Cryptologie : Cryptages classiques

Matthieu Amiguet

2006 – 2007

haute école arc ingénierie
neuchâtel berne jura — saint-imier le locle porrentruy

Pourquoi étudier les cryptages classiques ?

- Par *cryptages classiques*, nous entendrons les cryptages utilisés depuis l'antiquité jusqu'à l'apparition de l'informatique (plus ou moins...)
- Ces cryptages sont donc dépassés et ne sont plus utilisables dans des contextes cryptologiques sérieux
- Alors... pourquoi les étudier ?
  - Intérêt historique
  - Connaître les grands principes
  - Connaître les erreurs commises pour pouvoir les éviter

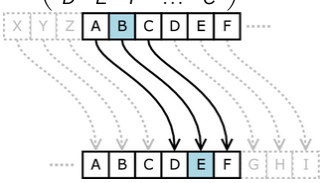
Principe

- L'idée est de remplacer chaque lettre du message par une autre, selon une règle fixe
- $\mathcal{K}$ = ensemble des permutations de $\mathcal{A}$
- $E_k(m_1 m_2 \dots m_t) = e(m_1)e(m_2)\dots e(m_t)$
- $k' = k^{-1}$
- $|\mathcal{K}| = |\mathcal{A}|!$
  - NB : $26! \approx 2^{88}$

Exemple : Les translations – 1

Aussi appelées "cryptages de Jules César"

- Jules César (~101-44 av. J.-C) utilisait un simple décalage de trois lettres
  - $\mathcal{A} = \{A, B, C, \dots, Z\}$
  - $k = \begin{pmatrix} A & B & C & \dots & Z \\ D & E & F & \dots & C \end{pmatrix}$

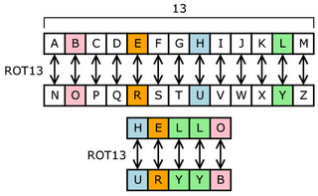


  - $E_K(CESAR) = FHVDU$
  - Exercice : décrypter "SDV WUHV VROLGH"

Exemple : Les translations – 2

Aussi appelées “cryptages de Jules César”

- Pour éviter d’exposer des contenus potentiellement choquants aux yeux de tous, les *newsgroups* des années 80 utilisaient le ROT13
  - Même principe que Jules César, mais avec un décalage de 13



  - Exercice : pourquoi 13 ?

Principe

- L’idée est de remplacer chaque *groupe* de lettres par un autre groupe, selon une règle fixe
- $\mathcal{K} =$ ensemble des permutations de $\mathcal{A}^n$
- $E_k(m_1 m_2 \dots m_t) = (e(m_1 \dots m_n) e(m_{n+1} \dots m_{2n}) \dots)$
- $k' = k^{-1}$
- $|\mathcal{K}| = |\mathcal{A}|^n !$
  - NB : $26^2 ! \approx 2^{5385}$

Exemple : Le Playfair

La clé

- On réduit l’alphabet à 25 lettres (remplacer w par v, ou j par i, . . .)
- La clé est alors constituée par le choix d’une disposition des 25 lettres dans un carré 5x5

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

- On peut aussi représenter la clé en ligne : BYDGZJSFUPLARKXCOIVEQNMHT
- On utilise ce carré pour remplacer un couple de lettre par un autre.

Exemple : Le Playfair

Les règles

- Les règles de substitution sont les suivantes
  - Si les deux lettres sont sur les coins d’un rectangle, alors les lettres chiffrées sont sur les deux autres coins (en gardant l’ordre des lignes)
  - Si deux lettres sont sur la même ligne, on les “décale d’un cran” vers la droite
  - Si deux lettres sont sur la même colonne, on les “décale d’un cran” vers le bas
  - Si le couple est composé de deux fois la même lettre, on insère un X entre deux.

Exemple : Le Playfair
Exercices

- À l'aide de la clé

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

- Crypter "PLAYFAIR"
  - JXOSSRMI
- Décrypter "SXKREM ZISL JXPF ANRCZI"

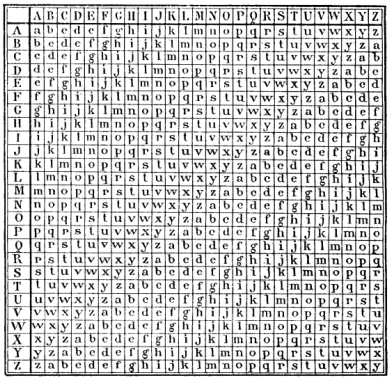
Principe

- Substitution dont la règle change au cours du temps.
- Quelques exemples célèbres
  - cryptage de Vigenère
  - cylindre de Jefferson
  - Enigma.

Exemple : Le cryptage de Vigenère

- Inventé par Blaise de Vigenère (1523-1596)
- Comparable à un cryptage de César, mais avec un décalage qui change pour chaque lettre
- Pour ce faire : on choisit un mot-clé que l'on répète autant de fois que nécessaire pour obtenir la longueur du message à coder
  - On peut aussi utiliser comme mot-clé un livre, ce qui évite la répétition du mot-clé
- Ensuite, on effectue une "addition modulo 26", avec A=0, B=1, . . .
  - ou bien on utilise la *table de Vigenère*.

La table de Vigenère



Vigenère – exemple

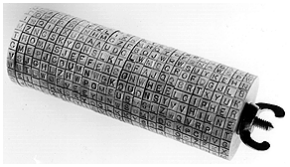
- En prenant pour message “VIGENERE” et pour mot-clé “CRYPTAGE”, on obtient

V	I	G	E	N	E	R	E
C	R	Y	P	T	A	G	E
X	Z	E	T	G	E	X	I

- Exercice : avec le même mot-clé, décrypter ULZHMIZYVZMC

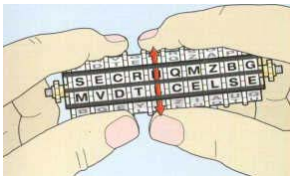
Exemple : Le cylindre de Jefferson – 1

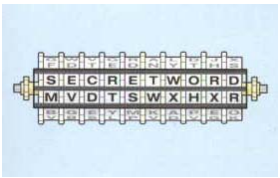
- Inventé par Thomas Jefferson (1743-1826) vers 1800
- Le cylindre consiste en 26 roues pouvant tourner autour d’un axe



- Chaque roue comporte les 26 lettres de l’alphabet en ordre aléatoire
- La “clé” correspond à l’ordre des roues
- Pour crypter un message, on le “compose” sur une ligne et on lit la ligne suivante.

Exemple : Le cylindre de Jefferson – 2



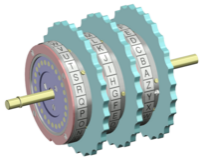


Exemple : Enigma – 1

- Célèbre machine utilisée par l’Allemagne nazie pendant la seconde guerre mondiale

Exemple : Enigma – 2

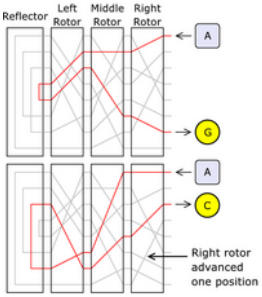
- Enigma fait partie de la famille des machines à tambours (ou rotors)
- Entre le clavier et les lampes, le signal passe par trois tambours successifs dont l'effet est simplement de réaliser une substitution



- La subtilité : à chaque pression de touche, les rotors tournent (comme un odomètre).

Exemple : Enigma – 3

- Ainsi, par exemple, deux pressions sur la touche *A* peuvent allumer successivement la lampe *G* et *C* :



Exemple : Enigma – 4

- La "clé" est donnée par l'ordre et la position initiale des tambours
- Il y a eu différentes versions avec un nombre variable de tambours
  - sur la machine
  - de réserve
- Dans la version à trois tambours installés, la période de la substitution est de $26^3 = 17576$ caractères.

Principe

- L'idée est de *réordonner* les lettres constituant le message
- $\mathcal{K} =$ ensemble des permutations de $\{0, 1, \ldots, n\}$
- $E_k(m_1 m_2 \ldots m_t) = (m_{e(1)} m_{e(2)} \ldots m_{e(t \bmod n)})$
- $k' = k^{-1}$
- $|\mathcal{K}| = n!$

Exemple : la scytale spartiate

- Procédé utilisé au Ve siècle av. J.-C. par les soldats spartiates

- Le diamètre du bâton fait office de clé
- Le procédé était combiné avec une forme de stéganographie : le soldat portait la bande en ceinture !
- Exemple : pour un “diamètre” de 3 lettres :
  - SCYTALE SPARTIATE → STEPTTCA AIEYLSRA .

Pour en savoir plus. . .

- `http://www.apprendre-en-ligne.net/crypto/`
- Wikipedia : `http://wikipedia.org/`

Principe

- Succession de plusieurs cryptages complémentaires
- Substitution : ajoute de la “confusion”
- Transposition : ajoute de la “diffusion”
- Une alternance des deux peut donner des cryptages relativement forts.