

undefined@startlos

0-0

Cryptologie à clef secrète

Roland Gillard

Mardi 17 avril 2001

Table des matières

1	Préliminaires	1
1.1	Codage par décalage	1
1.2	Décalage variable : clef	2
1.3	Xor, \mathbb{F}_2	3
2	D.E.S. (Data Encryption Standard)	5

2.1	Description : rondes de Feistel	5
2.2	Modes d'utilisation	7
3	A.E.S (Advanced Encryption Standard)	8
3.1	Le concours	8
3.2	Description de Rijndael	9
4	Principales Attaques sur le DES	11
4.1	Les types d'attaque	11
4.2	Attaques du DES	12
5	Analyse différentielle	13
5.1	Détails sur la fonction f du DES	13
5.2	Analyse différentielle des boîtes S	14
5.3	Application à l'analyse d'une ronde	16
5.4	Application : attaque du DES à 3 rondes	18
5.5	On complique : attaque du DES à 6 rondes	20
6	Analyse linéaire	22

6.1	Le principe	22
6.2	Analyse linéaire des boîtes S	24

7	Références	24-1
----------	-------------------	-------------

1 Préliminaires

1.1 Codage par décalage

On remplace chaque lettre par une autre suivant la table :

A	B	C	D	...	V	W	X	Y	Z
D	E	F	F	...	Y	Z	A	B	C

qui montre un décalage de 3 sur la droite exemple

B O N J O U R A T O U S

↓

E R Q M R X U D W R X V

Ce procédé aurait été utilisé par Jules César ! Le problème est que le décalage est facile à trouver car on connaît les fréquences des lettres dans les textes courants

1.2 Décalage variable : clef

On choisit une clef par exemple 1526 et on décale la première lettre de 1, la deuxième de 5, la troisième de 2, et la quatrième de 6 et on recommence :

B	O	N	J	O	U	R	A	T	O	U	S
1	5	2	6	1	5	2	6	1	5	2	6
C	T	P	P	P	Z	T	G	U	T	W	Y

Cette méthode s'appelle Chiffrement de Vigenère

(Blaise Vigenère a vécu au XVI^e siècle)

1.3 Xor, \mathbb{F}_2

Dans un ordinateur, tout est codé sous forme de 0 ou de 1 (=bit).
On introduit alors l'opération de Xor (ou exclusif) , \oplus , ainsi que la multiplication :

$$\begin{array}{ll} 0 \oplus 0 = 0 & 0.0 = 0 \\ 1 \oplus 0 = 1 & 1.0 = 0 \\ 0 \oplus 1 = 1 & 0.1 = 0 \\ 1 \oplus 1 = 0 & 1.1 = 1 \end{array}$$

$$(x \oplus y) \oplus y = x \oplus (y \oplus y) = x \oplus 0 = x . \quad (1)$$

Propriétés de calculs usuelles :

$\mathbb{F}_2 = \{0, 1\}, \oplus, .$ est un corps.

On peut donc coder un peu comme plus haut une suite de 0 et 1 à l'aide d'une clef K en faisant des Xor chiffre par chiffre . Si $K = 1101$,

à coder	0	1	0	0	0	1	1	0	1	1	0	0	0	1	0
clef K	1	1	0	1	1	1	0	1	1	1	0	1	1	1	0
sortie s	1	0	0	1	1	0	1	1	0	0	0	1	1	0	0

La formule (1) permet de retrouver le message initial :

$K \oplus s$	0	1	0	0	0	1	1	0	1	1	0	0	0	1	0
--------------	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Elle permet aussi une des premières analyses : si on connaît le texte en clair et le codage , on retrouve la clef.

2 D.E.S. (Data Encryption Standard)

Utilisé depuis 1977, il utilise une clef K de 56 bits, clef secrète qui est utilisée aussi bien pour crypter que pour décrypter.

56=8 fois 7 = 8 octets privés du bit de parité.

2.1 Description : rondes de Feistel

Le texte est découpé en blocs de 64 bits. Chacun des blocs est codé ainsi :

1. On fait une permutation IP sur les bits de ce bloc et on le découpe en 2 moitiés G_0 et D_0 .
2. On répète 16 fois (pour $i = 0, \dots, 15$) l'opération suivante, appelée **ronde**, utilisant une sous-variante K_i de K :

$$\boxed{G_i \mid D_i}$$

↓

$$\boxed{G_{i+1} = D_i \mid D_{i+1} = G_i \oplus f(D_i, K_i)}$$

Ici f est une fonction compliquée, construite de façon à masquer la clef K_i . Dans l'autre sens on trouve :

$$D_i = G_{i+1}, G_i = D_{i+1} \oplus f(G_{i+1}, K_i)$$

Le procédé est donc invariant en retournant à la fois le temps (remplacer i par $16 - i$ et la gauche et la droite (échanger G_i et D_i pour tout i).

3. On finit en faisant la permutation inverse IP^{-1} de celle du début.

2.2 Modes d'utilisation

3 critères :

Sécurité, Efficacité, Tolérance aux erreurs.

- ECB : $C_n = E_K(M_n)$ =Electronic Code Book
- CBC : $C_n = E_K(M_n \oplus C_{n-1})$ =Cipher Block Chaining
- CFB : $C_n = M_n \oplus E_K(C_{n-1})$ =Cipher Feedback
- OFB : $C_n = M_n \oplus S_n; S_n = E_K(S_{n-1}), S_0 = IV$
=Output Feedback

3 A.E.S (Advanced Encryption Standard)

3.1 Le concours

appel du NIST : 12 septembre 1997

Admission des candidatures : 15 retenues le 20 aout 1998

Finalistes : MARS, RC6, Rijndael, Serpent, and Twofish

Choix terminal (2 octobre 2000) : Rijndael conçu par 2 belges (Joan Daemen et Vincent Rijmen) you could pronounce it like "Reign Dahl", "Rain Doll", "Rhine Dahl".

cf Le rapport [12].

3.2 Description de Rijndael

Ce procédé utilise 10 répétitions d'un cycle comportant chacune 4 opérations sur le bloc (sauf la dernière qui n'en a que 3) : Le bloc de données est représenté par une matrice d'octets ayant 4 lignes et un nombre de colonnes Nb . Le bloc contient donc $32Nb$ bits.

- ByteSub : Une transformation affine dans l'espace vectoriel de dimension 8 sur \mathbb{F}_2 sur **l'inverse** de la chaîne.
- ShiftRow : Un décalage des lignes après représentation du bloc en tableau rectangulaire.
- MixColumn : Multiplication modulo $x^4 + 1$ par $03X^3 + 01X^2 + 01x + 02$ des colonnes considérées comme des polynômes sur \mathbb{F}_{256} .
- RoundKey addition : Xor par une sous-clef dépendant du numéro du cycle.

\mathbb{F}_{256} : c'est le corps engendré sur \mathbb{F}_2 par une racine x du polynôme irréductible

$$X^8 + X^4 + X^3 + X + 1$$

Un élément s'écrit comme un polynôme de degré 7 ou moins à coefficients 0 ou 1 :

$$x^6 + x^4 + x^2 + x + 1$$

représenté par l'octet :

$$01010111 = 57_x$$

4 Principales Attaques sur le DES

4.1 Les types d'attaque

- Texte chiffré connu : C
- Texte chiffré choisi : $C \Rightarrow M$
- Texte en clair connu : M et C
- Texte en clair choisi : $M \Rightarrow C$
- Texte en clair choisi adaptable

4.2 Attaques du DES

- Attaque exhaustive : Diffie-Hellman(70) ; Wiener (93) ; EFF (98)
- Davies (87), Biham-Binyukov (E94)
- Analyse différentielle : Biham-Shamir (C90)
- Analyse linéaire : Matsui (E93)
- Analyse de la consommation : Kocher ; variante différentielle (Goubin-Patarin)
- Analyse temporelle : Kieme Quisquater
-
-
-

5 Analyse différentielle

5.1 Détails sur la fonction f du DES

$$f(D, K) = P \circ S(E(D) \oplus K)$$

D et $f(D, K)$: 32 bits = 8×4

$E(D)$ et K (variante de la clef utilisée dans la ronde) : 48 bits 8×6

E : permutation expansive

P : permutation

$S = S_1, \dots, S_8$: paquet de 8 boîtes de substitutions : tableau 4 lignes et 16 colonnes qui permet de transformer la chaîne de 6 bits

$$B = b_5 b_4 b_3 b_2 b_1 b_0$$

en l'élément C de la ligne i et de la colonne j :

$$i = b_5 b_0, \quad j = b_4 b_3 b_2 b_1$$

5.2 Analyse différentielle des boîtes S

On considère des couples de chaînes B, B^* ainsi que :

$$B' = B \oplus B^* .$$

On fait de même pour les images par une boîte S_1 par exemple

$$C = S_1(B); C^* = S_1(B^*); C' = C \oplus C^* . \quad (2)$$

On s'intéresse aux xor B' et C' : pour chacune de leur valeur on considère le nombre

$$N_1(B', C')$$

de couples (B, B^*) vérifiant (1) soit encore le nombre d'éléments dans :

$$\Delta_1(B', C') = \{B \in \mathbb{F}_2^6 \mid S_1(B) \oplus S_1(B^*) = C'\} . \quad (3)$$

De même : $N_j(B', C') = \#\Delta_j(B', C')$ pour $S_j, j = 1, \dots, 8$

La valeur moyenne est 4 mais elle est souvent nulle et atteint même 14 pour $j = 1$, $B' = 34$ et $C' = E$ (en hexadécimal).

5.3 Application à l'analyse d'une ronde

$$f(D, K) = P \circ S(E(D) \oplus K)$$

On a les relations linéarité suivantes

$$E(D \oplus D^*) = E(D) \oplus E(D^*) \quad (4)$$

$$(E(D) \oplus K) \oplus (\oplus E(D^*) \oplus K) = E(D) \oplus E(D^*) \quad (5)$$

$$P(C \oplus C^*) = P(C) \oplus P(C^*) \quad (6)$$

$$\text{égalité analogue pour } P^{-1} \quad (7)$$

Rappel : $f(D, K) = P \circ S(E(D) \oplus K)$.

Partant d'un couple (D, D^*) d'images (E, E^*) par l'expansion et posant

$$F = f(D, K); F^* = f(D^*, K^*); C = P^{-1}(F); C^* = P^{-1}(F^*)$$

les xor C' et E' regroupent chacune 8 chaînes C'_j et E'_j et on a :

$$B_j := E_j \oplus K_j \in \Delta_j(E'_j, C'_j)$$

$$K_j \in \text{Test}_j(E_j, E_j^*, C'_j) := E_j \oplus \Delta_j(E'_j, C'_j) \quad (8)$$

5.4 Application : attaque du DES à 3 rondes

C'est une attaque à texte en clair connu.

On néglige IP . on a pour $i = 0, 1, 2$

$$G_{i+1} = D_i ; D_{i+1} = G_i \oplus f(D_i, K_i)$$

$$D_3 = G_2 \oplus f(D_2, K_3) \quad (9)$$

$$= D_1 \oplus f(D_2, K_3) \quad (10)$$

$$= G_0 \oplus f(D_0, K_1) \oplus f(D_2, K_3) \quad (11)$$

Idem avec (G_0^*, D_0^*) ; xorons les 2 égalités :

$$D'_3 = G'_0 \oplus f(D_0, K_1) \oplus f(D_0^*, K_1) \oplus f(D_2, K_3) \oplus f(D_2^*, K_3)$$

Si on choisit $D_0 = D_0^*$ ceci se simplifie en

$$D'_3 = G'_0 \oplus f(D_2, K_3) \oplus f(D_2^*, K_3)$$

$$f(D_2, K_3) \oplus f(D_2^*, K_3) = G'_0 \oplus D'_3$$

Si on observe qu'on connaît G'_0 et D'_3 , on pose :

$$C' = P^{-1}(G'_0 \oplus D'_3); E = E(G_3); E^* = E(G_3^*) \quad (12)$$

et on découpe tout le monde en 8 morceaux. Alors, comme dans (8) :

$$K_j \in \text{Test}_j(E_j, E_j^*, C'_j) \text{ pour } j = 1, \dots, 8 \quad (13)$$

On peut ainsi déterminer 48 des 56 bits de la clef K avec 3 paires de textes en clair (et les 3 paires de textes chiffrés associés) On obtient les 8 qui restent par une recherche exhaustive peu coûteuse.

5.5 On complique : attaque du DES à 6 rondes

Le principe s'inspire du cas précédent : attaquer la sous clef de la dernière ronde. Dans (13) on disposait des données issues directement des messages en clairs ou de leur codage, cf (12).

Lorsqu'il y a plus de rondes, ce n'est plus possible. On se débrouille en choisissant bien le message initial de façon à récupérer par la suite des (G'_i, D'_i) de sortie statistique élevée lorsque le choix des clefs varie. C'est la notion de **caractéristique**.

Une paire de données est dite **bonne** si elle donne une suite de (G'_i, D'_i) qui est celle décrite dans la caractéristique considérée, et **mauvaise** sinon. Les bonnes paires donnent des résultats prévus en proportion assez importante du nombre de paires de données (par exemple 1/6). Les mauvaises s'éparpillent suivant le grand nombre de clefs possibles. On utilise donc les ensembles

$$\text{Test}_j(E_j, E_j^*, C'_j)$$

comme dans (13) pour faire des statistiques des clefs suggérées. Sur 6 rondes, une caractéristique permet l'attaque de 30 bits de la clef : comparer 1/6 à 2^{-30} . Il faut d'autant plus de paires de messages que la probabilité globale de la caractéristique est petite. On peut supprimer les paires de données conduisant à des $\text{Test}_j(E_j, E_j^*, C'_j)$ vides.

6 Analyse linéaire

Cette attaque du DES a été introduite par Matsui (E93)

6.1 Le principe

Pour A une chaîne de bits, on note $A[i]$ le i^{e} bit.

$$A[i_1, i_2, \dots, i_n] = A[i_1] \oplus A[i_2] \oplus \dots \oplus A[i_n]$$

on recherche des relations linéaires du type

$$M[i_1, i_2, \dots, i_a] \oplus C[j_1, j_2, \dots, j_b] = K[k_1, k_2, \dots, k_c] \quad (14)$$

La proportion p de messages en clair vérifiant cette relation (14) devrait être $\frac{1}{2}$.

L'efficacité de la relation (14) est $|p - \frac{1}{2}|$. On recherche des relations d'efficacité maximale.

Si on part de N textes en clair M et que T d'entre eux donnent 0 pour $M[i_1, i_2, \dots, i_a] \oplus C[j_1, j_2, \dots, j_b]$, la valeur suggérée pour $K[k_1, k_2, \dots, k_c]$ est donnée par le tableau suivant :

	si $T > N/2$	si $T < N/2$
si $p > 1/2$	0	1
si $p < 1/2$	1	0

6.2 Analyse linéaire des boîtes S

Chaque boîte transforme 6 bits en 4 bits.

Pour $0 \leq \beta < 64$, écrit en base 2 : $\beta = b_5b_4b_3b_2b_1b_0$ On pose

$$B[\beta] = \bigoplus B[b_i], \oplus \text{ sur les } b_i \text{ égaux à } 1 .$$

Idem pour la sortie C et γ entre 0 et 15. Matsui calcule le tableau des quantités

$$NS_i(\beta, \gamma) = \#\{B, 0 \leq x < 64 \mid B[\beta] = S_i(B)[\gamma]\}$$

Ce nombre devrait idéalement toujours être 32. C'est loin d'être le cas :

$$NS_5(16, 15) = 12$$

Ce qui en tenant compte de E et P donne l'exemple de (14) :

$$B[15] \oplus f(B, K)[7, 18, 24, 29] = K[22] \text{ avec } p = 12/64 .$$

7 Références

Livres :

[1] D. Stinson : Cryptographie, théorie et pratique, . Int. Thomson Pub France 1996.

[2] B. Schneier : Cryptographie appliquée, Int. Thomson Pub France 1997

[3] EFF : Cracking D.E.S. O' Reilly 1998.

Articles de vulgarisation :

[4] F. Leprévost : Gazette des mathématiciens N° 85 pp. 9-23 : Les standards cryptographiques du XXI ième siècle, F. Leprévost

[5] S Landau : Notices AMS N° 47-3, p. 341-349, Data Encryption Standard,

[6] S Landau : Notices AMS N° 47-4, p.450-459 Advanced Encrytion Standard,

Articles :

[7] Bellovin Wagner : a programmable plaintext recognizer, 1994
<http://www.research.att.com/~smb>

[8] Biham, Shamir : C90, 1-21

[9] Matsui : E93, 386-397

[10] Nyberg : E93, 55-64

[11] Lai, Massey, Murphy : E91, 17-38

(E91= Adv. in Cryptology, Eurocrypt '91, Lecture Notes in Computer Sciences, Springer et

C90=Adv. in Cryptology, Crypto '90, Lecture Notes in Computer Sciences, Springer)

Liens Internet :

[12] <http://csrc.nist.gov/encryption/aes/round2/r2report.pdf>

[13] A.E.S : <http://csrc.nist.gov/encryption/aes/>

[14] Rijndael : <http://www.esat.kuleuven.ac.be/~rijmen/rijndael/>

[15] Biblio générale : <http://www.counterpane.com/biblio/>