

Cryptologie symétrique

DUT S4

Pierre Ramet: ramet@labri.fr

2014-2015

Plan

1 La cryptologie

- Introduction
- La cryptographie
- La cryptanalyse

2 Vieux chiffrements alphabétiques

3 Chiffrement par blocs

Un peu d'histoire

- Depuis la nuit des temps les hommes, surtout les militaires, ont pratiqué l'espionnage et le contre-espionnage
- Le chiffrement des messages est donc né presque en même temps que l'écriture



FIGURE: Le disque de Phaïstos
(Crète 1700 av. JC)



FIGURE: Le Scytale (Sparte 400 av. JC)

Introduction

- La cryptologie est la science des messages secrets et des codes chiffrés utilisée traditionnellement par les militaires et les gouvernements
- Depuis l'avènement des transactions électroniques, la cryptologie s'est démocratisée
 - Banques
 - Internet
 - Mail
 - ...

Définitions

■ Cryptographie

Definition

Ensemble des principes, méthodes et techniques dont l'application assure le chiffrement et le déchiffrement des données, afin d'en préserver la confidentialité et l'authenticité

■ Cryptanalyse

Definition

Ensemble des méthodes et procédés de décryptage visant à rétablir en clair un cryptogramme, sans connaissance préalable de la clé de chiffrement

Objectifs

- Le but de la cryptographie est de développer des procédés permettant à deux personnes de communiquer tout en protégeant leur messages
 - Préserver la **confidentialité** des messages
 - Vérifier l'**intégrité** des messages
- Outil important de la politique de sécurité

Plan

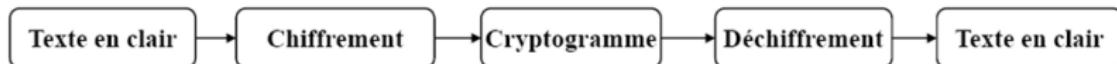
1 La cryptologie

- Introduction
- **La cryptographie**
- La cryptanalyse

2 Vieux chiffrements alphabétiques

3 Chiffrement par blocs

Définitions



■ **Texte en clair (*PlainText*)**

Definition

Texte d'origine, immédiatement intelligible et pouvant donc être exploité directement, sans recours au déchiffrement

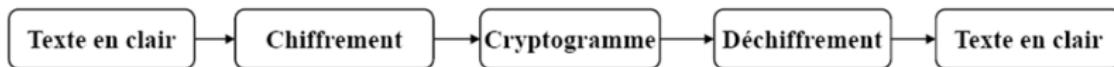
■ **Chiffrement (*Encryption*)**

Definition

Opération par laquelle est substitué, à un texte en clair, un texte inintelligible, inexploitable pour quiconque ne possède pas la clé permettant de le ramener à sa forme initiale



Définitions (2)



■ **Cryptogramme** (*Texte chiffré, Ciphertext*)

Definition

Message rendu inintelligible grâce au chiffrement, qui ne peut être compris et utilisé que par les seules personnes en possession de la clé permettant de le déchiffrer

■ **Déchiffrement** (*Decryption*)

Definition

Opération inverse d'un chiffrement réversible, permettant à une personne autorisée, en possession de la clé, de rétablir en clair un cryptogramme

Qu'est ce qu'un cryptosystème ?

Definition

Un cryptosystème est un quintuplet (M, C, K, E, D)

- M l'ensemble des textes clairs possibles
- C l'ensemble des textes chiffrés
- K l'ensemble des clés
- E l'ensemble des fonctions de chiffrement
 - De la forme $e_k, k \in K, \text{t.q } e_k(m) \in C$
- D l'ensemble des fonctions de déchiffrement
 - De la forme $d_k, k \in K, \text{ t.q } d_k(e_k(m)) = m$

Exemple

- Deux espions français veulent s'échanger des informations dans un café
- Protocole :
 - Ils se mettent d'accord sur une langue étrangère qu'ils connaissent tous les deux
 - Ils s'échangent leurs informations dans cette langue
- Déterminer M et C
- Déterminer K
- Déterminer e_k et d_k pour un k fixé
- Déterminer E et D

Qualités d'un cryptosystème

- Trois qualités recherchées :

- **Confusion**

- Aucune propriété statistique ne peut être déduite du message chiffré ⇒ message inintelligible

- **Diffusion**

- Toute modification du message en clair se traduit par une modification complète du chiffré

- **Robustesse de la clé**

- Difficile de déterminer k (difficile également d'énumérer tous les k)

Plan

1 La cryptologie

- Introduction
- La cryptographie
- La cryptanalyse

2 Vieux chiffrements alphabétiques

3 Chiffrement par blocs

Cryptanalyse

- Afin de briser un code secret et obtenir ainsi les textes en clair, l'attaquant a diverses possibilités :
 - Attaques passives : par écoute électronique, l'attaquant obtient une copie de tous les textes chiffrés échangés entre les intervenants
 - Attaques actives : l'attaquant joue un rôle actif lors du protocole et peut altérer ou détruire des messages

Types d'attaques

Attaques possibles :

1 A texte chiffré

- L'attaquant possède une copie des cryptogrammes échangés

2 A texte en clair connu

- L'attaquant possède plusieurs paires (texte clair, texte chiffré)

3 A texte clair choisi

- L'attaquant possède plusieurs paires (texte clair, texte chiffré) dont il a choisi le texte clair

4 A texte chiffré choisi

- L'attaquant choisit plusieurs cryptogrammes dont il obtient le texte en clair correspondant

Attaques physiques

Ne pas oublier les attaques physiques !

- Les algorithmes de chiffrement et déchiffrement doivent être implémentés sur un ordinateur
 - Ordinateur personnel
 - Carte à puce
- Observation indirecte du calculateur (*side channel attacks*)
 - Mesure de la consommation électrique (*Power Analysis*)
 - Mesure du rayonnement électromagnétique
 - Mesure du temps (*Timing attacks*)
 - RSA & Hyper Threading 2005
- Erreurs d'implémentation
 - Clés openssl debian 2006

Résultats d'une attaque

1 Cassage partiel

- L'attaquant calcule quelques informations sur le texte en clair

2 Cassage local

- L'attaquant calcule quelques couples (texte en clair, texte chiffré)

3 Cassage global

- L'attaquant calcule la fonction d_k , et peut donc déchiffrer tout message

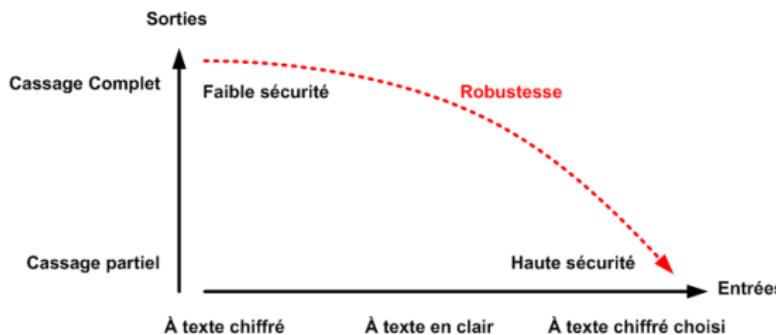
4 Cassage complet

- L'attaquant connaît la clé k

Sûreté d'un cryptosystème

Definition

Définir un protocole (ou cryptosystème) sûr c'est définir un protocole robuste face à une attaque disposant de moyens importants (Entrée) et ayant un objectif (Sortie) modeste.



Un exemple d'attaque célèbre

- La bataille de Midway
 - Juin 1942, Américains vs Japonais
- L'attaque :
 - Les américains ont envoyés un faux message en clair entre deux de leurs postes
 - Ils ont attendu que les Japonais l'interceptent
 - Et qu'ils le rétransmettent **chiffré** à leur état major !
- Les américains ont disposé d'un couple $(m, e_k(m))$ et ont pu en déduire k
- Quel type d'attaque ? Quel résultat ?

Récapitulatif

- La **cryptographie** est l'art de chiffrer. Elle renforce :
 - La **confidentialité**
 - L'**authenticité**
- La **cryptanalyse** est l'art de casser des chiffrements
 - Plusieurs types d'**attaques** (texte chiffré connu, texte clair connu, etc.)
 - Plusieurs types de **résultats** (cassage partiel, cassage total, etc.)
- Un protocole de cryptographie **robuste** est un protocole qui :
 - pour une attaque facile (entrées importantes) ...
 - révèle peu d'informations

Plan

1 La cryptologie

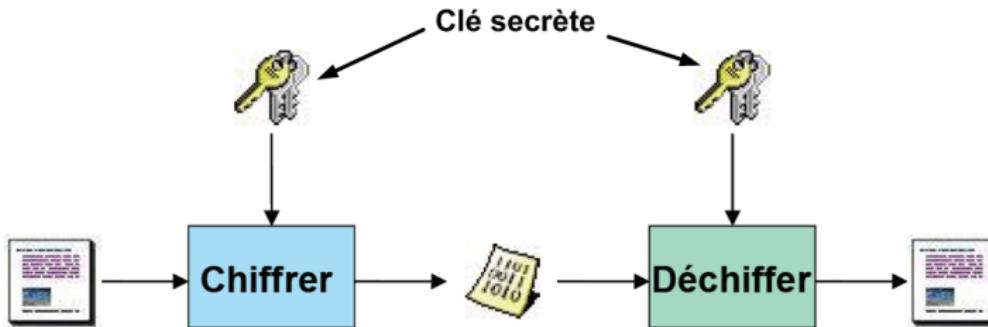
2 Vieux chiffrements alphabétiques

- Chiffrement par transposition
- Chiffrements monoalphabétiques
- Chiffrements polyalphabétiques

3 Chiffrement par blocs

La cryptographie à clé secrète

- La cryptographie à clé secrète
 - Les deux acteurs s'échangent une clé secrète (mot de passe)
- La sécurité du chiffrement dépend de la non divulgation de cette clé

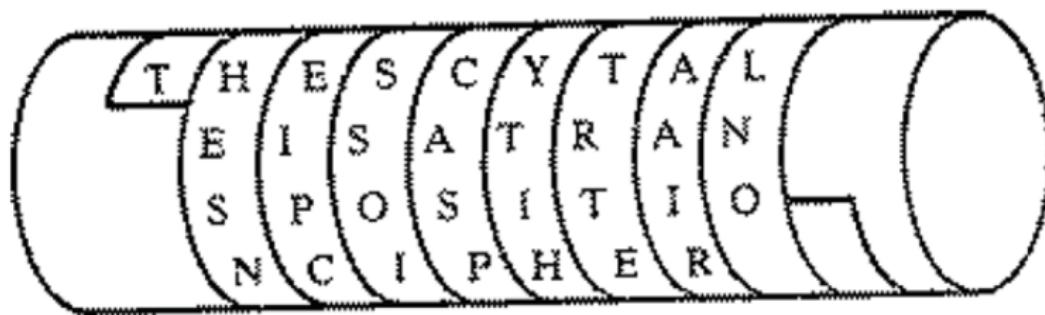


Chiffrement par transposition

- Chiffrement de type *anagramme*
 - Les lettres du messages sont déplacées
- Niveau de sécurité théorique
 - Message de 35 lettres : $35!$ chiffrés possibles
 - Problèmes
 - Confusion sur la syntaxe, mais chaque lettre conserve sa valeur
 - Diffusion ?
 - Pas robuste pour des messages courts
 - Clé "*complexe*"

Exemple de transposition

- La scytale spartiate (5ème siècle av. JC) :



Plan

1 La cryptologie

2 Vieux chiffrements alphabétiques

- Chiffrement par transposition
- **Chiffrements monoalphabétiques**
- Chiffrements polyalphabétiques

3 Chiffrement par blocs

Substitution

- Chiffrement en changeant d'alphabet
 - Kama Sutra : mlecchita-vikalpa ou art de l'écriture secrète (4ème siècle av JC)
- Niveau de sécurité **théorique**
 - Alphabet à 26 lettres : $26!$ alphabets possibles
- Problèmes
 - Confusion sur l'alphabet mais ...
 - ... chaque lettre conserve sa place d'origine

Le chiffrement de César

- Jules César : chiffrement d'un message par décalage des lettres dans l'alphabet ($a \rightarrow d, b \rightarrow e, c \rightarrow f \dots$)
- On travaille modulo 26
- La clé est le décalage (26 possibilités)

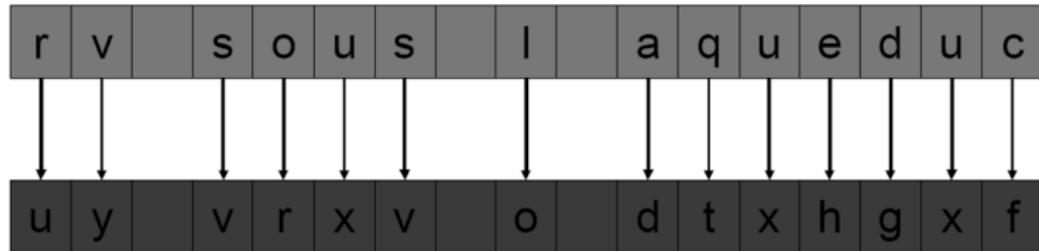
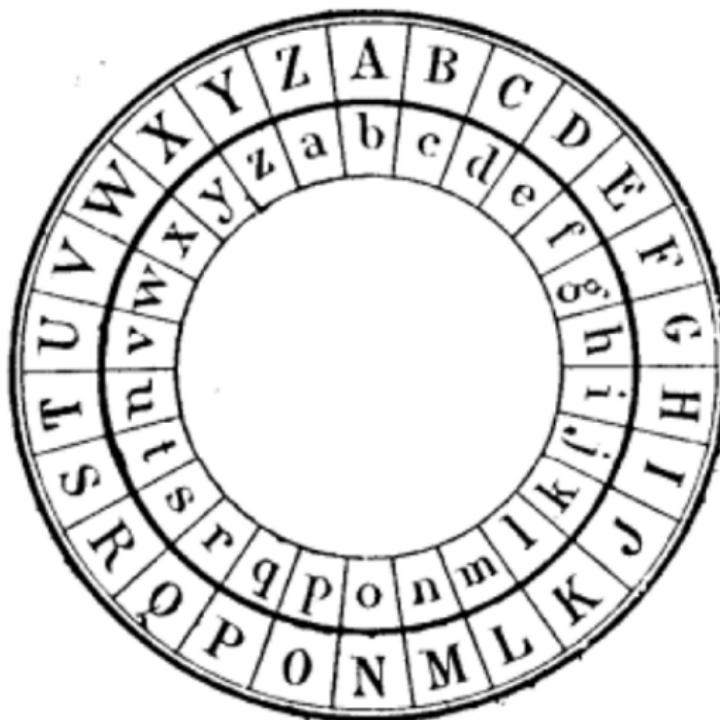


FIGURE: César, avec $d=3$

Le chiffrement de César (2)



Problèmes

- Confusion faible
- Pas de diffusion
- Seulement 26 clés possibles
- Cassage de l'algorithme :
 - Tester toutes les clés ! (attaque *exhaustive*)

La substitution monoalphabétique

La **substitution monoalphabétique** :

- Remplacer chaque lettre de l'alphabet par une autre
 - Revient à un décalage différent pour chaque lettre
- Clé : la **permutation**
 - Alphabet clair : abcdefghijklmnopqrstuvwxyz
 - Alphabet chiffré : MOTSECRUVWXYZABDFGHIJKLMNOPQ
- Texte clair : l erreur est humaine, y persévérez est diabolique
- Texte chiffré : Y EGGEJG EHI UJZMVAE, P DEGHEKEGEG EHI SVMOBYVFJE

La substitution monoalphabétique (2)

- Grand nombre de clés
- Mais toujours pas de diffusion
- Même si l'algorithme est connu, il est impossible d'essayer les $26! - 1$ clés possibles ($403291461126605635583999999$)
- Il est cependant possible de tirer partie des caractéristiques de la langue française

Cryptanalyse de la substitution monoalphabétique

- Principe (Al-Kindi - 9ème siècle)
- Toutes les lettres de la langue française n'ont pas la même fréquence d'apparition
- Par analyse statistique de la fréquence des lettres de l'alphabet chiffré, il est possible de retrouver les substitutions
- Particulièrement vrai si le texte chiffré est long

Cryptanalyse de la substitution monoalphabétique (2)

Lettre	Fréquence %
A	9.42
B	1.02
C	2.64
D	3.39
E	15.87
F	0.95
G	1.04
H	0.77
I	8.41
J	0.89
K	0.00
L	5.34
M	3.24

Lettre	Fréquence %
N	7.15
O	5.14
P	2.86
Q	1.06
R	6.46
S	7.90
T	7.26
U	6.24
V	2.15
W	0.00
X	0.30
Y	0.24
Z	0.32

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
t	f	g	i	w	y	d	q	e	a	s	n	l	c	x	u	h	r	v	z	m	k	j	b	o	p

Cryptanalyse de la substitution monoalphabétique (3)

- Pour déterminer les substitutions des lettres dont la fréquence est semblables à d'autres lettres :
 - Calcul des fréquences de blocs de deux lettres ("de", "au", "ch")
 - Calcul des fréquences des blocs de trois lettres
- Vérifier de manière automatique avec un dictionnaire
- Au pire, une dizaine d'essais sont nécessaires
 - Si le texte chiffré est suffisamment long !
 - Si le texte chiffré appartient bien à une langue !

Autres cryptosystèmes

- ... et bien d'autres cryptosystèmes à substitution monoalphabétique :
 - Chiffrement affine
 - OU logique
 - etc
- Mais tous sont vulnérables à une analyse fréquentielle

Récapitulatif

- Les deux méthodes précédentes appartiennent aux systèmes de **substitution mono-alphabétique**
 - Dans un texte en clair, une lettre est toujours substituée par la même lettre
- Si le texte est suffisamment long, il est possible de trouver la substitution en analysant **la fréquence des lettres**
 - Donc, le texte en clair peut être retrouvé à partir du cryptogramme seul
 - Quel type d'attaque ?

Même si le nombre de clés est grand, cette méthode n'est pas acceptable

Plan

1 La cryptologie

2 Vieux chiffrements alphabétiques

- Chiffrement par transposition
- Chiffrements monoalphabétiques
- Chiffrements polyalphabétiques

3 Chiffrement par blocs

Le chiffrement de Vigenere

L'algorithme de Vigenere

- Blaise Vigenère 1523-1596
- Clé=suite de lettres de longueur k (ex : "ac", $k=2$)
- Algorithme : Additionner à chaque lettre la lettre de la clé.

C	H	A	T	E	A	U
A	C	A	C	A	C	A
D	K	B	W	F	D	V

Le chiffrement de Vigenere (2)

- Le chiffre de Vigenère appartient aux systèmes de substitution poly-alphabétique.
 - Dans un texte en clair, une lettre est substituée par une autre lettre dépendant de sa position dans le texte
- Confusion : un peu mieux
- Diffusion : toujours aucune
- Si le texte est suffisamment long, il est possible de trouver les substitutions en découplant le texte selon la longueur présumée de la clé puis en analysant les fréquences des lettres
 - Donc, le texte en clair peut être retrouvé à partir du cryptogramme seul

Cryptanalyse Vigenere

Cryptanalyse Vigenere :

- Méthode en trois étapes :
 - 1 Trouver la longueur l de la clé
 - 2 Découper le message M en l messages $m_0 \dots m_{l-1}$
 - m_i contient l'ensemble des lettres dont la position dans le texte modulo l est égal à i
 - Exemple : si l'on aligne M sur l colonnes, m_i est la i ème colonne (cf. tableau)
 - Toutes les lettres d'un m_i sont chiffrées avec le même décalage
 - 3 Analyse fréquentielle sur chacun des m_i
 - Déterminer le décalage de chaque colonne
- Sortie : la clé k

Trouver la longueur de la clé

Première méthode : répétition de séquences

- On part du principe que :
 - Deux mots identiques dans le texte chiffré \Rightarrow sûrement deux mots identiques dans le texte en clair
- La première lettre de ces deux mots a été chiffrée avec la même lettre de la clé
 - Surtout à la même position dans la clé !
- La distance entre les deux mots est donc un multiple de la longueur de la clé
- Avec plusieurs séquences identifiées, on arrive à déterminer la longueur de la clé

h	i	v	e	r	h	i	v	e	r	h	i	v	e	r	h	i	v	e	r
K	E	Y	K	E	Y	K	E	Y	K	E	Y	K	E	Y	K	E	Y	K	E
R	M	T	O	V	F	S	Z	C	B	L	G	F	I	P	R	M	T	O	V

Exemple

XAUNMEESYIEDTLLFGSNBWQ UFXPQTYORUTYIINUMQIEUL
SMFAFXGUTYBXXAGBHMIFII MUMQIDEKRIFRIRZQUHIENO
O0IGRMLYETYOVQRYSIXEOK IYPYOIGRFBWPIYRBQURJIY
EMJIGRYKXYACPPQSPBVESI RZQRUFREDYJIGRYKXBLOP J
ARNPUGEFBWMILXMZSMZYXP NBPUMYZMEEFBUGENLRDEPB
JXONQEZTMBWOEFIIPAHPHQ BFLGDEMFWFAHQ

- On trouve :
 - UMQI se retrouve après 30 caractères
 - OIGR se retrouve après 25 caractères
 - JIGRY se retrouve après 30 caractères
- La longueur de la clé doit être un diviseur de 30 et de 25 : il est possible qu'il s'agisse de 5

Trouver la longueur de la clé

Deuxième méthode : indices de coïncidence

- Indice de coïncidence d'un texte :
 - L'indice de coïncidence est la probabilité que deux lettres choisies au hasard dans un message m donné soient identiques
 - $IC \simeq \sum_{i \in [1, 26]} \frac{f_i^2}{|m|^2}$
 - f_i est le nombre d'occurrence de la lettre i dans le message
 - $|m|$ est la taille du message
 - Pour un message en français, on a $IC \simeq 0,075$
 - ... et également pour toute substitution **monoalphabétique**
 - Calculé d'après la fréquence des lettres (cf. précédemment)
 - Pour un message aléatoire, on a $IC \simeq 26 * \frac{1}{26^2} \simeq 0,038$

Trouver la longueur de la clé

Algorithme :

- Pour l de 1 à $+\infty$
 - Découper le message M en l messages $m_0 \dots m_{l-1}$
 - m_i est l'ensemble des lettres dont la position modulo l vaut i
 - Pour tout message m_i :
 - Calculer $IC_i = IC(m_i)$
 - Si tous les IC_i sont proches de 0,075, renvoyer l

Exemple pour le texte précédent :

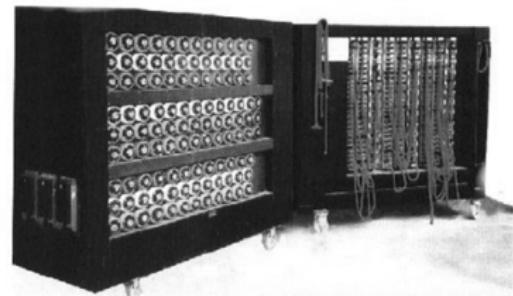
	$i=1$	$i=2$	$i=3$	$i=4$	$i=5$
$l=1$	0,045				
$l=2$	0,046	0,041			
$l=3$	0,043	0,050	0,047		
$l=4$	0,042	0,039	0,046	0,040	
$l=5$	0,063	0,068	0,069	0,061	0,072

Casser la clé

- Avec la connaissance de l , casser la clé devient trivial
- Découper le message M en l messages $m_0 \dots m_{l-1}$
 - m_i est l'ensemble des lettres dont la position modulo l vaut i
- Déterminer le décalage d_i pour chaque m_i
 - Via l'analyse de fréquence "*classique*"
- La clé est $d_0 d_1 \dots d_{l-1}$
- L'algorithme de Vigenere est donc sensible à une **attaque à texte chiffré**
 - Encore une fois si le texte est long, et qu'il est écrit dans un langue

Améliorations

- Améliorations des chiffrements polyalphabétiques
 - Enigma (1920) : 5 rotors de substitution (2^{50} clés)
 - La Bombe de Turing l'a cassé en une heure
 - Etape décisive dans la victoire des alliés



Le *One-Time Pad*

- Chiffrement parfait
 - La clé est aussi longue que le message à chiffrer
 - La clé est nouvelle pour chaque nouveau message
- Confusion totale
 - Chiffrement de "aa...aaa" complètement aléatoire
- Diffusion totale
 - Assurée car la clé n'est **jamais** réutilisée : résultat différent lorsque on rechiffre "aa...aaa"
- Utilisé par le *KGB* (malette diplomatique)
- Problèmes :
 - Transmission de la clé ? Stockage ?
 - Si on arrive à transmettre la clé, pourquoi pas le message ?

Récapitulatif

- Les chiffrement à substitution polyalphabétique
 - Vigenere : protocole **faible**
 - *One-Time Pad* : **peu pratique**
- Les chiffrement alphabétiques ont été peu à peu **abandonnés**
- Pour laisser la place aux chiffrements par **blocs**

Plan

1 La cryptologie

2 Vieux chiffrements alphabétiques

3 Chiffrement par blocs

- Le principe
- Les réseaux de Feistel
- DES, AES et les autres

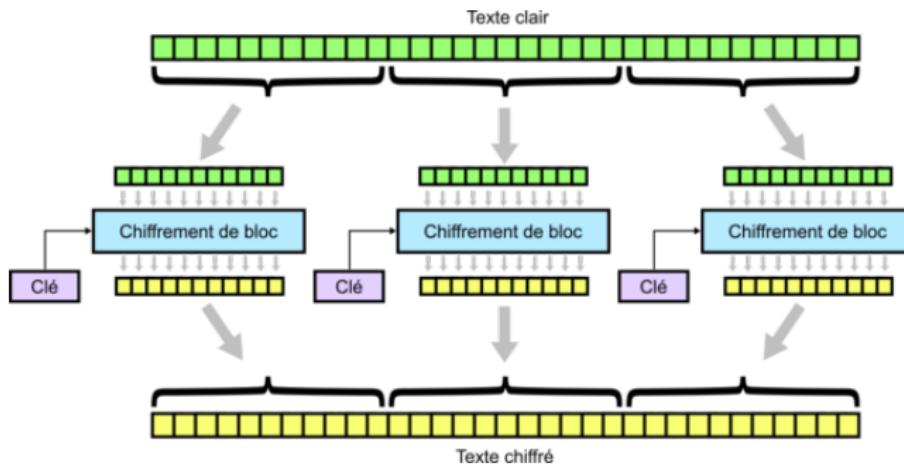
Chiffrement par blocs

Chiffrement par blocs :

- On ne travaille plus sur des lettres de l'alphabet, mais sur un ensemble de **blocs**
- Taille des blocs : 32bits ... 256bits
- Le message m est découpé en n blocs
- Chaque bloc est chiffré
- Le message chiffré m' est la concaténation des blocs chiffrés

Premier exemple : le mode ECB

- Le mode **ECB** (Electronic Cypher Block)
- Mode de chiffrement **le plus simple**
- Chaque bloc est chiffré tout simplement avec la clé



Problèmes

Mode **trop** simple :

- Mode de chiffrement pas très sûr
- Revient à faire de la substitution monoalphabétique (sur un alphabet plus grand)
- A votre avis :
 - Confusion ?
 - Diffusion ?
- Rarement utilisé

Problèmes (2)

- Deux textes en clair :

JOHN 105000

JACK 500000

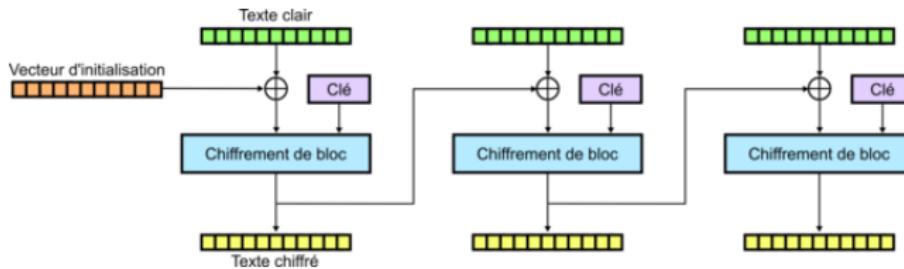
- Textes chiffrés (blocs de deux lettres) :

Q9|2D|**FP**|VX|**C9**|**IO**
LD|AS|**FP**|**C9**|**IO**|**IO**

- Si John connaît son salaire, il peut deviner celui de Jack
 - Et être très jaloux !

Le mode CBC

- Le mode **CBC** (Cypher Block Chaining)
- Le résultat du chiffrement d'un bloc m dépend
 - De la clé
 - Du bloc $m - 1$
- Exemple :

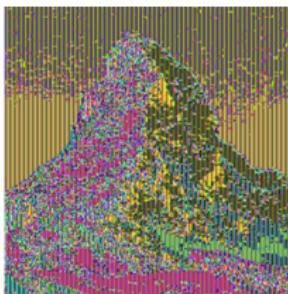


Etude

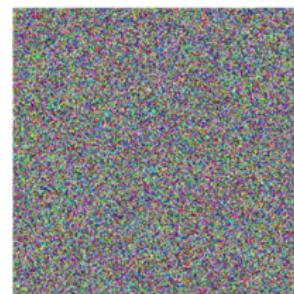
- Avantages :
 - Bien meilleure diffusion !
- Inconvénients :
 - Il faut se mettre d'accord sur un vecteur d'initialisation
- Mode **très utilisé**



Clair



ECB



CBC

FIGURE: Image chiffrée (blocs de 4 pixels)

Les autres modes

- D'autres modes dans la même veine :
 - **CFB** : Cypher FeedBack Mode
 - **OFB** : Output FeedBack Mode
 - **CTR** : CounTeR Mode
 - etc.
- Presque tous ont une bonne diffusion
- Voyons maintenant les algorithmes de **chiffrement** des blocs

Plan

1 La cryptologie

2 Vieux chiffrements alphabétiques

3 Chiffrement par blocs

- Le principe
- **Les réseaux de Feistel**
- DES, AES et les autres

Les réseaux de Feistel

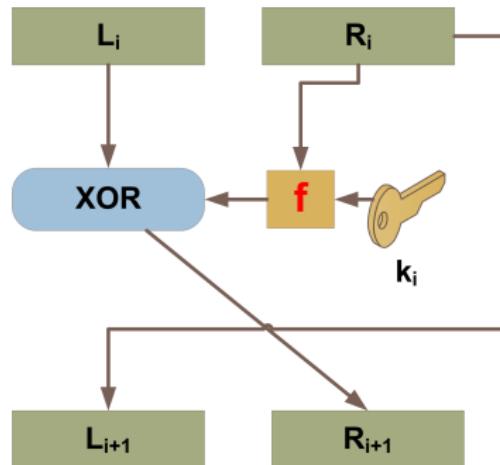
Definition

Un réseau de Feistel est une construction utilisée dans les algorithmes de chiffrement par bloc, nommée d'après le cryptologue d'IBM, Horst Feistel

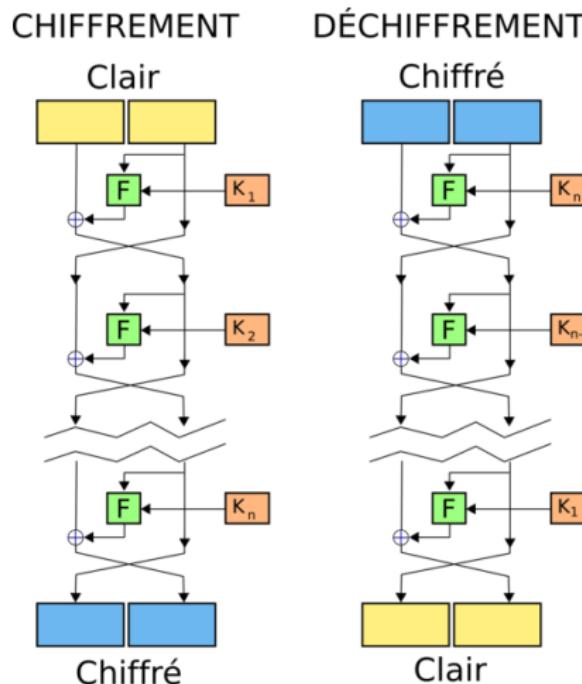
- Fonction de chiffrement des blocs (le carré "Chiffrement de bloc" des schémas précédent)
- Un réseau de Feistel est défini par :
 - Une longueur de bloc l
 - Un espace de clé K
 - Un nombre de ronde r
 - Un générateur de sous-clés g , qui divise une clé k en r sous-clés
 - Une fonction de chiffrement f (f^{-1} doit exister)

Fonctionnement

- Principe d'un réseau de Feistel ;
 - On découpe le bloc à chiffrer en deux bloc L et R de même taille
 - On calcule r sous-clés $k_1 \dots k_r$ à partir de la clé k
 - On effectue r rondes consécutives :



Les réseaux de Feistel (2)



Les réseaux de Feistel (3)

■ Quelques précisions :

- Générateur des clés k_i : on choisit x bits depuis k
 - Et on les permute éventuellement
- La fonction f :
 - Souvent **Substitution + Permutation**

■ Avantages des réseaux de Feistel

- Bonne diffusion si r bien choisi
- Bonne confusion si f bien choisie
- Facile à implémenter (hardware)
- Parallélisable

Plan

1 La cryptologie

2 Vieux chiffrements alphabétiques

3 Chiffrement par blocs

- Le principe
- Les réseaux de Feistel
- DES, AES et les autres**

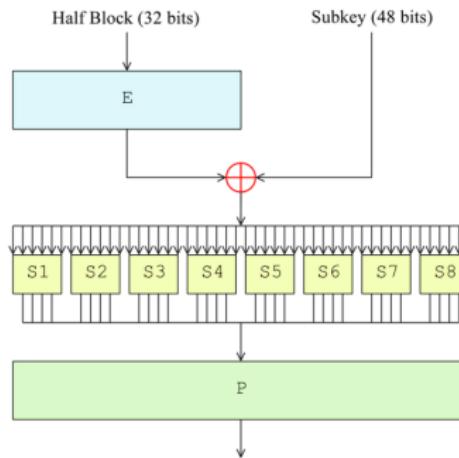
DES

L'algorithme DES :

- **Data Encryption Standard**
- Historique :
 - Milieu des années 70
 - Premier algorithme de chiffrement pour l'industrie
- Principe :
 - C'est un réseau de Feistel
 - Blocs de 64bits (32+32)
 - Clé k de 56bits
 - Sous-clés k_i de 48bits
 - Nombre de rondes $r = 16$
 - Fonction f : permutation + substitution

La fonction f de DES

- La fonction f de DES :
 - On XOR le demi-bloc avec k_i
 - Substitution de bits (SBOXes)
 - Puis permutation (PBOX)



Propriétés de DES

- Avantages
 - Rapide !
 - Puces dédiées au DES : en 1995, le 6868 de VLSI permettait de chiffrer 64 Mo par seconde
 - Bonne diffusion
 - Bonne confusion
 - Facile à implémenter en hard (cartes à puce)
- Inconvénients
 - Taille de la clé (56 bits)
 - Méthodes pour casser la clé :
 - Attaque exhaustive
 - Cryptanalyse linéaire
 - Cryptanalyse différentielle (2^{47} textes clairs choisis nécessaires)

Confusion et diffusion

■ Confusion

- Confusion totale
- Chiffrement de "aaaaaaaaaaaaaaaaaaa" :

```
f99a 4388 c6a8 57db 1a0c c4d4  
ad1a 89f7 119d 9d91 7827 94b5
```

■ Diffusion

- Diffusion totale (en mode CBC)
- Chiffrement de "eaaaaaaaaaaaaaaaaaa" :

```
a290 3816 10d3 97e7 aa2a 25f3  
c3e0 a3cf 9438 f2b2 dbb8 f3da
```

Coûts des attaques

Méthode d'attaque	Texte connu	Texte choisi	Complexité de stockage	Complexité de calcul
Préc calcul exhaustif		1	2^{56}	1 tableau
Recherche exhaustive	1			2^{55}
Cryptanalyse linéaire	2^{43}		<i>Pour les textes</i>	2^{43}
	2^{38}		<i>Pour les textes</i>	2^{50}
Cryptanalyse différentielle		2^{47}	<i>Pour les textes</i>	2^{47}
	2^{55}		<i>Pour les textes</i>	2^{55}

Attaque exhaustive

- Coût d'une attaque exhaustive en 1996 :

Type d'attaquant	Budget	Outil	Clé de 40 bits	Clé de 56 bits
Simple hacker	Négligeable	Soft	1 semaine	Impossible
	300 €	Circuit prédiffusé	5 heures	38 ans
PME	7500 €	Circuit prédiffusé	12 minutes	18 mois
Grande entreprise	225 k€	Circuit prédiffusé	24 secondes	19 jours
	225 k€	ASIC	0.18 seconde	3 heures
Multinationale	7,5 M€	ASIC	5 msec.	6 minutes
Etat	225 M€	ASIC	0.2 msec.	12 secondes

- Maintenant, encore moins cher ! (Clusters de PS3)
- Et DES représente toujours 50% du marché
 - Car pas cher et rapide
 - Rapporte entre 75M\$ et 125M\$ aux USA chaque année

Cluster de PS3



	DES Cracker	PS3 cluster
Prix	\$250'000	\$120'000
Temps	9 jours	6 jours
Clés/sec	88.8 mia	142.5 mia
Unités de calcul	37050	1320
Année	1999	2009

Autres algorithmes

Autres algorithmes de type réseau de Feistel :

- **TDES (Triple DES)**

- On enchaîne trois DES (force effective 112bits de clé)
 - Lent

- **BlowFish**

- Blocs de 64bits
 - Clé de 32 à 448bits
 - 16 rondes

- **Camelia**

- Clé de 128 à 256bits
 - 18 à 24 rondes
 - Standard du gouvernement Japonais

- **RC5**

AES

L'algorithme **AES** (Advanced Encryption Standard) :

- Devant l'échec de DES, nouveau standard en 2000
- Variante du réseau de Feistel
- Trois versions :
 - Chiffrement de blocs de 128 bits avec une clé de 128 bits (10 rondes)
 - Chiffrement de blocs de 192 bits avec une clé de 192 bits (12 rondes)
 - Chiffrement de blocs de 256 bits avec une clé de 256 bits (14 rondes)
- Fonction f : calcul matriciel

AES

- Plusieurs modes (ECB, CBC, CTR, etc)
- Plus rapide que TDES
- Nécessite peu de mémoire (cartes à puces)
- Résistant aux attaques :
 - Pas de cryptanalyse linéaire
 - Pas de cryptanalyse différentielle
- Actuellement, la seule solution est la **recherche exhaustive**
- C'est le nouveau standard

Récapitulatif

- Cryptologie = cryptographie + cryptanalyse
- Substitutions alphabétiques
 - Vulnérables aux analyses de fréquences
 - Sauf One-Time Pad mais peu pratique
- Actuellement, chiffrement par **blocs**
 - Plusieurs **modes** (ECB, CBC, CTR, etc)
 - Bonnes confusion et diffusion (sauf pour ECB)
 - **DES** : rapide mais clé trop faible aujourd'hui
 - Successeur : **AES**