Université Paris 6
Master d'Informatique – STL

Crypto
L. Perret – G. Renault
Année 2009-2010

TD/TME Crypto

Exercice 1 (S-Box du DES)
On donne ci-dessous la table de la dernière S-box S_8 du DES.

- Calculer $S_8(000000), S_8(010111), S_8(110101), S_8(111101), S_8(111111)$, et $S_8(101010)$.

S_8															
13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Exercice 2 (Schéma de Feistel)
Un schéma de Feistel fonctionne de la manière suivante. On se donne une fonction F de n bits vers n bits et un message $x = x_1||x_2$ de $2n$ bits ($x_1,\ x_2\ \in \{0,1\}^n$). Ensuite, on définit :

$$G(x, K) = y,$$

où $K \in \{0,1\}^n$ et $y = y_1 \| y_2$, avec $y_1,\ y_2\ \in \{0,1\}^n$ tels que

$$\begin{cases} y_1 &= x_2 \\ y_2 &= x_1 \oplus F(x_2, K). \end{cases}$$

1. Représenter schématiquement cette fonction.
2. Comment retrouve-t-on x_1, x_2 à partir de y_1, y_2 ? Représenter schématiquement cette opération.
3. Une méthode classique pour construire un chiffrement par blocs consiste à "concaténer" plusieurs tours de Feistel.
   - Représenter schématiquement un tel chiffrement avec 4 tours.
   - Donner le schéma du déchiffrement.

Exercice 3 (Dérivation des sous-clefs du DES)
Nous décrivons rapidement la méthode permettant de construire les sous-clefs du DES à partir d'une clef K de 64 bits. Les bits 8, 16, ..., 64 de K servent à la détection des erreurs (pour chacun des 8 octets, le dernier bit de l'octet détecte une erreur dans les 7 autres bits). Ces bits n'entrent pas dans le calcul des sous-clefs, et ne sont donc pas pris en compte. On permute d'abord selon une permutation PC − 1 définie par :

PC − 1						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	44

– Calculer PC-1($00\cdots00$), et PC-1($00\cdots10000001$).

Les 28 premiers bits du résultat sont notés C_0, les 28 derniers D_0. A chaque tour i, $1 \leq i \leq 16$, on calcule :

$$C_i = rol_{\alpha_i}(C_{i-1}),\ D_i = rol_{\alpha_i}(D_{i-1}),$$

où rol_{α_i} désigne un décalage circulaire à gauche de 1 ou 2 bits selon le numéro du tour. Les valeurs du décalage selon le numéro du tour sont :

tour	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
α_i	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

– Calculer $rol_{\alpha_2}(00\cdots00)$, et $rol_{\alpha_2}(10\cdots00)$.

Finalement, la sous-clef K_i est obtenue par :

$$K_i = \mathrm{PC}-2(C_iD_i),$$

où (C_iD_i) indique la concaténation de C_i et D_i, et $\mathrm{PC}-2$ est une permutation de 48 des 56 bits de (C_iD_i) :

PC − 2							
14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

– Donner le nombre de bits à 0 et 1 dans $\mathrm{PC}-2(00\cdots00)$ et $\mathrm{PC}-2(10\cdots00)$.

Exercice 4 (Complémentation)

Soient x un mot binaire et $\overline{x}$ le complément bit-à-bit de x. L'objectif de l'exercice est de montrer que :

$$\mathrm{DES}_k(m) = \mathrm{DES}_{\overline{k}}(\overline{m}).$$

Nous allons prouver la propriété sur un tour.

– Soit $\overline{k}$ la clef maître, monter que la première sous-clef dérivée est $\overline{k_1}$ (avec k_1 la sous-clef dérivée de k).

Montrer que :

$$\overline{x} \oplus \overline{y} = x \oplus y \text{ et } \overline{x \oplus y} = \bar{x} \oplus y.$$

Utiliser ces résultats pour prouver :

$$(\overline{L_0}, \overline{R_0}) \overset{\overline{k_1}}{\to} (\overline{L_1}, \overline{R_1}).$$

TME – Les propriétés des boîtes S

Nous mentionnons ici les principaux critères :

1. Chaque ligne de chaque boîte est une permutation des entiers de 0 à 15.
2. Aucune boîte n'est une fonction linéaire ou affine de ses entrées : c'est là que réside la non-linéarité du DES.
3. La modification d'un bit en entrée entraîne la modification d'au moins deux bits en sortie.
4. Pour tout $x \in \mathbb{F}_2^6$, $S(x)$ et $S(x \oplus 001100)$ diffèrent d'au moins deux bits (ou encore : si deux entrées diffèrent seulement sur leur deux bits du milieu, leurs sorties diffèrent sur au moins deux bits).
5. Pour $x \in \mathbb{F}_2^6$, et $i, j \in \{0,1\}$, $S(x) \neq S(x \oplus 11ij00)$ (si deux entrées diffèrent sur leur deux premiers bits, et sont identiques sur leur deux derniers bits, alors leur sorties diffèrent d'au moins un bit).
6. Si l'on fixe un bit de l'entrée de S, et que l'on regarde un bit fixé de la sortie, le nombre d'entrées pour lesquelles le bit de sortie prendra la valeur 0 est "proche" du nombre d'entrées pour lesquelles ce bit sera égal à 1 (i.e. proche de 16).

L'objectif du TME est de tester ces propriétés en utilisant MAPLE. On vous demande donc :

- Écrire une fonction **is_linear** permettant de tester si une S-boîte est une fonction linéaire de ses entrées. Pour cela, vous utiliserez le test suivant : si pour $x, y \in \mathbb{F}_2^6$, $S(x+y) \neq S(x)+S(y)$, alors nous pouvons déduire que S n'est pas une fonction linéaire.
- Écrire les fonction **is_avalanche**, **diff1**, **diff2** permettant de tester 3., 4. et 5.
- Écrire la fonction **is_uniforme** permettant de tester 6.

Vous testerez vos fonctions sur les boîtes S du DES donnés sur la page suivante.

S_1															
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2															
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3															
10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4															
7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5															
2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6															
12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7															
4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8															
13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11