*Université Paris Diderot*
L3 informatique
Sécurité 2016-2017

# Examen
# mardi 23 mai 2017
# 8h30-10h30 (2 heures)

*Aucun document n'est autorisé*

**Exercice 1.—**

1. On a un texte que l'on sait avoir été chiffré avec un chiffrement de César. Si l'on sait que le texte initial était en français, comment peut-on faire pour essayer de décrypter ce texte sans connaitre le décalage?
2. Quelle est la complexité en temps par rapport à la taille du texte du décryptage?

**Exercice 2.—** On considère l'ensemble $\mathcal{C}$ sur l'alphabet $\{0,1\}$:
$\mathcal{C}$=$\{000000, 010101, 110011, 001111, 100110, 011010, 111100, 101001\}$

1. Est-ce un code linéaire?
2. Donner une matrice génératrice sous forme standard de ce code.
3. Quelle est la dimension de ce code?
4. On dispose d'un canal de communication. Il peut y avoir des erreurs de transmission sur ce canal. On utilise le code $\mathcal{C}$ pour chiffrer des mots de 3 lettres, le mot chiffré est transmis sur le canal. Le destinataire le déchiffre et le corrige éventuellement pour retrouver le mot initial.

   Comment fait-on pour chiffrer un mot de 3 lettres avec le code $\mathcal{C}$?
5. Si on suppose qu'il y a au plus une erreur lors de la transmission d'un mot chiffré pour $\mathcal{C}$, peut-on toujours detecter s'il y a eu une erreur et le cas échéant retrouver le mot qui a été chiffré ?
6. Si on suppose qu'il y a au plus deux erreurs lors de la transmission d'un mot chiffré pour $\mathcal{C}$, peut-on toujours detecter s'il y a eu une erreur et le cas échéant retrouver le mot qui a été chiffré ?
7. On suppose qu'il y a au plus une erreur dans la transmission d'un mot chiffré pour le code $\mathcal{C}$. Le destinataire reçoit 110 001. Quel était le mot initial? Décrire l'algorithme utilisé.

**Exercice 3.—** Dans la cryptographie asymétriques chaque entité possède une paire de clefs ($Kpub_i$/ $Kpriv_i$) avec i : identité de l'entité i.

1. Expliquez la différence entre ces deux clefs?
2. Quelle(s) clef(s) A peut-il utiliser (et comment) pour envoyer un message destiné à R et que seul R puisse le lire ?
3. Quelle(s) clef(s) A peut-il utiliser (et comment) pour envoyer un message destiné à R et que seul R puisse le lire et que R puisse verifier que ce message provient bien de A?

**Exercice 4.—**

1. En matière de sécurité informatique dans une infrastructure de clés publiques (PKI), rappelez ce qu'est une autorité de certification? un certificat? Décrire le mécanisme de certification de clés.

2. Expliquez en quoi consiste l'injection de code?
3. Pourquoi la fonction `strcpy` (`char *strcpy(char *dest, const char *src)`) en C peut poser un problème de sécurité?
4. Expliquez en quoi consiste le mécanisme de "sandbox" ?
5. Qu'est-ce que le MAC (Mac Auhtentication Code), à quoi peut-il servir?
6. Qu'est-ce qu'un "Message Digest", à quoi peut-il servir?