Master CSI 2 2017-2018

Cryptanalyse — M1MA9W06

Responsable : G. Castagnos

Projet sur la cryptanalyse du DES

À faire en binôme ou en trinôme. Vos programmes clairs et bien commentés ainsi qu'un rapport contenant les réponses aux questions (démonstrations, explications du code Sage) sont à rendre avant le vendredi 8 décembre 23 :59 par mail à

guilhem.castagnos@math.u-bordeaux.fr

Le projet consiste en une cryptanalyse d'une version à 8 tours du DES en combinant des idées des cryptanalyses linéaires et différentielles.

Dans tout le projet, si X et Y sont deux chaînes binaires, X||Y désigne leur concaténation. Si X est une chaîne de n bits, on note $X[i] \in \{0,1\}$ le bit de X d'indice i, en numérotant de 0 à $n-1$ et de gauche à droite, c'est à dire que $X = X[0]||X[1]|| \dots ||X[n-1]$.

On considère la variante suivante du DES à 8 tours, notée DES-8 :

- On utilise la fonction de tour $f(X,K)$ du DES prenant en entrée un bloc X de 32 bits et une clef de tour K de 48 bits et ressortant un bloc de 32 bits. Vous pouvez trouver une description complète de cette fonction de tour ici (à partir de la page 13) :

  http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

  Attention : contrairement aux notations du projet, dans ce document du NIST les bits d'une chaîne de longueur n sont numérotés de 1 à n et non de 0 à $n-1$!

- Les messages clairs m sont de 64 bits. Ils sont chiffrés par 8 tours de schéma de Feistel : On note $m = L_0||R_0$ avec L_0 et R_0 de 32 bits, puis pour $i \in \{1, \dots 8\}$,

  $$L_i = R_{i-1}, \qquad R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

  Le chiffré est $c = R_8||L_8$. On n'utilise pas les permutations initiale et finale du DES.

- La clef de chiffrement sk est de 64 bits. Les clefs de tours de 48 bits, $K_1, \dots, K_8$, sont obtenues en appliquant les 8 premiers tours de l'algorithme de cadencement de clefs du DES à la clef sk. Cet algorithme de cadencement est décrit Annexe 1 du précédement document à partir de la page 19.

1 Programmer (avec Sage) le chiffrement de cette variante DES-8. Il sera utile pour la suite de diviser le code en plusieurs fonctions (fonctions de tours, cadencement des clefs, applications des boîtes S...). Vos fonctions doivent manipuler des entrées sorties sous forme de listes de bits (éléments de `GF(2)` ou entiers 0 et 1). Vous pouvez tester vos fonctions à l'aide du fichier suivant :

`https://www.math.u-bordeaux.fr/~gcastagn/Cryptanalyse/test_vectors.sage`

2 On note S_5 la cinquième boîte S du DES. Calculer la matrice des approximations linéaires de cette boîte S_5 du DES, c'est à dire la matrice de taille $2^6 \times 2^4$ contenant à l'entrée α, β le nombre

$$L[\alpha, \beta] = Card\{x \in \mathbf{F}_2^6, \langle \alpha, x \rangle + \langle \beta, S_5(x) \rangle = 0\}$$

où l'on identifie $\alpha \in \mathbf{F}_2^6$ et $\beta \in \mathbf{F}_2^4$ avec les entiers de 0 à 63 et de 0 à 15 pour les indices de ligne et de colonne de la matrice, via leur écriture en binaire avec bits de poids faible à droite.

3 Soit K une clef de tours de 48 bits fixée. Soit X une chaîne de 32 bits aléatoire, uniformément distribuée. On note $Y = f(X, K)$ où f désigne la fonction de tour du DES. Montrer quelle est la probabilité d'avoir $X[16] = Y[2] \oplus Y[7] \oplus Y[13] \oplus Y[24]$.

Vérifier expérimentalement cette probabilité avec Sage (se donner une clef de tour et tester avec un grand nombre de X aléatoires).

4 On considère les 3 premiers tours du DES-8, avec une clef *sk* fixée et pour une entrée $m = L_0 \| R_0$ uniformément distribuée parmi les chaînes de 64 bits. Montrer quelle est la probabilité d'avoir l'équation suivante :

$$L_0[2] \oplus L_0[7] \oplus L_0[13] \oplus L_0[24] \oplus R_0[16] \oplus R_3[2] \oplus R_3[7] \oplus R_3[13] \oplus R_3[24] \oplus L_3[16] = 0.$$

Dans les 3 questions suivantes (5, 6 et 7), on considère le chiffrement par DES-8 avec la même clef secrète K, d'un message clair m et d'un message clair $m^\star$. On note (L_i, R_i) pour $i = 0, \dots, 8$ les valeurs intermédiaires prises lors du chiffrement de m et $(L_i^\star, R_i^\star)$ pour $i = 0, \dots, 8$ les valeurs prises lors du chiffrement de $m^\star$. On note c et $c^\star$ les chiffrés par DES-8, c'est à dire $c = R_8 \| L_8$ et $c^\star = R_8^\star \| L_8^\star$.

On suppose qu'à l'entrée du second tour, les valeurs prises lors du chiffrement de m et de celui de $m^\star$ différent seulement au niveau des indices 1 et/ou 2, c'est à dire que

$$R_1 = R_1^\star \text{ et } L_1 \neq L_1^\star \text{ et } L_1 \oplus L_1^\star = 0\alpha\beta 0000000000000000000000000000 \text{ avec } \alpha, \beta \in \{0, 1\}. \quad (1)$$

5 Sur quels indices L_4 et $L_4^\star$ ne différent pas ? Même question avec R_4 et $R_4^\star$.

6 Quelle est la probabilité d'avoir l'équation suivante ?

$$R_7[2] \oplus R_7[7] \oplus R_7[13] \oplus R_7[24] \oplus L_7[16] \oplus R_7^\star[2] \oplus R_7^\star[7] \oplus R_7^\star[13] \oplus R_7^\star[24] \oplus L_7^\star[16] = 0.$$

Vérifier expérimentalement cette probabilité avec Sage : se donner une clef secrète K, prendre un grand nombre de messages clairs m aléatoires, et pour chaque message m considérer une exécution normale du chiffrement de m et une exécution où l'on modifie la valeur de L_1 au niveau des indices 1 et/ou 2.

7 On suppose avoir à disposition un grand nombre de couples de messages chiffrés $(c, c^\star)$ correspondant aux chiffrements de clairs $(m, m^\star)$ tels que lors des deux chiffrements, on ait la différence donnée à l'équation (1) à l'entrée du second tour. On suppose de plus que tous ces chiffrements ont été fait avec la même clef secrète. Montrer comment récupérer 6 bits de la clef du dernier tour, K_8. Application : récupérer dans le fichier suivant une telle liste de 2000 couples $(c, c^\star)$ et en déduire ces 6 bits de la clef K_8 utilisée.

`https://www.math.u-bordeaux.fr/~gcastagn/Cryptanalyse/question7.sage`

8 Soit m un message clair connu. On note $\mathscr{M}$ l'ensemble des 64 messages clairs obtenus en faisant varier les bits d'indices $8, 16, 22, 30, 33, 34$ de m. On suppose connus l'ensemble des 64 chiffrés par DES-8 des éléments de $\mathscr{M}$, avec une même clef secrète. Montrer que connaissant seulement 6 bits de la clef K_1 du premier tour, il est possible de construire une liste de couples de chiffrés de la forme $(c, c^\star)$ comme à la question précédente, c'est à dire, tels que lors des deux chiffrements menant à c et $c^\star$, on ait la différence donnée à l'équation (1) à l'entrée du second tour.

Application : avec Sage, se donner un tel ensemble $\mathscr{M}$ et les chiffrés correspondants pour une clef secrète de votre choix. Ensuite, construire une telle liste de chiffrés $(c, c^\star)$.

9 En déduire une attaque à messages clairs choisis permettant de trouver 6 bits de K_1 et 6 bits de K_8. Application : programmer cette attaque avec Sage pour une clef secrète de votre choix. De combien de messages clairs choisis avez-vous besoin ?

10 Proposer des idées pour trouver d'autres bits de clef.