Introduction à la Cryptographie

Gérard Beuchot

Maître de conférences au

Département Informatique de l 'INSA de Lyon

Membre du laboratoire ICTT de l 'INSA de Lyon

beuchot@if.insa-lyon.fr

http://ictt.insa-lyon.fr/beuchot/

- Cryptographie
  - L'art d'écrire en caractères secrets...
- Chiffre
  - Méthode d'écriture secrète qui remplace un message clair par un message chiffré (cryptogramme)
- Chiffrement ou chiffrage
  - action de rédiger un texte en chiffre (régulier ou irrégulier)
- Chiffrer
  - transformer un langage clair en langage chiffré
- Déchiffrer
  - reconvertir en clair un message chiffré, en utilisant la clé que l 'on possède de droit.
- Décrypter
  - déchiffrer un cryptogramme alors qu'on en possède pas la clé ou après avoir reconstitué celle-ci

- **Clair**
  - message avant qu'il ai été chiffré ou codé
- **Clé**
  - mot, locution, phrase, nombre utilisé pour chiffrer ou déchiffrer un message
- **Code**
  - système cryptographique selon lequel des groupes de lettres sont substitués à des éléments d'un message clair
  - Moyen secret de communication autre que le chiffre, grâce auquel deux personnes peuvent échanger secrètement des informations
- **Transposition**
  - chiffre dans lequel chaque lettre du clair est reprise dans le cryptogramme mais placée à un autre emplacement
- **Substitution**
  - chiffre dans lequel chaque lettre ou groupe de lettres du clair est remplacée par une autre lettre, groupe de lettres, figure, symbole ….
- **Cryptanalyse**
  - Science de décrypter les messages secrets par analyse et déductions

- Jules César (Imperator ….)
  - inventeur d'un code à substitution élémentaire qu'il abandonna quand il ne fit plus confiance à Cicéron…
  - Tyro : scribe de Cicéron qui inventa une écriture secrète proche de la sténographie …
- Lysandre de Sparte 405 av. JC
  - Inventeur (ou utilisateur) du « scytale » qui fournissait une sorte de transposition
- Abbé Trithème 1499
  - auteur de « Polygraphia » premier traité de cryptographie
  - inventeur d 'un système chiffré : les Ave Maria (14 alphabets où une lettre est remplacée par un mot)
- Giovani Batista Belaso Della Porta 1563
  - porte le titre de père de la cryptographie moderne
- Vigenère (Blaise de) (
  - code de substitution basé sur une table de codage et un mot clé quelconque en usage jusqu'à la fin du 19ème siècle

- Diffie et Hellman
- Rivest, Shamir et Adleman
- J. Daemen et V. Rijmen
- B. Gladman

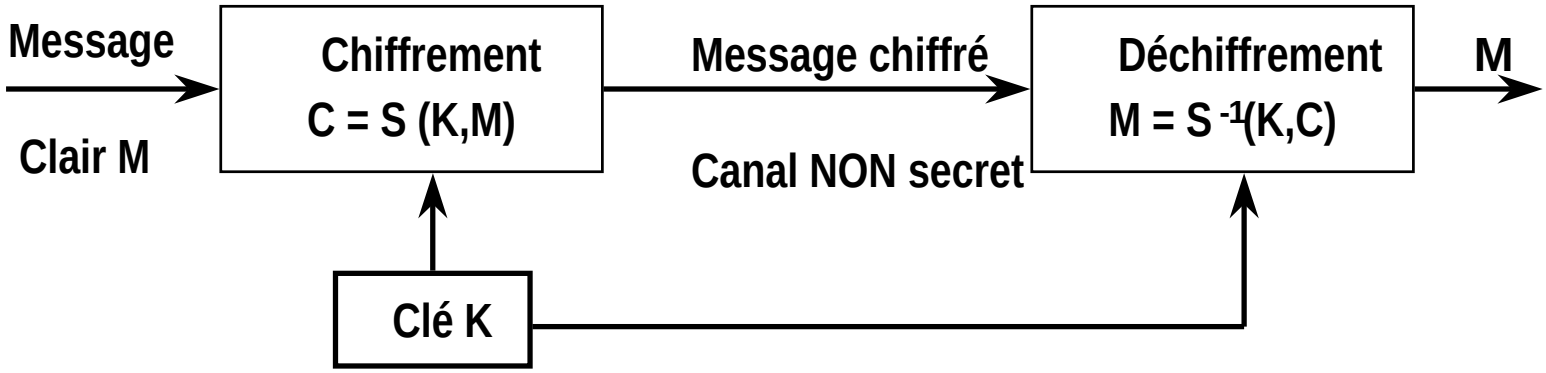
Méthodes de chiffrement

- Sûr ou inconditionnellement sûr
- Au vol ou Bloc par bloc
- à clé PRIVEE (secrète) ou à clé PUBLIQUE

Seul code inconditionnellement sûr : Vernam

- Clé aléatoire utilisée une seule fois
- C = M ⊗ K et M = C ⊗ K
- exemple
  - M = 1 0 1 1 0 0 0 1 1 1 0 1 0 1
  - K = 1 0 0 1 1 0 0 1 0 0 1 0 1 1
  - C = 0 0 1 0 1 0 0 0 1 1 1 1 1 0
  - K = 1 0 0 1 1 0 0 1 0 0 1 0 1 1
  - M = 1 0 1 1 0 0 0 1 1 1 0 1 0 1

- Utilise la même clé SECRETE pour chiffrement et déchiffrement
- Fragilité : partage de cette clé



La fonction Crytographique S est inversible

- exemples :
  - DES : Data Encryption Standard 2^{56} # 7,2 10^6 clés possibles
  - IDEA: International Data Encryption Algorithm - clé sur 128 bits
- Pour casser DES (trouver la clé)

  il suffit théoriquement de 18 caractères des textes clair et chiffré

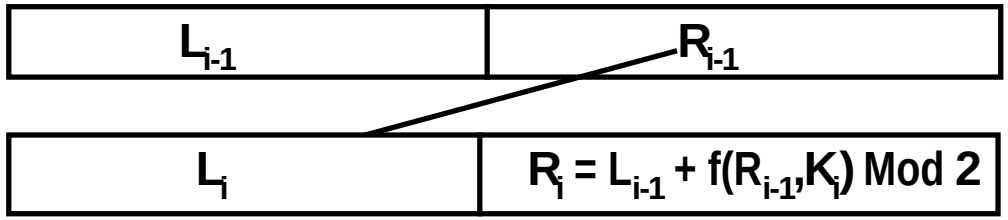
- Exemple de table (volontairement simplifiée …)

	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																										
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

- Mot clé : CADRE
  - mot clé étendu : CADRECA DR ECAD RE CADRECADRE
- Message : exemple de code de vigenere
- Codage
  - e est sous le C de CADRE : le code est à la ligne C et « g » est substitué à « e »
  - x est sous le A de CADRE : le code est à la ligne A et « x » est substitué à « x »
  - e est sous le D de CADRE : le code est à la ligne D et « h » est substitué à « e »
- Cryptogramme : gxhdtne gv gogv gi xijvrgrg

- **DES (1977)**
  - Ancien standard . Voir ci-dessous
- **DES-3**
  - DES-EEE3 : 3 DES avec 3 clés différentes
  - DES-EDE3 : 3 Opérations en séquence (chiffrement-déchiffrement-chiffrement) avec 3 clés
  - DES-EEE2 ou DES-EDE2 : comme ci-dessus mais avec clés 1 et 3 identiques
- **IDEA**
  - Code de blocs proposé par Lai et Massey. Clé de 128 bits, blocs de 64 bits, 8 itérations
- **RC2**
  - Rivest (rfc2268). Code de bloc (64 bits) clé variable de 8 à 128 bits. Plus rapide que DES
- **RC4**
  - Code des flux d'octets (stream) par de permutations aléatoires (très rapide par logiciel)
- **RC5**
  - Code de blocs. Rapide. Clé de 8 à 2048 bits. Bloc de 32, 64 ou 128 bits. 1 à 255 itérations
- **AES**
  - remplaçant de DES à partire de novembre 2001 (voir ci-dessous)

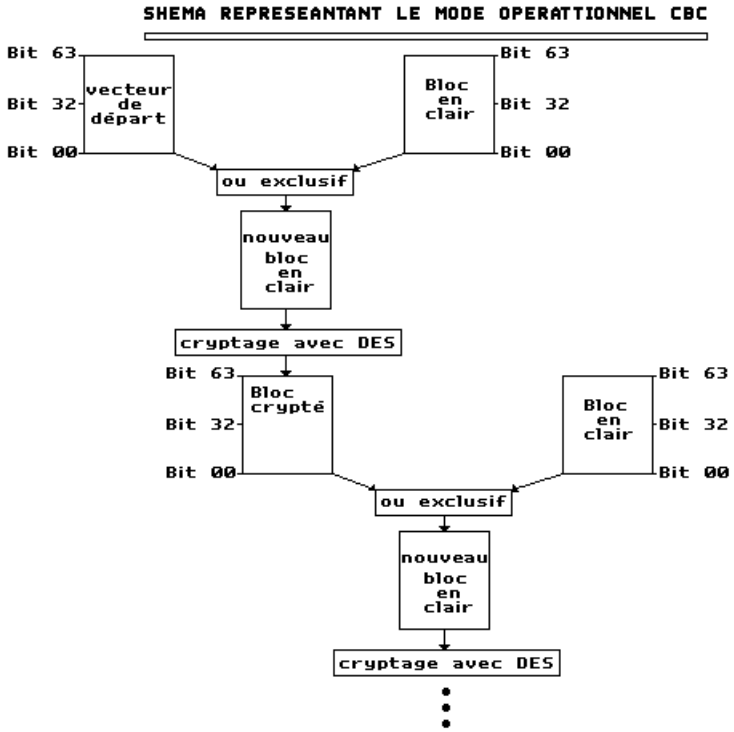
- Blocs d'information de 64 bits (8 octets)
- Clé à 56 bits (+8 de contrôle)
- Entre Transposition initiale et Transposition finale 16 itérations d'une Fonction mêlant Transposition et Substitution NON LINEAIRE (table)



$K_i = KS(i,clé)$

R_{i-1} est étendu de 32 à 48 bits par duplication de 16 de ses bits
La clé K_i est ajoutée (bit à bit , ou exclusif)
Le champ est réduit à 32 bits grâce à une table (publique)
qui fait correspondre des champs de 4 bits aux champs de 6 bits trouvés.

- Toute la puissance du DES vient de cette table qui n'a pas de propriétés mathématiques
- Difficulté: QUALITE DE LA CLE (nombre réellement aléatoire ...)



Mode EBC

- Electronic Code Book ("catalogue électronique de codes").
- Blocs de 64 bits indépendants les uns des autres
  - Problème si blocs identiques et même clé

Mode CBC

- Chain Block Cipher ("Cryptogramme à blocs chaînés").
- Chaque bloc clair est soumis avec bloc précédemment chiffré
  - en plus de la clé commune : vecteur initial

- Nouveau standard élaboré pour remplacer DES
- Cahier des charges
  - Très robuste
  - Blocs de 128 bits (autres tailles en option)
  - Clés symétriques (privées) de 128, 192 et 256 bits
  - Plus efficace et sécurisant que Triple DES
  - Élaboré et évalué publiquement - libre de droits
- 15 propositions dont DFC de ENS (Vaudanay) : 5 retenues
  - MARS d'IBM : même principe que DES - blocs de 4*32bits - clés 128 à 448 bits
    - très robuste - 8 itérations initiales et finales - S-Bloc de 512 mots de 32bits
  - RC6 de RSA : extension de RC5 - simple et rapide - clé jusqu'à 2040 bits
  - Rijndael de J. Daemen et V. Rijmen
  - Serpent de R. Anderson, E. Biham, L. Knudsen : robuste le + lent par soft
  - Twofish de B.Schneier, J.Kelsey, D.Whiting, D.Wagner, C.Hall, N.Ferguson
    - flexible - implication sur sécurité difficile à analyser
- Choix final : Rijndael le 26112001 – standard FIPS PUB 197

- Principes similaires à ceux du DES, plus robuste
  - Avec clé de 128 bit , plus puissant que RC5 de RSA avec clé de 512 bits
  - Suite de 9, 11 ou 13 « rondes » (round) , selon la taille de la clé, associant :
    - **des transpositions**
    - **des substitutions non linéaires**
    - **adaptées à la technologie actuelle utilisable par les coprocesseurs**
- Caractéristiques
  - Clés de 128, 192 ou 256 bits
  - portant sur des blocs de même taille
  - Blocs organisés en tables d'octets:
    - **de 4 colonnes de 4 , 6 ou 8 octets**
  - Les transpositions portent
    - **sur un ligne (rotation)**
    - **sur les colonnes**
  - Les substitutions portent sur les octets et utilisent une table non-linaire , la S-box
  - Opérations : « Ou exclusif » et multiplications dans GF(2^8)
    - **Voir Théorie de l'Information**

- **Standard pour l'AES**
  - Federal Informaryion Processing Standards
  - http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
- **Description de l'algorithme**
  - http://home.ecn.ab.ca/~jsavard/crypto/co040401.htm
  - http://www.uqtr.ca/~delisle/Crypto/prives/blocs_rijndael.php

- la table « State » contient les valeurs successives d'un bloc manipulé par les procédures ci-dessous
- Algorithmes simples basé sur 7 sous-programmes
  - AddRoundKey :
    - « Ou exclusif » entre lignes de la «State » et clé intermédiaire
    - les clés intermédiaires sont des mots de 4 octets générés à partir de la clé K par la procédure d'expansion de clé
      - Cette fonction est sa propre inverse
  - SubBytes : substitution utilisant la S-box
  - ShiftRows : rotation des octets d'une ligne
  - MixColumns : permutation de colonnes
    - Fonctions inverses des précédentes
  - InvSubBytes : substitution utilisant la S-box
  - InvShiftRows : rotation des octets d'une ligne
  - InvMixColumns : permutation de colonnes

- Pour plus de détails voir site
  http://home.ecn.ab.ca/~jsavard/crypto/co040401.htm
- Pseudo-algorithme de chiffrement

```
InvCipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
    byte state[4,Nb]
    state = in
    AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])

    for round = Nr-1 step -1 downto 1
        InvShiftRows(state)
        InvSubBytes(state) AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
        InvMixColumns(state)
    end for

    InvShiftRows(state)
    InvSubBytes(state)
    AddRoundKey(state, w[0, Nb-1])
    out = state
end
```

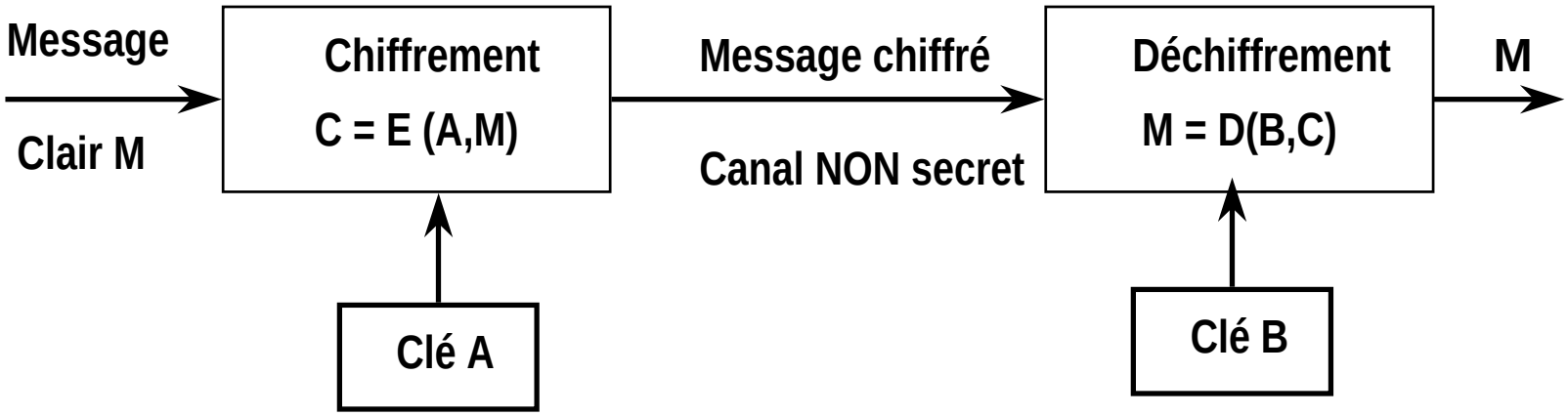
EqInvCipher(byte in[4*Nb], byte out[4*Nb], word dw[Nb*(Nr+1)])

```
begin
byte state[4,Nb]
state = in
AddRoundKey(state, dw[Nr*Nb, (Nr+1)*Nb-1])
for round = Nr-1 step -1 downto 1
        InvSubBytes(state)
        InvShiftRows(state)
        InvMixColumns(state)
        AddRoundKey(state, dw[round*Nb, (round+1)*Nb-1])
end for
InvSubBytes(state)
InvShiftRows(state)
AddRoundKey(state, dw[0, Nb-1])
out = state
End
```

For the Equivalent Inverse Cipher, the following pseudo code is added at the end of the Key Expansion routine :

```
for i = 0 step 1 to (Nr+1)*Nb-1
    dw[i] = w[i]
end for
for round = 1 step 1 to Nr-1
    InvMixColumns(dw[round*Nb, (round+1)*Nb-1])     // note change of type
end for
```

- RSA (Rivest-Shamir-Adleman) est le plus connu ...(1977)
- D'autres codes existent sur des principes voisins



  - L'algorithme E et la clé A sont publiques
  - D et B sont secrets et permettent de décoder le message chiffré C
- Basé sur la décomposition en facteurs premiers de nombres très grands nombres produits de 2 nombres premiers de plus de 100 chiffres ...

Exemple:

p=31, q=47, n=1457
Φ(n)=30*46=1380

E= 889

889*1009modulo1380= 1
D=1009

B=« 11101010 »
B=234

C=234^{889}mod1457
C=892
C=« 1101111100 »

B=892^{1009}mod1457
B=234
B=« 11101010 »

- **Clés**
  - **Chiffrement**
    pet q premiers très grands; n=pq
    Φ(n)= Indicateur d'Euler de N
    nombre aléatoire E, 3 <E<Φ(n)
  - **Déchiffrement**
    D tel que E*D modulo Φ(n) = 1
- **Chiffrement**
  - **Message découpé en blocs B_i**
  - **Codage**

$$C_i = B_i^E \text{ modulo n}$$

- **Déchiffrement**

$$B_i = C_i^D \text{ modulo n}$$

- 1976
- Vulnérable à attaque par personne intermédiaire
- Blocs de taille n (assez grand), taille de la clé
- Code
  - B=[b_1,b_2, ,b_n] clé privée du destinataire — b_i entier naturel aléatoire $b_i > \sum_{j=0}^{i-1} b_j$
  - A=[a_1,a_2, ,a_n] clé publique utilisée par la source — a_i: entier naturel
    - $a_i = b_i * w$ modulo m
    - gâche z = w^{-1} soiy z*w modulo m = 1
  - M=[x1,x2, ,xn] un bloc du message clair — x_i : bit du message (0 ou 1)
- Chiffrement : $C=AM=a_1x_1+a_2x_2+ \ldots +a_nx_n$
- Déchiffrement :
  - on calcule x tel que Bx = C*z modulo m = AM*z modulo m
  - puis algorithme d 'empilement pour i = n jusqu 'à 1

$$\text{si } b_i > C - \sum_{j=i+1}^{n} x_j b_j \text{ alors } x_i = 0 \text{ sinon } x_i = 1$$

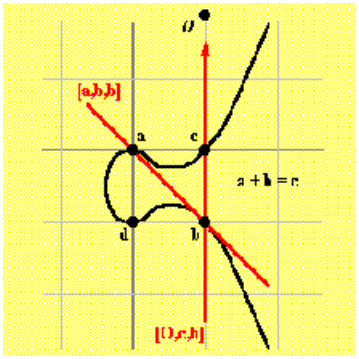
- Exemple
  - w=889 m=1457 B=[3,7,12,23,47,95,189,377] z=1398 tel que 889*1398 modulo 1457=1
  - a_i=889b_i modulo1457 soit A=[1210,395,469,49,987,1406,466,43]

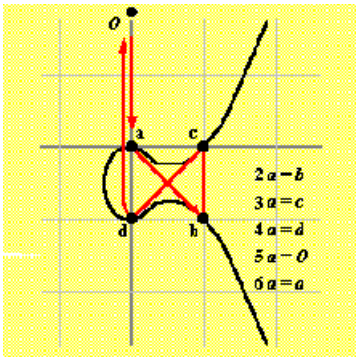
Code Diffie-Hellman : exemple de chiffrement et déchiffrement

- M = 01001101
- Chiffrement
  - C=395+987+1406+43 =2831
- Déchiffrement

- Déchiffrement

exemple :
$y^2 + y = x^3 - x^2$





- Plus rapide et clés plus courtes que RSA
  - ➟ si la fonction elliptique est bien choisie ……
  - ☞ donc plus facile à implanter sur carte à puce
- Fonction du type $y^2 + K\,y = x^3 + A\,x^2 + B$ (modulo p)
  - ☞ p premier très grand
- On s'intéresse aux points de coordonnées entières
  - ☞ certains de ces points forment un groupe
  - ☞ dans espace de p lignes et p colonnes cette courbe contient N points qui forment un groupe elliptique convenable où N est presque égal à p avec N=k*q où k est petit et q premier
  - ☞ exemple : $p = 2^{192} - 2^{64} - 1$
  - ☞ p = 6 277 101 735 386 680 763 835 789 423 207 666 416 083 908 700 390 324 961 279
  - ☞ N = 6 277 101 735 386 680 763 835 789 423 337 720 473 986 773 608 255 189 015 329
- le code est bâti à partir de couples de ces points ?

- En cours d'harmonisation au niveau européen
- pas encore tout à fait libre en France mais en voie de libéralisation complète
- loi 96-659 du 26/7/1996 et décret du 17/3/1999 + arrêté du 17/3/1999
- 2 cas
  - usage ou importation de services ou moyens cryptographiques
    - Voir ci-dessous
  - Fourniture de services et moyens cryptographiques
    - système d 'enregistrement
      - création, import (hors CE), export de fonctions d 'authentification ou de confidentialité à clé courte
    - système d 'autorisation préalable
      - tous les autres cas
      - sauf développement, test, démonstration : prévenir SCSSI 2 semaines à l 'avance

Usage ou importation de services ou moyens cryptographiques

- pour authentification : totalement libre

- pour confidentialité, libre si :
  - clé de moins de 40 bits (décret du 24/2/1998....)
  - clé de 40 à 128 bits pour usage individuel
  - clé de 40 à 128 bits pour usage collectif si
    enregistrée auprès d 'un Tiers de Confiance
  - le fournisseur a une autorisation générale
    - **par exemple groupement bancaire ….**

- SCSSI : service central de la sécurité des systèmes d'information
  - 18 rue du Dr Zamenhof 92131 Issy les Moulineaux
  - tel +33 1 4146 3700 Fax: +33 1 4146 3701
  - http://www.legifrance.gouv.fr/citoyen/officiels.ow

- Attaque : Rechercher le texte clair ou la clé
- Base de départ
  - Texte chiffré seulement
  - Texte clair connu (avec texte chiffré)
  - Texte clair défini
    - chiffrer et comparer à texte chiffrer
  - Texte chiffré défini
    - déchiffrer et comparer à texte clair
  - Clé choisie
    - procéder à de modifications de clés ou des comparaisons entre clés
  - Temps
    - mesure du temps de chiffrement pour avoir informations sur clé ou données
  - Analyse des défauts
    - défauts supposés du système de chiffrement
  - Man-in-the-Middle
    - s'introduire au centre du système par exemple système d 'authentification

- Force brute ou « cassage »
  - cassage si résultat demande moins d'effort que la force brute : essai de toutes les clés
- Livre code
  - apprche classique du cassage de code: rechercher les transformations entre texte clair et texte chiffré
- Cryptoanalyse différentielle
  - corrélations statistiques
- Cryptoanalyse linéaire
  - approximation linéaire des S-Boxes (tables non linéaires) pour trouver clé
- Meet-in-the-middle
  - pour codage à deux niveaux
- plan de clés (Key schedule)
  - choisir clés qui produisent des effets connus à différentes itérations
- Date de naissance
  - paradoxe de la... : recherche de valeurs particulières

- Codage formel
  - Propriétés algébriques
- Correlation
  - Dans un chiffrement au vol, rechercher des corrélations entre séquences, des propriétés statistiques ,....
- Dictionnaire
  - Essayer les clés une par une à partir d'un dictionnaire de mots fréquement utilisés
- Rejouer (Replay)
  - Enregistrer et sauver des messages ou des blocs chiffrés et renvoyer ces blocs quand besoin (exemple : mots de passe chiffrés)

- De nombreuses attaques essayent d 'isoler de petits composants ou des aspects qui peuvent être traités séparément

- Historique
  - Histoire de la cryptologie : http://www.multimania.com/marief/
    - histoire et nombreux liens
  - Petit code des codes secrets J.Laffin Ed. Arts et voyages
- Cryptographie
  - http://www.scssi.gouv.fr/document/chiffre.html
  - http://www.securite.org/db/crypto/
  - http://www.cryptosoft.com/html/privacy.htm
  - http://www.rsa.com/rsalabs/faq/html/sections.html
  - http://www.reapertech.com.it/RSAEuro/RSAEuro/rsaann.html
    - téléchargement de programmes sources
  - http://home.ecn.ab.ca/~jsavard/crypto/jscrypt.htm
- Aspects légaux
  - http://www.scssi.gouv.fr/
- Glossaires, acronymes
  - http://www.io.com/~ritter/GLOSSARY.HTM
  - http://www.cnet.com/Resources/Info/Glossary/num.html
  - http://www.csrstds.com/acro-a-d.html