Calcul sécurisé – Contrôle continu

Université Paris-Saclay – M1 Informatique / M1 MINT

26 février 2019

1 Introduction

Le sujet porte sur l'étude précise d'une attaque par fautes sur l'algorithme DES (cf Feuille d'exercices numéro 2, exercice 3).

2 Énoncé

Question 1 (*Attaque par faute sur le DES*)
Décrire le plus précisément que vous pouvez le principe d'une attaque par fautes contre le DES. On supposera que l'attaquant est capable d'effectuer une faute sur la valeur de sortie R_{15} du $15^{\text{ème}}$ tour.

Question 2 (*Application concrète*)
Dans le fichier `enonce-cc.txt` chacun(e) d'entre vous trouvera un exemple correspondant à l'exécution du DES sur un message clair :

- une première fois sans injection de faute, ce qui donne donc le chiffré juste ;
- puis 32 fois avec diverses injections de fautes, qui donnent donc 32 chiffrés faux ;

Ces 33 exécutions utilisent bien sûr le même message clair en entrée, et la même clé. En revanche pour chaque étudiant, il s'agit d'une clé différente.

Le but de la question est pour chacun(e) d'entre vous, de retrouver la clé qui lui a été assignée.

1. Décrire précisément ce que vous faites pour retrouver la clé.
2. Donnez les 48 bits de clé que vous obtenez grâce à cette attaque par fautes.

Question 3 (*Retrouver la clé complète du DES*)
Dans la question précédente, on obtient 48 bits de la clé (qui fait au total 56 bits).

1. Expliquer comment on peut retrouver les 8 bits manquants.
2. Faites-le, et donner ainsi la valeur complète de la clé qui vous a été assignée.

Remarque: Vous fournirez la clé sous forme de 8 octets en hexadécimal, chaque octet contenant 7 bits de clé et un "bit de parité" (le bit de poids faible).

Exemple: Supposons que les 56 bits trouvés soient

00101101011001111010110011101101101111001000101101000110

On les considère comme 8 blocs de 7 bits

0010110 1011001 1110101 1001110 1101101 1110010 0010110 1000110

On complète alors chaque bloc de 7 bits par un bit de parité (de façon à ce qu'à chaque fois le bloc de 8 bits obtenu contienne un nombre impair de "1") :

- 0010110 est complété par 0, ce qui donne 00101100 (3 bits "1")
- 1011001 est complété par 1, ce qui donne 10110011 (5 bits "1")
- ...

On obtient finalement

00101100 10110011 11101010 10011101 11011010 11100101 00101100 10001100

Soit, en hexadécimal :

$$2C\ B3\ EA\ 9D\ DA\ E5\ 2C\ 8C$$

Voir le document de référence qui spécifie le DES:
`http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf`
page 1 :

> A DES key consists of 64 binary digits ("0"s or "1"s) of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, may be used for error detection. The 8 error detecting bits are set to make the parity of each 8-bit byte of the key odd, i.e., there is an odd number of "1"s in each 8-bit byte.

Question 4 (plus difficile) (*Fautes sur les tours précédents*)
Les questions précédentes supposaient que l'attaquant provoquait une faute sur la valeur de sortie R_{15} du $15^{\text{ème}}$ tour. Décrivez le plus précisément possible le fonctionnement d'une attaque en supposant cette fois que la faute est provoquée sur la valeur de sortie R_{14} du $14^{\text{ème}}$ tour. Même question si la faute est provoquée sur la valeur de sortie R_{13} du $13^{\text{ème}}$ tour. Et ainsi de suite. Estimez à chaque fois la complexité de l'attaque. Jusqu'à quel tour l'attaque est-elle réaliste ?

Question 5 (*Contre-mesures*)
Imaginer une ou plusieurs contre-mesures contre ce type d'attaque par fautes sur le DES. Décrivez la(les) le plus précisément possible et analysez l'impact sur le temps de calcul (par rapport à une implémentation non sécurisée).

3 Que faut-il faire, et pour quand ?

Les réponses aux questions (y compris la valeur si possible complète de la clé) seront rédigées, le plus clairement possible dans un fichier (Word, PDF, ...) que vous m'enverrez par mail (`Louis.Goubin@uvsq.fr`), **au plus tard le lundi 25 mars 2019 à 23h59**.

4 Documentation utile

4.1 Fichiers utiles

Vous trouverez sur l'espace "Calcul sécurisé" d'e-campus :

- `Sujet_controle-continu.pdf` : le présent sujet.
- `enonce-cc.txt` : contient, pour chaque étudiant(e), le message clair, le chiffré juste et les 32 chiffrés faux.
- `DES.pdf` : contient une description détaillée de l'algorithme DES.

4.2 URL utile

`http://www.emvlab.org/descalc/`
Cette page web contient une "calculette DES", qui vous permet d'obtenir le message chiffré à partir d'un message clair et d'une clé de votre choix.