Cours : Cryptographie et Sécurité Informatique

Cryptographie classique I
Chiffres par transpositions

I. Akharraz
Université Sidi Mohamed Ben Abdellah

ismail.akharraz@usmba.ac.ma

Sommaire.

- Chiffres à répertoire.
- Chiffres par transposition.

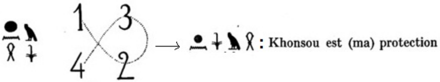
1. Introduction.

- La cryptographie classique nous permet de comprendre les principes de chiffrement modernes.

- Il y avait deux familles de codes classiques :
  (1) Les codes à répertoire
  (2) Les codes à clefs secrètes :
    - Les codes de transposition ou de permutation qui sont des codes par blocs.
    - les codes de substitution qui peuvent être des codes par blocs ou par flots.

- Exemples historiques :
  - Sparte entre 4000 et 5000 av.JC : scytales (bâton et un ruban pour colporter le message).

  - Egypte à partir de 2350 Av.JC : plusieurs méthodes.



  - Rome, vers 50 Av.JC, code Jules César : décalage des caratères.

2. Codes à répertoire.

- Utilisés jusqu'au début du 20ème siècle.
- Consiste à réaliser un dictionaire binaire qui fait correspondre à chaque mot de la langue utilisée un autre mot ou symbole.
- Le dictionaire (= code) doit rester secret.
- Nécessite l'envoi de documents volumineux.

Langue utilisée	Code
guerre	oiseaux
la	30
commence	sur
à	17
minuit	arbres

Langue utilisée	Code
tombe	du
sidi abed	mois
dans	premier
la	jours
trésor	le

30 oiseaux sur 17 arbres $\longrightarrow$ la guerre commence à minuit.
le premier jours du mois $\longrightarrow$ trésor dans la tombe sidi abed.

3. Chiffrement par transposition (permutation)

- On chiffre le message en permutant l'ordre des lettres du message suivant des règles bien définies.
- On découpe le texte clair en blocs de taille identique : on applique une permutation à tous les blocs.
- permutation = transposition = bijection :

  bloc_initial ⟶ bloc_chiffré.
- Le texte doit être complété (si nécessaire) pour permettre ce découpage.
- La clef de chiffrement est la permutation elle-même.

3. Chiffrement par transposition (permutation)

- Nombre de permutations possibles sur un bloc de taille n est : n!.

- $S_n = \{$ permutation (bijection) : $\{1, 2, ..., n\} \longrightarrow \{1, 2, ..., n\}\}$

$$|S_n| = n!$$

- Avec des blocs de grande taille il est trés difficile de retrouver le texte original sans connaître la permutation, et sans aucune connaissance sur le texte clair.

- Blocs de 20 caractères : 20! = 2 432 902 008 176 640 000 combinaisons.

3.1 Transposition rectangulaire.

- Méthode de codage utilisée par les Allemands en 1914.
- On écrit le message dans une grille rectangulaire et on arrange les colonnes de cette grille selon un ordre défini par un mot secret(clé).

- On veut envoyer le message suivant : la guerre commence à minuit.
- L'expéditeur (A) et le destinataire (B) du message se mettent d'accord sur une grille de largeur fixée à l'avance.

- Grille de largeur 6 :

l	a	□	g	u	e
r	r	e	□	c	o
m	m	e	n	c	e
□	à	□	m	i	n
u	i	t	□	□	□

3. Chiffrement par transposition (permutation).

- A lit le texte par colonne et envoi à B le message:

lrm□uarmài□ee□tg□nm□ucci□eoen□

- Pour décrypter il suffit de diviser le texte en 6 blocs et de le transposer en matrice : un bloc = une colonne.

- On peut augmenter le secret de ce code en ajoutant une *clé secrète* : l'ordre de lecture des colonnes.

Exemple : A et B choisissent VOYAGE pour clé secrète. On numérote les colonnes en fonction du rang des lettres du mot VOYAGE dans l'alphabet.

3. Chiffrement par transposition (permutation)

A=0, B=1, C=2,D=3, E=4, F=5, G=6, H=7, I=8, J=9, K=10, L=11, ,M=12, N=13, O=14, P=15, Q=16, R=17, S=18, T=19, U=20,V= 21, W=22, X=23, Y=24, Z=25

V	O	Y	A	G	E
21	14	24	0	6	4
5	4	6	1	3	2
l	a	□	g	u	e
r	r	e	□	c	o
m	m	e	n	c	e
□	à	□	m	i	n
u	i	t	□	□	□

Tri colonnes $\longrightarrow$

g	e	u	a	l	□
□	o	c	r	r	e
n	e	c	m	m	e
m	n	i	à	□	□
□	□	□	i	u	t

Message chiffré : g□nm□eoen□ucci□armàilrm□u□ee□t

Message initial : la guerre commence à minuit.

3.2. Expression mathématique du chiffre par transposition.

Pour un message X de longueur n dont les lettres sont $x_1, x_2, ..., x_n$; on a :

$$C(X) = (x_{\pi(1)}, x_{\pi(2)}, ..., x_{\pi(n)})$$
$$D(Y) = (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)}, ..., y_{\pi^{-1}(n)})$$

Exemple : n =6, $|S_n|$ =6! = 720.

On prend par exemple : π : $S_n \longrightarrow S_n$ tel que $\pi(i) = i + 1$ pour i=1, ...,5 et $\pi(6) = 1$. Alors :

$C(X) = (x_2, x_3, x_4, x_5, x_6, x_1)$

On a : $\pi^{-1}(i) = i - 1$ pour i=2, ...,6 et $\pi^{-1}(1) = 6$.

Donc $D(Y) = (y_6, y_1, y_2, y_3, y_4, y_5)$

3.3. Cryptanalyse du chiffre par transposition.

- Le chiffre par transposition ne résiste pas aux attaques à texte clair connu (un couple clair-chiffré).

- Le chiffrement par transposition n'est plus pratiqué en lui seul, mais ...

- Tous les cryprosystèmes symétrique l'intégre pour assurer la confusion.