M1 informatique **2023-2024**

Examen de réseau et sécurité (première session)

Consignes : documents interdits (sauf dictionnaire papier), équipements électroniques interdits (téléphones portables, calculatrices, etc.)

Exercice 1 : Cryptanalyse différentielle de DES (5 points)

La figure 1 représente la S-box S_5 de DES. Pour rappel, $S_5(110110)=5_{10}$ car l'entrée 110110 correspond à la ligne 1----0 et à la colonne -1011-.

S_5	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
01	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
10	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

Figure 1 : La S-box S_5 de DES.

Nous allons essayer de cryptanalyser S_5. Pour cela, nous générons deux messages M_1 et M_2 tels que $I_1+I_2=000011$ (l'opérateur + représentant le XOR). Nous observons que $O_1+O_2=0010$ (l'opérateur + représentant à nouveau le XOR).

Question 1.1 (1 point) : Combien de valeurs de I_1 sont possibles ?

Question 1.2 (3 points) : Nous allons nous limiter aux valeurs de I_1 telles que $I_1<8$. Complétez le tableau 1.

Question 1.3 (1 point) : En considérant que la répartition des couples valides parmi ces 8 valeurs étudiées pour I_1 est représentative de la répartition des couples valides pour toutes les valeurs de I_1, est-ce que cette approche vous a permis de réduire l'espace des clés possibles ? De combien ?

I_1	I_2	O_1	O_2	O_1+O_2	(I_1, I_2) valide ?
000000					
000001					
000010					
000011					
000100					
000101					
000110					
000111					

Tableau 1 : tableau de cryptanalyse de la S-box S_5 de DES.

Exercice 2 : Attaque de broadcast sur RSA (9 points)

Cet exercice se concentre sur une attaque de RSA inventée par J. Hastad [1]. Supposons qu'Alice envoie un message *M*, chiffré avec RSA, à plusieurs destinataires : Bob, Bobby, Benoît, Bertrand, etc. Nous nommerons ces destinataires B_1, B_2, ..., B_k. Chaque

destinataire B_i possède sa propre clé publique (N_i, e_i). Nous faisons l'hypothèse que l'attaquant peut obtenir le message chiffré transmis à chacun des destinataires.

Question 2.1 (1 point) : Montrez que s'il existe $i \neq j$ tel que $gcd(N_i, N_j) \neq 1$, alors l'attaquent peut trouver M. Rappelons que la fonction *gcd* représente le plus grand diviseur commun entre deux entiers : par exemple, $gcd(20, 15) = 5$.

Question 2.2 (1 point) : Déduisez de la question précédente que si les N_i ne sont pas deux à deux premiers entre eux, alors l'attaquent peut trouver M.

Dans la suite, nous étudions le cas où tous les N_i sont deux à deux premiers entre eux. Nous faisons aussi l'hypothèse que $e_i = 3$ pour tout i.

Question 2.3 (1 point) : Est-ce que l'hypothèse d'un e_i commun à tous les B_i est réaliste pour RSA ? Pourquoi ?

Question 2.4 (1 point) : En utilisant le théorème des restes chinois, montrez que l'attaquent peut calculer $M^3 [N_1 \times N_2 \times \ldots \times N_k]$ si $k \geq 3$. Pour rappel, le théorème des restes chinois indique qu'étant donné k entiers $n_1, n_2, \ldots, n_k$ deux à deux premiers entre eux, alors pour toute séquence $a_1, a_2, \ldots, a_k$, il est possible de déterminer efficacement l'unique entier x modulo $n_1 \times n_2 \times \ldots \times n_k$ tel que $x \equiv a_1 [n_1]$, $x \equiv a_2 [n_2]$, ..., $x \equiv a_k [n_k]$.

Question 2.5 (1 point) : Avec RSA, il n'est pas possible de chiffrer des messages plus grands que le modulo N_i d'une clé. Pourquoi ?

Question 2.6 (1 point) : Déduisez des deux questions précédentes le fait que l'attaquant peut calculer M^3 (sans modulo).

Question 2.7 (1 point) : Déduisez de la question précédente le fait que l'attaquant peut calculer M si $k \geq 3$.

Question 2.8 (1 point) : Proposez une manière d'éviter cette attaque.

Question 2.9 (1 point) : Proposez une autre manière d'éviter cette attaque.

[1] J. Hastad. *Solving simultaneous modular equations of low degree*. SIAM Journal of computing, 17:336—341, 1988.

Exercice 3 : Fonctions de hachage (6 points)

Question 3.1 (1 point) : Donnez deux exemples d'utilisation des fonctions de hachage en sécurité informatique.

Question 3.2 (1 point) : Le paradoxe des dates anniversaire indique que la probabilité que deux personnes d'un groupe aient leur anniversaire le même jour dépasse 50% si la taille du groupe est de 23 personnes ou plus. Expliquez en quoi il s'agit d'un paradoxe (sans expliquer la probabilité).

Question 3.3 (1 point) : Considérons un groupe de 23 personnes ou plus. Est-ce que la probabilité qu'au moins une de ces personnes ait son anniversaire aujourd'hui dépasse 50% ?

Question 3.4 (1 point) : Expliquez pourquoi la probabilité de la question 3.2 dépasse 50%.

Question 3.5 (1 point) : Est-ce qu'il est possible de concevoir une fonction de hachage qui a moins de 50% chances de produire une collision avec des hashs représentés sur 8 bits (donc sur 256 valeurs, en considérant que $265 \approx 365$) ?

Question 3.6 (1 point) : Quelle est la conséquence de la question 3.5 sur les fonctions de hachage utilisées en sécurité informatique ?