite.
- C'est-à-dire le seul moyen de casser le cryptosystème est d'essayer toutes les clefs possibles.
- On parlera alors d'**attaque exhaustive**.
- Pour lancer une telle attaque, un cryptanalyste a besoin d'un petit bout de texte chiffré et du texte en clair correspondant.

Longueur des clefs

Solidité de l'algorithme

- **Hypothèse forte**: la solidité de l'algorithme est parfaite.
- C'est-à-dire le seul moyen de casser le cryptosystème est d'essayer toutes les clefs possibles.
- On parlera alors d'**attaque exhaustive**.
- Pour lancer une telle attaque, un cryptanalyste a besoin d'un petit bout de texte chiffré et du texte en clair correspondant.
- une attaque exhaustive est une attaque à texte en clair connu.

Longueur des clefs

complexité d'une attaque exhaustive

- Si la clef a 8 bits, il y a $2^8 = 256$ clefs possibles.

Longueur des clefs

complexité d'une attaque exhaustive

- Si la clef a 8 bits, il y a $2^8 = 256$ clefs possibles.
- Il faudra donc 256 tentatives pour trouver la bonne clef et en moyenne 128 suffiront.

Longueur des clefs

complexité d'une attaque exhaustive

- Si la clef a 8 bits, il y a $2^8 = 256$ clefs possibles.
- Il faudra donc 256 tentatives pour trouver la bonne clef et en moyenne 128 suffiront.
- Si la clef a 56 bits, il y a alors $2^{56} \approx 7,2 \times 10^{16}$ clefs possibles.

Longueur des clefs

complexité d'une attaque exhaustive

- Si la clef a 8 bits, il y a $2^8 = 256$ clefs possibles.
- Il faudra donc 256 tentatives pour trouver la bonne clef et en moyenne 128 suffiront.
- Si la clef a 56 bits, il y a alors $2^{56} \approx 7,2 \times 10^{16}$ clefs possibles.
- En faisant l'hypothèse qu'un super-ordinateur peut essayer un million de clefs par seconde, il faudra 2000 ans pour trouver la bonne clef.

Longueur des clefs

Complexité d'une attaque exhaustive -suite-

- Si la clef a 64 bits, il faudra alors 600000 ans à ce même super-ordinateur pour trouver la bonne clef parmi les $2^{64} \approx 1,8 \times 10^{19}$ clefs possibles.

Longueur des clefs

Complexité d'une attaque exhaustive -suite-

- Si la clef a 64 bits, il faudra alors 600000 ans à ce même super-ordinateur pour trouver la bonne clef parmi les $2^{64} \approx 1,8 \times 10^{19}$ clefs possibles.
- Si la clef a 128 bits, il faudra 10^{25} années. L'âge de l'univers est évalué à environ 10^{10} ans

Longueur des clefs

Complexité d'une attaque exhaustive -suite-

- Si la clef a 64 bits, il faudra alors 600000 ans à ce même super-ordinateur pour trouver la bonne clef parmi les $2^{64} \approx 1,8 \times 10^{19}$ clefs possibles.
- Si la clef a 128 bits, il faudra 10^{25} années. L'âge de l'univers est évalué à environ 10^{10} ans
- Avec une clef de 2048 bits, un million de super-ordinateurs hypothétiques travaillant en parallèle passeraient 10^{597} années pour trouver la clef.

Longueur des clefs

Complexité d'une attaque exhaustive -suite-

- Si la clef a 64 bits, il faudra alors 600000 ans à ce même super-ordinateur pour trouver la bonne clef parmi les $2^{64} \approx 1,8 \times 10^{19}$ clefs possibles.
- Si la clef a 128 bits, il faudra 10^{25} années. L'âge de l'univers est évalué à environ 10^{10} ans
- Avec une clef de 2048 bits, un million de super-ordinateurs hypothétiques travaillant en parallèle passeraient 10^{597} années pour trouver la clef.
- Deux paramètres déterminent la vitesse d'une attaque exhaustive : le nombre de clefs à tester et la vitesse de chaque test.

Problème de factorisation

Chiffrement public

- Il est facile de multiplier les nombres pour obtenir un produit, mais difficile de factoriser ce produit et de retrouver les deux grands nombres premiers.

Problème de factorisation

Chiffrement public

- Il est facile de multiplier les nombres pour obtenir un produit, mais difficile de factoriser ce produit et de retrouver les deux grands nombres premiers.
- Aujourd'hui, les algorithmes dominants de chiffrement à clef publique sont basés sur la difficulté de factoriser des grands nombres qui sont le produit de deux grands nombres premiers.

Problème de factorisation

Chiffrement public

- Il est facile de multiplier les nombres pour obtenir un produit, mais difficile de factoriser ce produit et de retrouver les deux grands nombres premiers.
- Aujourd'hui, les algorithmes dominants de chiffrement à clef publique sont basés sur la difficulté de factoriser des grands nombres qui sont le produit de deux grands nombres premiers.
- Ces algorithmes sont aussi sensibles aux attaques exhaustives, mais d'un type différent.

Problème de factorisation

Chiffrement public

- Il est facile de multiplier les nombres pour obtenir un produit, mais difficile de factoriser ce produit et de retrouver les deux grands nombres premiers.
- Aujourd'hui, les algorithmes dominants de chiffrement à clef publique sont basés sur la difficulté de factoriser des grands nombres qui sont le produit de deux grands nombres premiers.
- Ces algorithmes sont aussi sensibles aux attaques exhaustives, mais d'un type différent.
- Casser ces algorithmes ne veut pas nécessairement dire essayer toutes les clefs possibles

Problème de factorisation

Longueur du nombre

- Casser ces algorithmes veut dire essayer de factoriser un grand nombre.

Problème de factorisation

Longueur du nombre

- Casser ces algorithmes veut dire essayer de factoriser un grand nombre.
- Si le nombre est trop petit, vous n'avez aucune sécurité.

Problème de factorisation

Longueur du nombre

- Casser ces algorithmes veut dire essayer de factoriser un grand nombre.
- Si le nombre est trop petit, vous n'avez aucune sécurité.
- Si le nombre est assez grand, vous êtes protégé contre toute la puissance de calcul mondiale du moment.

Problème de factorisation

Longueur du nombre

- Casser ces algorithmes veut dire essayer de factoriser un grand nombre.
- Si le nombre est trop petit, vous n'avez aucune sécurité.
- Si le nombre est assez grand, vous êtes protégé contre toute la puissance de calcul mondiale du moment.
- Factoriser des grands nombres est dur.

Problème de factorisation

Longueur du nombre

- Casser ces algorithmes veut dire essayer de factoriser un grand nombre.
- Si le nombre est trop petit, vous n'avez aucune sécurité.
- Si le nombre est assez grand, vous êtes protégé contre toute la puissance de calcul mondiale du moment.
- Factoriser des grands nombres est dur.
- Les algorithmes de factorisation de nombres de grande taille sont souvent exécutés sur des super ordinateurs pour des périodes de temps considérables.

Déchiffrement affine

Exemple et exercice

- Soit le texte chiffré suivant:

  ntjmpumgxpqtstgqpgtxpnchumtputgfsftgthnngxnchumwx
  ootrtumhpyctgktjqtjchfooxujqhgztumxpotjxotfoqtohr
  xumhzutwftgtopfmntjmpuatmfmshodpfrxpjjtqtghbxuj

Déchiffrement affine

Exemple et exercice

- Soit le texte chiffré suivant:

  ntjmpumgxpqtstgqpgtxpnchumtputgfsftgthnngxnchumwx
  ootrtumhpyctgktjqtjchfooxujqhgztumxpotjxotfoqtohr
  xumhzutwftgtopfmntjmpuatmfmshodpfrxpjjtqtghbxuj

- Utiliser la table de fréquences des lettres pour déchiffrer ce texte

Déchiffrement affine

Exemple et exercice

- Soit le texte chiffré suivant:

  ntjmpumgxpqtstgqpgtxpnchumtputgfsftgthnngxnchumwx
  ootrtumhpyctgktjqtjchfooxujqhgztumxpotjxotfoqtohr
  xumhzutwftgtopfmntjmpuatmfmshodpfrxpjjtqtghbxuj

- Utiliser la table de fréquences des lettres pour déchiffrer ce texte

- Expliquer de manière exhaustive tout le processus de déchiffrement et illustrer le dans Sagemath.

Déchiffrement et Mise en situation non triviale

Exemple et exercice

- Soit le texte chiffré suivant:

YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ
NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ
NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ
XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR

Déchiffrement et Mise en situation non triviale

Exemple et exercice

- Soit le texte chiffré suivant:

```
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ
NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ
NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ
XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR
```

- Utiliser l'analyse statistique sur des lettres et polygrammes pour déchiffrer ce texte

Déchiffrement et Mise en situation non triviale

Exemple et exercice

- Soit le texte chiffré suivant:

YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ
NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ
NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ
XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR

- Utiliser l'analyse statistique sur des lettres et polygrammes pour déchiffrer ce texte
- Expliquer de manière exhaustive tout le processus de déchiffrement et illustrer le dans Sagemath.

Test de Kasiski et Indice de coïncidence

Exemple et exercice

- Soit le texte chiffré suivant:

```
CHREEVOAHMAERATBIAXXWTNXBEEOPHBSBQMQEQERBW
RVXUOAKXAOSXXWEAHBWGJMMQMNKGRFVGXWTRZXWIAK
LXFPSKAUTEMNDCMGTSXMXBTUIADNGMGPSRELXNJELX
VRVPRTULHDNQWTWDTYGBPHXTFALJHASVBFXNGLLCHR
ZBWELEKMSJIKNBHWRJGNMGJSGLXFEYPHAGNRBIEQJT
AMRVLCRREMNDGLXRRIMGNSNRWCHRQHAEYEVTAQEBBI
PEEWEVKAKOEWADREMXMTBHHCHRTKDNVRZCHRCLQOHP
WQAIIWXNRMGWOIIFKEE
```

Test de Kasiski et Indice de coïncidence

Exemple et exercice

- Soit le texte chiffré suivant:

```
CHREEVOAHMAERATBIAXXWTNXBEEOPHBSBQMQEQERBW
RVXUOAKXAOSXXWEAHBWGJMMQMNKGRFVGXWTRZXWIAK
LXFPSKAUTEMNDCMGTSXMXBTUIADNGMGPSRELXNJELX
VRVPRTULHDNQWTWDTYGBPHXTFALJHASVBFXNGLLCHR
ZBWELEKMSJIKNBHWRJGNMGJSGLXFEYPHAGNRBIEQJT
AMRVLCRREMNDGLXRRIMGNSNRWCHRQHAEYEVTAQEBBI
PEEWEVKAKOEWADREMXMTBHHCHRTKDNVRZCHRCLQOHP
WQAIIWXNRMGWOIIFKEE
```

- Utiliser le test de Kasiski puis l'indice de coïncidence pour déchiffrer ce texte

Test de Kasiski et Indice de coïncidence

Exemple et exercice

- Soit le texte chiffré suivant:

```
CHREEVOAHMAERATBIAXXWTNXBEEOPHBSBQMQEQERBW
RVXUOAKXAOSXXWEAHBWGJMMQMNKGRFVGXWTRZXWIAK
LXFPSKAUTEMNDCMGTSXMXBTUIADNGMGPSRELXNJELX
VRVPRTULHDNQWTWDTYGBPHXTFALJHASVBFXNGLLCHR
ZBWELEKMSJIKNBHWRJGNMGJSGLXFEYPHAGNRBIEQJT
AMRVLCRREMNDGLXRRIMGNSNRWCHRQHAEYEVTAQEBBI
PEEWEVKAKOEWADREMXMTBHHCHRTKDNVRZCHRCLQOHP
WQAIIWXNRMGWOIIFKEE
```

- Utiliser le test de Kasiski puis l'indice de coïncidence pour déchiffrer ce texte
- Expliquer de manière exhaustive tout le processus de déchiffrement et illustrer le dans Sagemath.

Chiffrement de Hill

Attaque à texte clair connu

- Déchiffrer le texte suivant qui a été obtenu en appliquant le chiffrement de Hill sur des blocs de taille 2 sur un mot de la langue française :

  gzatzxjihvbreosu

  sachant que le chiffrement du mot *chiffrer* avec la même clé donne le chiffré *jvfrtqnb*.

Chiffrement de Hill

Attaque à texte clair connu

- Déchiffrer le texte suivant qui a été obtenu en appliquant le chiffrement de Hill sur des blocs de taille 2 sur un mot de la langue française :

  gzatzxjihvbreosu

  sachant que le chiffrement du mot *chiffrer* avec la même clé donne le chiffré *jvfrtqnb*.

- Expliquer de manière exhaustive tout le processus de déchiffrement et illustrer le dans Sagemath.

Chiffrement de Hill

Attaque à texte chiffré connu

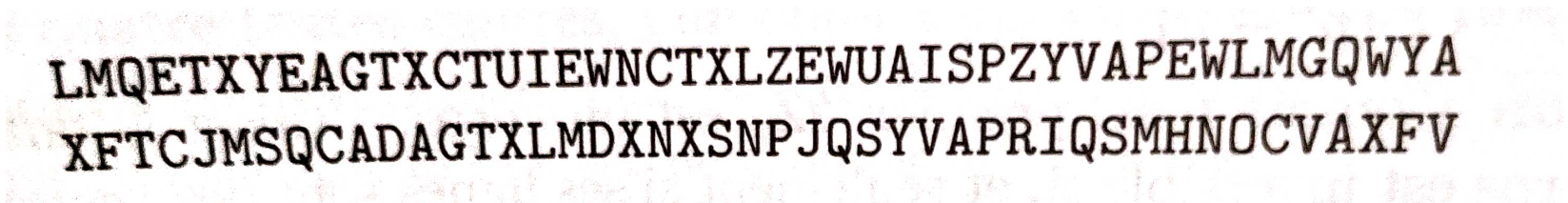
- Supposons que la taille $m = 2$. Casser le texte chiffré en blocs de deux caractères (digrammes). Chaque bloc provient du chiffrement d'un digramme du texte clair par une matrice de chiffrement inconnue. Prendre le digramme le plus fréquent et supposer à un digramme fréquent de la table des fréquences des digrammes. Pour chaque possibilité, procéder comme dans l'attaque à texte clair connu jusqu'à ce que la matrice de chiffrement soit obtenue.

Chiffrement de Hill

Attaque à texte chiffré connu

- Supposons que la taille $m = 2$. Casser le texte chiffré en blocs de deux caractères (digrammes). Chaque bloc provient du chiffrement d'un digramme du texte clair par une matrice de chiffrement inconnue. Prendre le digramme le plus fréquent et supposer à un digramme fréquent de la table des fréquences des digrammes. Pour chaque possibilité, procéder comme dans l'attaque à texte clair connu jusqu'à ce que la matrice de chiffrement soit obtenue.

- Déchiffrement et illustration dans Sagemath du texte:



Fin du chapitre

Merci de votre Attention