Introduction à la Cryptologie

Cryptographie symétrique

IUT Lannion

Chiffrement symétrique

Chiffrement symétrique

- Alice et Bob partage la même clé,
- Deux familles de chiffrement symétriques : blocs et flot,
- Rapide,
- Échange de clé au préalable,
- Une clé pour chaque correspondant.

Des exemples simples : Chiffrement de César I

Principe :

- Décalage de l'alphabet de k lettres où k est la clé.
- Interprétation mathématique : Les lettres sont représentées par $\mathbb{Z}/26\mathbb{Z}$. La fonction suivante est appliquée avec la clé k.

$$\begin{array}{rcl} f : \mathbb{Z}/26\mathbb{Z} & \to & \mathbb{Z}/26\mathbb{Z} \\ x & \mapsto & x + k \end{array}$$

Des attaques

- Force brute : tester les 26 clés possibles.
- Analyse de fréquence :
  - Détermination de la lettre la plus fréquente dans le message chiffré,
  - En français : e $\leftrightarrow$ 15%, a $\leftrightarrow$ 10%, s et i $\leftrightarrow$ 8%.
- On connaît un couple de message clair/message chiffré.

Des exemples simples : Chiffrement de César II

Exercices

- Décrire le cryptosystème d'après la définition.
- Soit $k = 3$ la clé de chiffrement, chiffrer le message $m = LEMESSAGEACHIFFRER$.
- Soit $c = qf\ qjyywj\ qf\ uqzx\ kwjvzjsyj\ js\ kwfshfnx\ jy\ qj\ j.\ Qj\ xfatnw\ fnij\ f\ hfxxjw\ hjxfw$. Retrouver le message clair.

Des exemples simples : Chiffrement de Vigenère I

Principe

- La clé est un mot ou une phrase.
- Chaque lettre en clair correspond à une colonne de la table de Vigenère.
- Chaque lettre de la clé correspond à une ligne.
- La lettre chiffré correspond au croisement de la ligne et de la colonne.
- La clé est répétée en boucle autant que nécessaire.

Des exemples simples : Chiffrement de Vigenère II

Chiffrement - exemple

Soit $M = message$ et $k = cle$. Pour chiffrer M:

- Regarder l'intersection de la ligne m et de la colonne $c \Rightarrow o$.
- Faire la même chose pour le reste du message.

Table de Vigenère

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

Lettre Codée

Des exemples simples : Chiffrement de Vigenère III

Déchiffrement - exemple

Soit $C = opwulkg$ et $k = cle$. Pour déchiffrer C:

- Regarder la ligne c.
- Trouver la lettre o dans cette ligne, puis voir à quelle colonne elle correspond.
- Faire la même chose pour le reste du message.

Table de Vigenère

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

Lettre Codée

Des exemples simples : Chiffrement de Vigenère IV

Des attaques

- Force brute,
- Attaque à clair connu,
- Analyse de fréquence : une lettre pas toujours chiffrée de la même façon $\Rightarrow$ non trivial.
- Trouver la taille de la clé ℓ : Test de Kasiski, Test de Friedman.
  - Découper le chiffré en mot de taille ℓ,
  - Même méthode que pour le chiffrement de César appliqué sur les lettres de même "indice".

Des exemples simples : Chiffrement de Vigenère V

Test de Kasiski

Consiste à repérer des répétitions de lettres dans le texte chiffré. Des répétitions se produisent, car :

- une suite de lettres clairs se chiffrent avec une même partie de clé;
- ou des suites différentes de lettres clairs se chiffrent de la même façon.

Analyse des écarts entre deux répétitions de séquence $\Rightarrow$ multiple de la taille de clé.

Des exemples simples : Chiffrement de Vigenère VI

Test de Friedman ou test par indice de coïncidence

- Indice de coïncidence : probabilité que 2 lettres soient identiques.
  - Indice de coïncidence français : 0,0778.
- N le nombre de lettre dans l'alphabet, n la taille du chiffré c et i l'indice de coïncidence de c.
- La taille de la clé vaut : $\frac{(I-\frac{1}{N})n}{(n-1)i-\frac{n}{N}+I}$

Exercice à faire à la maison

- Soit $k = cle$ la clé de chiffrement, chiffrer le message $m = LEMESSAGEACHIFFRER$.
- Soit $c = Wi\ aamf\ pm\ jioyb\ ji\ y\ ibkvambk\ pn\ jqt\ hh\ xmstf\ ib\ ji\ y\ iavepi\ tk\ gbqukrpiukrg\ hm\ zshxm\ lma\ ib\ re\ smv\ ji\ gsczi\ eekk\ Uhm\ aamf\ nm$. Résoudre l'énigme.

Des exemples simples : Enigma I

Historique

- Inventé par Arthur Scherbius,
- Utilisée par les Allemands pendant la Seconde Guerre mondiale,
- Cassée par Turing (voir : Imitation game).

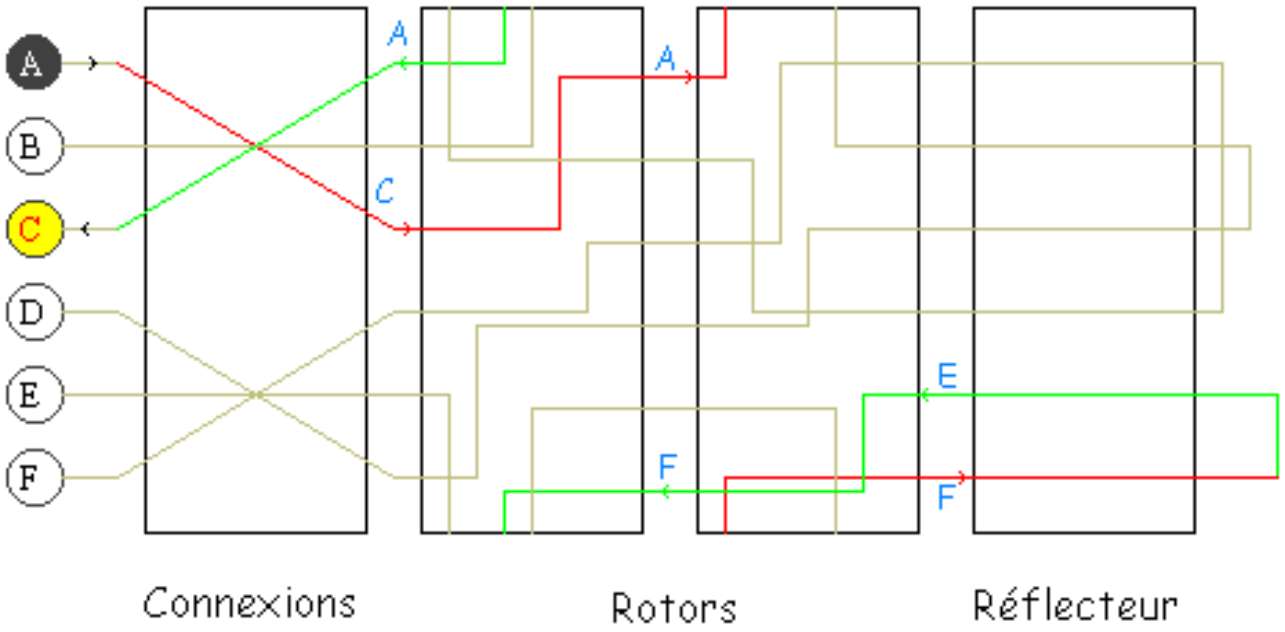
Principe

Utilisation de :

- rotors contenant des fils électriques,
- connecteur,
- clavier pour entrer le message clair,

Lorsqu'une lettre est tapée, les rotors tournent $\Rightarrow$ une même lettre n'est pas chiffrée de la même manière.

Des exemples simples : Enigma II



La clé secrète dépend du connecteur et des rotors (disposition, nombre et type) utilisés.

- Avec 3 rotors : 10^{20} clés possibles.

Des exemples simples : Enigma III

Chiffrement symétrique - par blocs

Chiffrement par blocs ou bloc ciphers

- Le message est découpé en blocs de taille n,
- Chiffrement et déchiffrement bloc par bloc,
- Différents modes $\circledast$: comment les blocs seront chiffrés,
  - ECB (Electronic Code Book)
  - CBC (Cipher Block Chaining)
  - CFB (Cipher FeedBack)
  - ...
- Blocs itérés
- Exemples : DES, AES, ...

Blocs itérés

Définition

Le bloc m_i du message m est transformé r fois successivement par une **fonction de ronde**.

- Le nombre r est le nombre de rondes.
- La fonction de ronde dépend d'une **clé de ronde**.

Exemple :

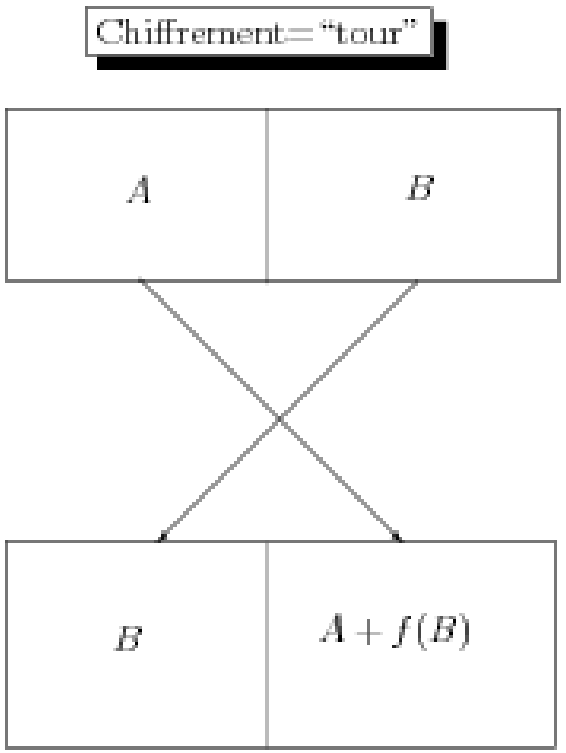
$$C_i = g(Ci - 1, K_i) \text{ pour } i = 1, \ldots, r \text{ avec}$$

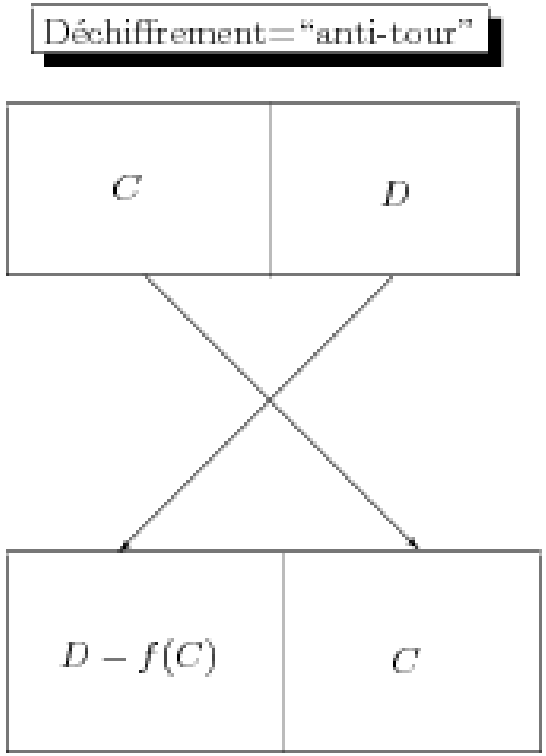
- C_0 : le clair,
- g : la fonction de ronde avec g inversible,
- K_i : les clés de ronde,
- C_r : le chiffré.

Le déchiffrement se déroule suivant le processus inverse.

Exemple : le cryptosystème DES

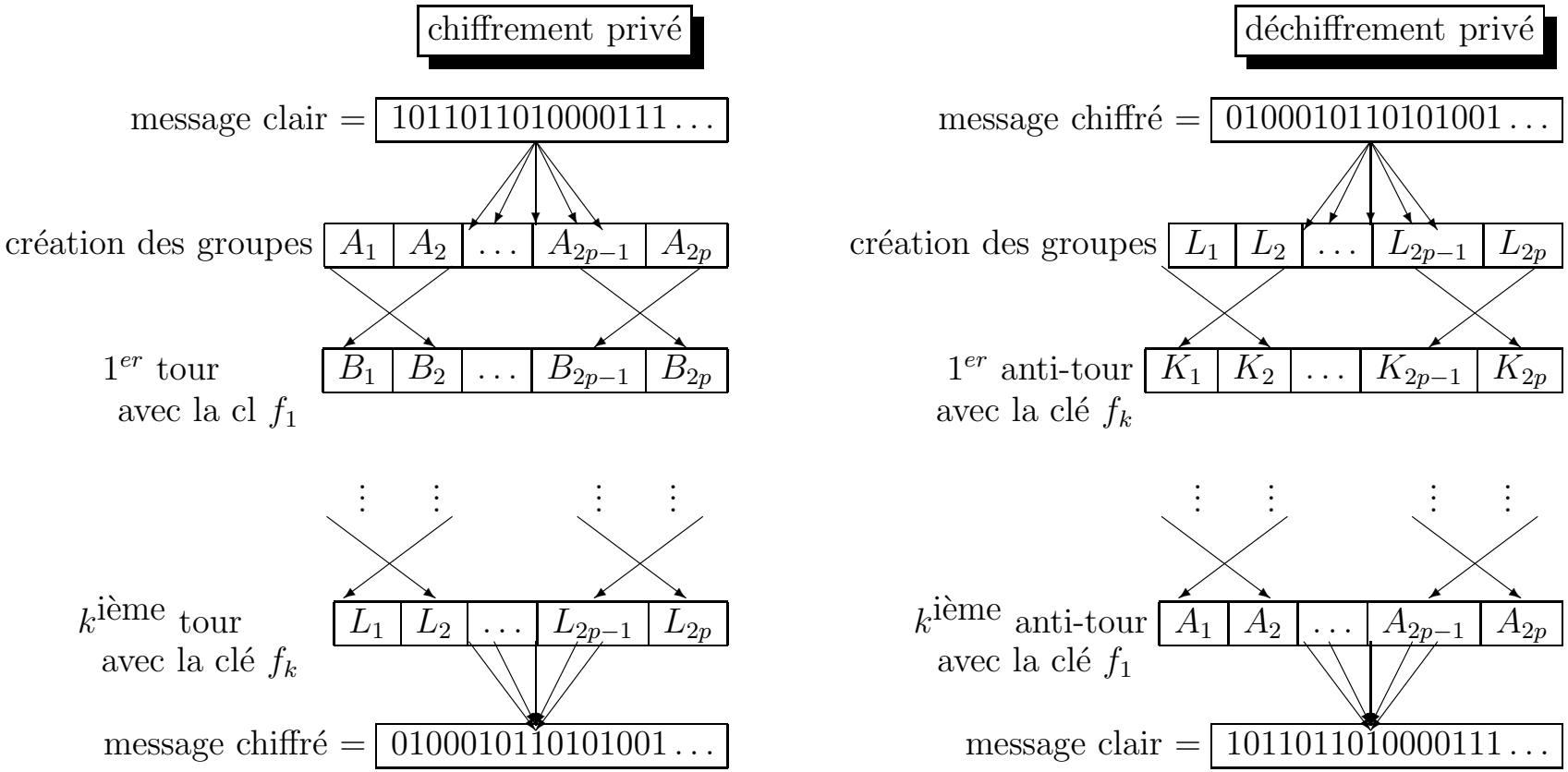
L'opération de base de l'algorithme DES est *La méthode de Feistel* et consiste à échanger/combiner deux groupes de bits adjacents.





Exemple : le cryptosystème DES

Le DES consiste à répéter de nombreuses fois de suite la méthode de Feistel avec différentes fonctions à chaque fois.



Exemple : le cryptosystème DES

Pour cet exemple on raisonne modulo 10 et les opérations se font chiffre par chiffre : $[1\,2\,3\,4] \oplus [5\,3\,9\,0]$.

Exemple

Supposons que l'on veuille chiffrer le message $M = [1\,2\,3\,4\,5\,6\,7\,8]$ avec la clef $C = [2\,5\,1\,2]$.

1. **Initialisation.** On découpe M en une partie gauche et une partie droite que l'on note M_0.
2. **Premier tour.**
   - On échange la partie droite et la partie gauche de M_0.
   - On fait une permutation circulaire des chiffres de la partie droite.
   - On ajoute la clef secrète C à la partie droite pour obtenir M_1.
3. **Deuxième tour.** On recommence le processus pour obtenir un message M_2.