**M1 - Réseau et sécurité**
**Année universitaire :** 2017-2018
**Durée :** 2h
**Consignes :** Documents interdits. Calculatrices interdits.

# Examen de réseau et sécurité

## Exercice 1 – TCP (10 points)

**Question 1.1 (1 point) :** Rappelez la différence entre TCP et UDP.
**Question 1.2 (1 point) :** Rappelez pourquoi TCP retransmet certains paquets.
**Question 1.3 (1 point) :** Rappelez quand TCP retransmet certains paquets.

Dans TCP, la retransmission est faite après un certain délai qui dépend du temps d'aller-retour (RTT, pour *round trip-time*) entre l'émetteur et le récepteur. Le RTT est estimé en utilisant les paquets ACK de TCP.

**Question 1.4 (1 point) :** Que se passe-t'il si les paquets sont retransmis trop lentement (c'est-à-dire, si le RTT estimé est très supérieur au RTT réel) ?
**Question 1.5 (1 point) :** Que se passe-t'il si les paquets sont retransmis trop vite (c'est-à-dire, si le RTT estimé est très inférieur au RTT réel) ?

Le RTT est calculé comme le temps de réception d'un acquittement moins le temps d'émission du paquet correspondant.

**Question 1.6 (1 point) :** Expliquez pourquoi ce calcul du RTT peut être ambigu pour les ACK correspondant à des paquets retransmis.

L'algorithme de Karn, implémenté dans TCP, utilise deux mécanismes. Le premier mécanisme consiste à ignorer les ACK ambigus pour calculer le RTT.

**Question 1.7 (2 points) :** Supposons que le RTT d'une connexion TCP augmente brutalement. Quelle est la conséquence de cette augmentation, quand le premier mécanisme de l'algorithme de Karn est utilisé ? Pour répondre, vous étudierez les paquets envoyés par l'émetteur, les ACK retournés par le récepteur, et l'estimation du RTT.

Le deuxième mécanisme de l'algorithme de Karn définit une variable, appelée RTO (pour *retransmission timeout*), qui sert à quantifier le délai minimum avant la retransmission d'un paquet. Le RTO est initialisé à une valeur arbitraire. À chaque retransmission, le RTO est doublé.

**Question 1.8 (1 point) :** Supposons (à nouveau) que le délai sur une communication TCP augmente brutalement. Quelle est la conséquence de cette augmentation quand les deux mécanismes de l'algorithme de Karn sont utilisés ?
**Question 1.9 (1 point) :** Quand faut-il réinitialiser le RTO à sa valeur initiale ?

## Exercice 2 – 3-DES (5 points)

L'algorithme 3-DES est un algorithme se basant sur DES qui est plus robuste aux attaques. L'algorithme 3-DES consiste à chiffrer un message en appliquant trois fois successivement l'algorithme DES. Si $f(M, k)$ désigne le chiffrement de $M$ par DES avec la clé $k$, alors l'algorithme 3-DES consiste à calculer $f(f(f(M, k_1), k_2), k_3)$.

**Question 2.1 (1 point) :** Quelle est la taille d'une clé 3-DES ? Quelle est la complexité pour casser 3-DES en force brute ?
**Question 2.2 (1 point) :** Quelle est la complexité pour casser 3-DES avec la technique meet-in-the-middle ? Vous utiliserez un dessin pour justifier votre réponse.

Comme la complexité pour casser 3-DES (cf question 3.2) est inférieure à la taille de clé de 3-DES (cf question 3.1), des chercheurs ont proposé de réduire la taille de la clé de 3-DES, ce qui évite un faux sentiment de protection. Ils proposent que parmi les trois clés $k_1$, $k_2$ et $k_3$, deux clés soient identiques.

**Question 2.3 (1.5 points) :** Montrez que si $k_1=k_2$ (ou $k_2=k_3$), alors l'algorithme 3-DES se casse facilement.
**Question 2.4 (1.5 points) :** Montrez que si $k_1=k_3$ ($k_2$ étant différente), alors la complexité pour casser l'algorithme 3-DES est égale à la taille de la clé de 3-DES.

## Exercice 3 – Cryptanalyse différentielle (5 points)

La figure 1 représente la S-box S5 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 S5 de DES.

**Question 3.1 (1 point) :** Quelle est la valeur de $S_5(100101)$, en décimal ?
**Question 3.2 (3 points) :** Nous allons maintenant essayer de cryptanalyser S5. Pour cela, nous générons deux messages $M_1$ et $M_2$, tels que $I_1 \oplus I_2 = 100000$. Nous observons que $O_1 \oplus O_2 = 1111$. Quels sont les couples $(I_1, I_2)$ valides ? Pour répondre à la question, utilisez la table de la figure 2 (il n'est pas nécessaire de remplir toutes les cases, typiquement pour $I_2$ ou parfois pour $O_1 \oplus O_2$).
**Question 3.3 (1 point) :** Déduisez-en les clés possibles, sachant que $E_1=110100$ ? Rappelons que $I_1=E_1 \oplus K$.

**Nom :** **Prénom :**

| $I_1$ | $I_2$ | $O_1$ | $O_2$ | $O_1 \oplus O_2$ | Valide ? | $I_1$ | $I_2$ | $O_1$ | $O_2$ | $O_1 \oplus O_2$ | Valide ? |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 000000 | | | | | | 100000 | | | | | |
| 000001 | | | | | | 100001 | | | | | |
| 000010 | | | | | | 100010 | | | | | |
| 000011 | | | | | | 100011 | | | | | |
| 000100 | | | | | | 100100 | | | | | |
| 000101 | | | | | | 100101 | | | | | |
| 000110 | | | | | | 100110 | | | | | |
| 000111 | | | | | | 100111 | | | | | |
| 001000 | | | | | | 101000 | | | | | |
| 001001 | | | | | | 101001 | | | | | |
| 001010 | | | | | | 101010 | | | | | |
| 001011 | | | | | | 101011 | | | | | |
| 001100 | | | | | | 101100 | | | | | |
| 001101 | | | | | | 101101 | | | | | |
| 001110 | | | | | | 101110 | | | | | |
| 001111 | | | | | | 101111 | | | | | |
| 010000 | | | | | | 110000 | | | | | |
| 010001 | | | | | | 110001 | | | | | |
| 010010 | | | | | | 110010 | | | | | |
| 010011 | | | | | | 110011 | | | | | |
| 010100 | | | | | | 110100 | | | | | |
| 010101 | | | | | | 110101 | | | | | |
| 010110 | | | | | | 110110 | | | | | |
| 010111 | | | | | | 110111 | | | | | |
| 011000 | | | | | | 111000 | | | | | |
| 011001 | | | | | | 111001 | | | | | |
| 011010 | | | | | | 111010 | | | | | |
| 011011 | | | | | | 111011 | | | | | |
| 011100 | | | | | | 111100 | | | | | |
| 011101 | | | | | | 111101 | | | | | |
| 011110 | | | | | | 111110 | | | | | |
| 011111 | | | | | | 111111 | | | | | |

*Figure 2 :* Tableau de cryptanalyse différentielle de S5.