

Cryptographie

Introduction & Histoire de la cryptographie

Alexander Schaub¹

schaub.alexander@free.fr

17/11/2025

¹DGA-MI, Bruz

Cryptographie

Écriture cachée

ATTAQUEZ A L'AUBE

ATTAQUEZ A L'AUBE



ATTAQUEZ A L'AUBE



HDJQKLFO K M ALFY

Chiffres historiques

Chiffre de substitution



Chiffre de transposition



Chiffres historiques

Chiffre de substitution

A → N

B → O

C → P

D → Q

...

Z → M

Chiffre de transposition

Chiffres historiques

Chiffre de substitution

Chiffre de transposition

ATTAQUEZAL AUBE



A | T | T | A | Q → T | T | Q | A | A
U | E | Z | A | L E | Z | L | U | A
A | U | B | E | U | B | A | E | E



TEUTZBQLAUAAAE

Le texte c'est bien, mais à l'oral ?



Et si je veux cacher l'existence du message ?



ATTAQUEZ A L'AUBE

Stégano·graphie

Écriture hermétique (?)

Un peu de vocabulaire

Texte clair Message à transmettre

Texte chiffré Transformation “incompréhensible” du message

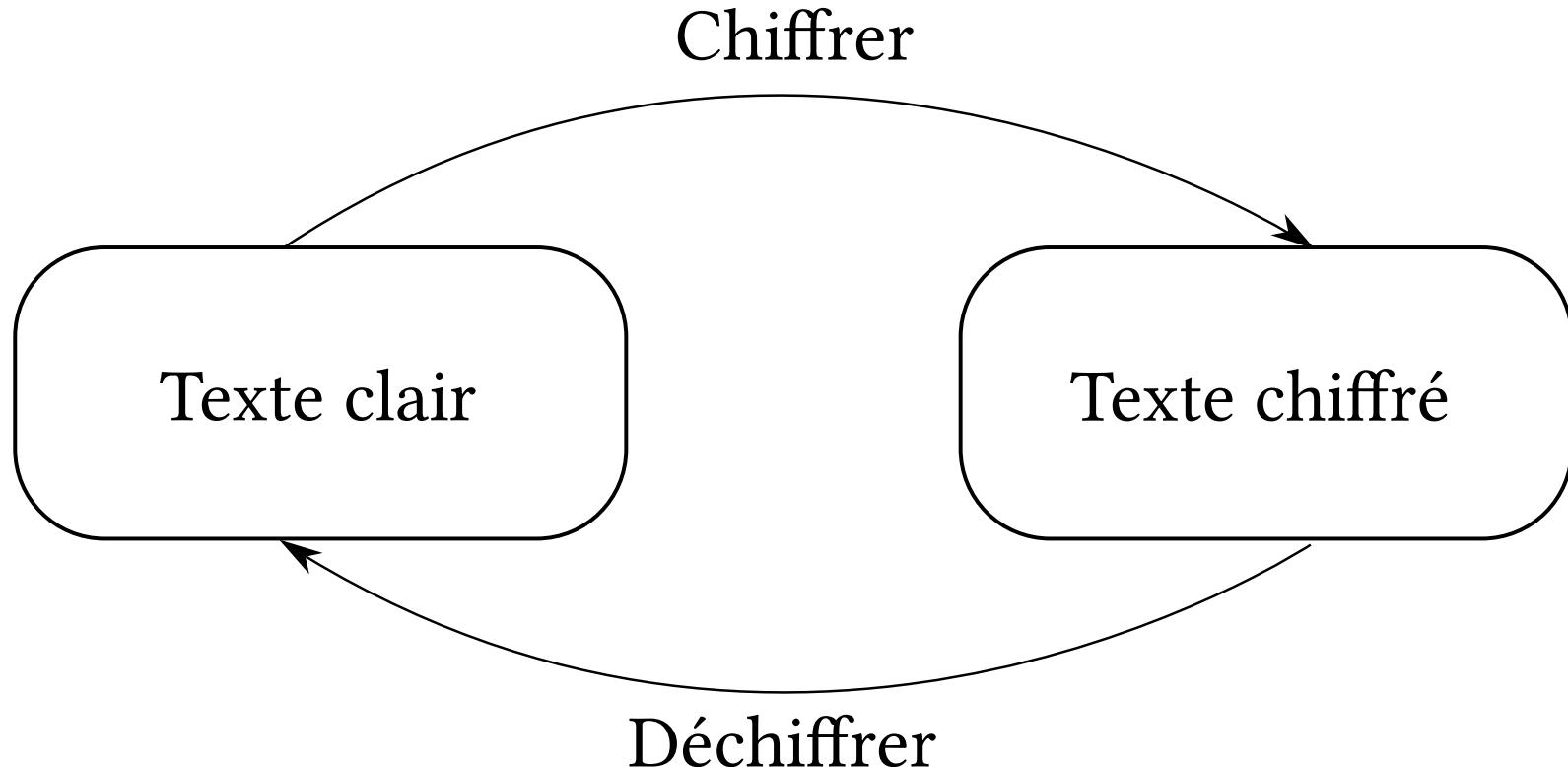
Chiffrer Transformer le texte clair en texte chiffré

Déchiffrer Transformer le texte chiffré en texte clair

Remarque:

- ~~crypter~~

En images



Un peu de notation (provisoire)

Alphabet Ensemble de symboles, ici : $\Sigma = \{A, B, \dots, Z\}$

Message (ou texte, ou mot) Suite de symboles, i.e. élément de Σ^+

(Note: $\Sigma^+ = \Sigma \cup \Sigma^2 \cup \Sigma^3 \cup \dots = \bigcup_{n=1}^{\infty} \Sigma^n$)

Fonction de chiffrement $f : \Sigma^+ \mapsto \Sigma^+$

Fonction de déchiffrement $g : \Sigma^+ \mapsto \Sigma^+$ telle que

$$\forall x \in \Sigma^+, g(f(x)) = x$$

Est-ce suffisant ?

Est-ce suffisant ?

Pourquoi ?

Principe de Kirchhoff

La sécurité d'un système de chiffrement ne doit reposer que sur le secret de la clef.

Il faut distinguer entre:

L'algorithme général

Ex: décaler chaque lettre dans
l'alphabet

Ex: Écrire le texte dans un rectangle
et lire de haut en bas

et la composante secrète

Ex: de combien de lettres décaler

Ex: la largeur du rectangle

Notation revisitée

Un système de chiffrement se compose de:

- Trois ensembles E, F, K
- De deux fonctions, $f : E \times K \mapsto F, g : F \times K \mapsto E$ telles que
 - $\forall x \in E, k \in K, g(f(x, k), k) = x$
 - On ne doit pas pouvoir retrouver x à partir de $f(x, k)$ sans connaître k

Exemple

Chiffre de substitution simple (dit *de Caesar*):

- $E = F = \Sigma^+$
- $K = [1; 25]$
- $f(x = (x_i)_i, k) = F(x_i, k)_i$ où $F(x_i, k) = x_i + k$

Exemple

Chiffre de transposition simple:

- $E = F = \Sigma^+$
- $K = (n, \mathfrak{S}(n))_{n \in \mathbb{N}}$
- $f(x = (x_i)_i, (k, \sigma)) = \left(x_{\sigma(\lfloor \frac{i}{n/k} \rfloor) + k*(i \% \frac{n}{k})} \right)_i$ où n est la longueur du message, en supposant que n est un multiple de k

Un peu de pratique

Partie I du TP n°1

O tempora o moris

Le chiffrement de Caesar n'est pas vraiment sûr !

O tempora o moris

Le chiffrement de Caesar n'est pas vraiment sûr !

Il n'y a que 25 transformations (= 25 clés différentes)

O tempora o moris

Le chiffrement de Caesar n'est pas vraiment sûr !

Il n'y a que 25 transformations (= 25 clés différentes)

C'est facile de toutes les essayer

Améliorations possibles

- Considérer *toutes* les permutations possibles:
 - ▶ $26! \approx 4 \times 10^{26} > 25$
 - ▶ Un attaquant ne peut pas toutes les essayer
- Changer régulièrement de système
 - ▶ Par exemple, alterner entre $A \rightarrow C$ et $A \rightarrow F$
 - ▶ Deux systèmes ne suffisent pas, mais si on en utilise plus...
 - ▶ On obtient le chiffre de *Vigenère*

Chiffre de substitution généralisé

- $E = F = \Sigma^+$
- $K = \mathfrak{S}(\Sigma)$ l'ensemble des bijections dans Σ
- $f\left(x = (x_i)_i, \sigma\right) = (\sigma(x_i))_i$
- $g\left(x = (x_i)_i, \sigma\right) = (\sigma^{-1}(x_i))_i$

Chiffre de Vigenère

- $E = F = \Sigma^+$
- $K = [0; 25]^m$
- $f\left(x = (x_i)_i, k = (k_j)_j\right) = F(x_i, k_{i \% m})_i$ où $F(x_i, k) = x_i + k$

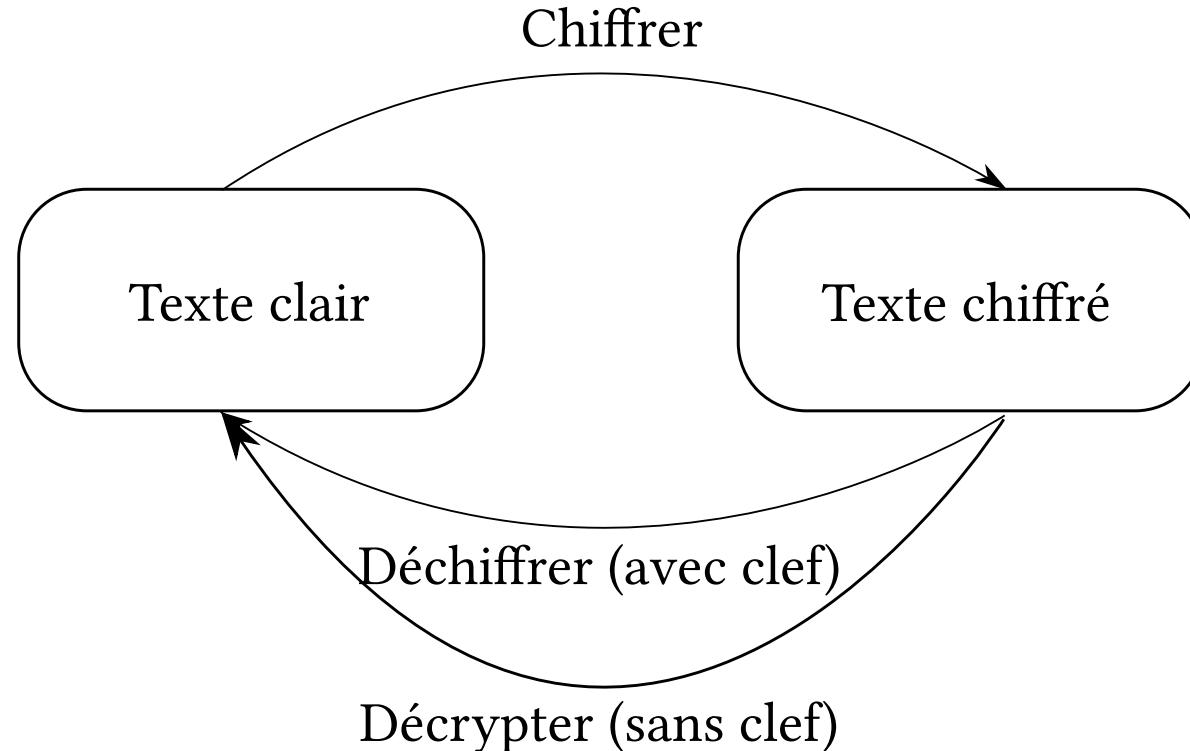
Exemple: clef = MOT

AAABBBCCCCDDDD...



MOTNPUOQVPRW...

Un peu de cryptanalyse



Une histoire de fréquences

Toutes les lettres n'apparaissent pas à fréquence égale en français :

- “e” est la letter la plus courante, puis “a”, “i”, “s”, ...

Les bigrammes ont des fréquences différentes aussi !

- l'enchaînement “nt” est beaucoup plus courant que “tn”

Une permutation unique appliquée à tout un texte **préserve les fréquences** (y compris des bigrammes)

Retrouver la permutation

Si on sait qu'un texte *français* (suffisamment long!) a été chiffré en utilisant une *permutation* unique :

- La lettre la plus présente correspond *probablement* au “e”
- la deuxième la plus fréquente au “a”, etc.
- on peut s'aider des fréquences de bigrammes également

Contre-ex : *La Disparition* de Georges Perec

Décrypter Vigenère

- Si on connaît la *longueur* de la clé utilisée dans un chiffre de Vigenère, alors il “suffit” de décrypter m chiffres de Caesar
- On peut retrouver cette longueur grâce aux fréquences des lettres de la langue du texte clair... (mais d'autres méthodes existent aussi !)

Au boulot ! A l'attaque de Vigenère...

Partie II du TP n°1

Chiffres pré-modernes

- Vigenère publié au XVI siècle, cassé fin du XIX siècle.
- Mais plusieurs améliorations sont possibles !

Chiffrements polygraphiques

- Dans les cryptosystèmes de César et de Vigenère, **une** lettre est transformée en **une** autre lettre...

Chiffrements polygraphiques

- Dans les cryptosystèmes de César et de Vigenère, **une** lettre est transformée en **une** autre lettre...
- ... et ce indépendamment lettre par lettre

Chiffrements polygraphiques

- Dans les cryptosystèmes de César et de Vigenère, **une** lettre est transformée en **une** autre lettre...
- ... et ce indépendamment lettre par lettre
- Et si on considérait des **groupes** de lettres plutôt ?

Chiffrement digraphique

- $E = F = \Sigma^+$
- $K = \mathfrak{S}(\Sigma^2)$ l'ensemble des bijections dans Σ^2
- $f\left(x = (x_i)_i, \sigma\right) = (\sigma(x_{2i}, x_{2i+1}))_i$
- $g\left(x = (x_i)_i, \sigma\right) = (\sigma^{-1}(x_{2i}, x_{2i+1}))_i$

Chiffre de Hill

- Une substitution générique est coûteuse à représenter
- Chiffre de Hill : César mais en digraphique
- César : $y = x + a$ où y chiffré, x clair, a décalage
- Généralisation (Hill) :

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} ax_1 + bx_2[26] \\ cx_1 + dx_2[26] \end{pmatrix}$$

- Pour déchiffrer : il faut inverser la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ (dans $\mathbb{Z}/26\mathbb{Z}$)

Cryptanalyse du chiffre de Hill

- Les fréquences de digrammes différent !
- Le chiffre de Hill est donc vulnérable à l'analyse statistique

Chiffre de Hill généralisé

- Le chiffre de Hill se généralise assez bien :
 - ▶ à des dimensions supérieures
 - ▶ à des corps plus grands ($\mathbb{F}_{2^8}^n$ i.e. des chaînes d'octets)
- Le chiffrement et déchiffrement sont très rapides
- En dimension assez grande, l'analyse statistique n'est plus efficace

Chiffre de Hill généralisé

- Le chiffre de Hill se généralise assez bien :
 - ▶ à des dimensions supérieures
 - ▶ à des corps plus grands ($\mathbb{F}_{2^8}^n$ i.e. des chaînes d'octets)
- Le chiffrement et déchiffrement sont très rapides
- En dimension assez grande, l'analyse statistique n'est plus efficace
- Cependant, il n'est plus utilisé aujourd'hui. Pourquoi d'après vous ?

Les chiffres de la Première Guerre Mondiale

- Avec l'avènement des méthodes de communication longue distance (télégrammes), protéger ses communications devient indispensable
- Les belligérants sont capables d'intercepter les communications des autres pays
- Si la sécurité n'est pas bonne: aïe aïe aïe...

Le chiffre Ubchi

- Chiffre utilisé par **toute** l'armée allemande en 1914 lorsqu'éclate la Première Guerre Mondiale
- La même clé est utilisée pour **tous** les échanges...
- L'algorithme est une double transposition :

M	A	C	L	E		M	A	C	L	E		M	A	C	L	E		EQAUL
5	1	2	4	3		5	1	2	4	3		5	1	2	4	3		UZAXT
A	T	T	A	Q	→	T	E	U	T	Z	→	E	Q	A	U	L	→	AATBE
U	E	Z	A	L		B	Q	L	A	A		U	Z	A	X	T		
A	U	B	E			E	A	U	A	X		A	A	T	B	E		

Comment les français ont-il cassé Ubchi ?

Un opérateur a oublié la deuxième transposition...



Ubchi a été décrypté !

- Tout le monde utilisait la même clef → oups !
- Maintenant, les français peuvent déchiffrer les conversations
- Comment les Français vont-il utiliser cette information ?

La réaction française

Comment on a manqué le kaiser de bien peu

LONDRES, 5 novembre. — *Du correspondant particulier du « Matin ».* — On télégraphie au *Times* du nord de la France, en date d'aujourd'hui :

« Voici de nouveaux détails sur la façon dont le kaiser a failli être tué par des bombes jetées par un aviateur de l'armée alliée occupant le front Nieuport-Ypres :

» Pendant cinq jours, l'empereur d'Allemagne a assisté aux opérations sur ce front et c'est en raison de sa présence que l'ennemi a fait des attaques aussi persistantes, aussi vigoureuses, sans souci des énormes sacrifices humains qui en résultaitent.

» Dimanche dernier, le kaiser, avec quelques-uns de ses aides de camp, est arrivé en automobile vers cinq heures de l'après-midi devant une auberge de Thielt. Des appartements lui avaient été réservés et son repas était préparé.

» Après le repas, au lieu d'aller dans sa chambre, il quitta précipitamment l'auberge avec deux de ses aides de camp et se rendit en automobile à l'autre bout de la ville où il retint un nouvel appartement. Vingt minutes après que le kaiser eut quitté la taverne où il avait dîné, six bombes tombèrent sur l'immeuble, et la chambre où se trouvait ses bagages fut complètement détruite.

» Deux de ses aides de camp restés en arrière furent tués et une automobile innommable qui était dans la cour fut brisée. »



Le chiffre ABC

- La mèche est vendue, les allemands sont au courant du décryptage !
- Et du coup, la clef est changée 😓
- Mais les Français finissent par trouver un mode direct de décryptage !
😊
- Et du coup les allemands sont obligés de changer de cryptosystème : ils utilisent le chiffre dit “ABC”

Le chiffre ABC (suite)

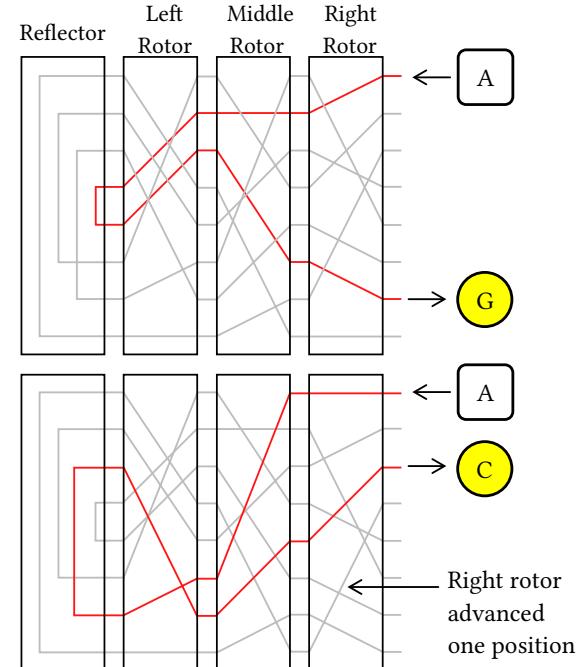
- Bonne nouvelle pour les Français : ce chiffre est encore moins sûr !
- Il s'agit simplement d'un chiffre Vigenère **avec une clé immuable égale à ABC**,
- suivie d'une **simple** transposition (la moitié d'Ubchi)
 - ▶ pour leur défense, la clé de la transposition changeait régulièrement
- cet algorithme ne résiste pas longtemps aux spécialistes français...

Et ensuite ?

- Les Allemands changèrent de code plusieurs fois :
 - ▶ KRU
 - ▶ ADFGVX (substitution génériques en encodant sur deux lettres puis transposition)
- Tous deux furent décryptés !
- Un message ADFGVX décrypté fut crucial dans la victoire française : il s'agit du “Radiogramme de la victoire”, permettant d'anticiper une attaque allemande à Compiègne !

Puis vint la Deuxième Guerre
Mondiale !

Enigma



Colossus et son créateur

