# Introduction à la sécurité informatique

Examen - sans document

Durée: 1 heure 30

L'énoncé comporte de nombreuses questions, pensez à gérer votre temps. Attention, pour les questions type QCM, une mauvaise réponse **enlève des points**: si vous ne savez pas, ne répondez pas. Pour certaines questions, plusieurs réponses peuvent être justes. Bon courage !

**Répondez directement sur cette feuille.**

**NOM :** **PRENOM :**

## Cryptologie

### Concepts généraux

**Question 1** L'art de déchiffrer des messages sans connaître la clé de chiffrement est appelé:

- ☐ La cryptographie
- ☐ La cryptologie
- ☐ La cryptanalyse

**Question 2** Un algorithme de chiffrement qui possède une bonne propriété de *diffusion* est tel que:

- ☐ le chiffrement du message s'effectue rapidement
- ☐ une petite modification du message en clair se traduit par une modification complète du chiffré
- ☐ aucune propriété statistique ne peut être déduite du message chiffré

**Question 3** Oscar a réussi à intercepter un couple (message chiffré, message en clair correspondant). A l'aide de ce couple, il a réussi à déterminer la clé $k$ utilisée entre Alice et Bob. C'est une attaque de type:

- ☐ Attaque à texte chiffré
- ☐ Attaque à texte clair connu
- ☐ Attaque à texte clair choisi

Le résultat de l'attaque est un:

- ☐ Cassage partiel
- ☐ Cassage local
- ☐ Cassage complet

## Chiffrements symétriques

**Question 4** Le chiffrement de César est :

☐ une substitution polyalphabétique

☐ une substitution monoalphabétique

☐ un chiffrement par bloc

**Question 5** Un message $m$ (en français) chiffré avec l'algorithme de César a été intercepté par Oscar. Les plus fortes fréquences des lettres de ce messages sont les suivantes:

| **Lettre** | **Fréquence dans le message chiffré** |
|---|---|
| J | 15% |
| F | 8% |
| N | 7,5% |
| X | 7% |
| Autres lettres | <7% |

A l'aide de cette information, retrouvez **la clé** utilisée pour chiffrer $m$ (Rappel: la lettre la plus fréquente en moyenne dans un texte français est le `e`).

- _____

**Question 6** Oscar a intercepté un message chiffré avec l'algorithme de Vigenere. Il a calculé l'indice de coïncidence de ce message (qui est en français) et a obtenu:

| | i=1 | i=2 | i=3 | i=4 | i=5 |
|---|---|---|---|---|---|
| l=1 | 0,045 | | | | |
| l=2 | 0,046 | 0,041 | | | |
| l=3 | 0,083 | 0,075 | 0,081 | | |
| l=4 | 0,042 | 0,039 | 0,076 | 0,039 | |
| l=5 | 0,043 | 0,058 | 0,049 | 0,031 | 0,052 |

Que peut-il déduire de ces résultats ?

- _____

Quelle autre méthode aurait-il pu utiliser pour obtenir cette information ?

- _____

**Question 7** Les chiffrements alphabétiques sont désormais moins utilisés que les chiffrements par bloc.

☐ Vrai

☐ Faux

☐ Les deux sont autant utilisés

**Question 8** Quel est le mode de chiffrement par bloc qui possède la plus mauvaise propriété de diffusion ?

☐ le mode ECB

☐ le mode CTR

☐ le mode CBC

**Question 9** Le principal défaut de DES était:

☐ Sa lenteur

☐ La petite taille de la clé

☐ La complexité de l'algorithme

**Question 10** Après l'abandon de DES, un nouveau standard Américain a été choisi. L'algorithme qui a remplacé DES est:

☐ TDES

☐ Blowfish

☐ AES

## Chiffrements asymétriques

**Question 11** L'avantage des chiffrements asymétriques par rapport aux chiffrements symétriques est que:

☐ Ils sont plus rapides que les chiffrements symétriques

☐ Il n'y a pas besoin de s'échanger de clé secrète

☐ Ils possèdent une meilleure propriété de *confusion*

**Question 12** Qu'est ce qu'une *fonction à sens unique à brêche secrète* ?

---

**Question 13** Le protocole Diffie-Hellman est un protocole qui sert principalement à:

☐ chiffrer/déchiffrer des messages

☐ signer des messages

☐ s'échanger une clé secrète

**Question 14** Alice veut envoyer un message $m$ à Bob. Elle décide de chiffrer ce message via l'algorithme RSA. Elle aura besoin de:

☐ la clé publique de Bob

☐ la clé privée de Bob

☐ la clé privée et la clé publique de Bob

Soit $(n_b, e_b)$ la clé publique de Bob et $d_b$ sa clé privée. Posez le calcul que vont effectuer:

- Alice lorsqu'elle chiffrera le message $m$: $m' =$ _____
- Bob lorsqu'il déchiffrera le message $m'$: $m =$ _____

**Question 15** Sur quel(s) problème(s) difficile(s) est basé le cryptosystème RSA ?

☐ Factorisation

☐ LogarithmeDiscret

☐ Diffie-Hellman

☐ RacineIemeModulaire

**Question 16** Alice veut **signer** le message qu'elle envoie à Bob. Le message va être signé avec

☐ la clé publique d'Alice

☐ la clé privée d'Alice

☐ la clé privée de Bob

**Question 17** Quelle(s) propriété(s) du message permet de garantir la signature ?

☐ l'intégrité du message

☐ la confidentialité du message

☐ l'authenticité du message

**Question 18** Alice veut envoyer un message chiffré via RSA à Bob. L'infrastructure à clé publique (ou PKI) lui permet de:

☐ chiffrer le message de manière plus efficace

☐ augmenter la confidentialité du message

☐ s'assurer que la clé publique du destinataire est bien celle de Bob

# Sécurité logicielle

## Failles logicielles

**Question 19** Soit le programme suivant:

```
int main(int argc, char** argv) {
   char texte[46];
   ...
   strcpy(texte,argv[1]);
   ...
   return 0;
}
```

Ce programme est vulnérable à une attaque de type:

- ☐ buffer overflow
- ☐ race condition
- ☐ format string

**Question 20** Donnez deux moyens de prévenir ou d'empêcher les stack overflow :

- _____
- _____

**Question 21** La variable argv[1] est renseignée par l'utilisateur. Laquelle de ces instructions est alors vulnérable à une attaque de type *format string* :

- `strcpy(buffer,argv[1])`
- `printf(argv[1])`
- `sprintf(chaine,"%10s",argv[1])`

**Question 22** Quel(s) conseil(s) donneriez-vous à un jeune programmeur qui débute pour développer des applications comportant le moins de failles possible ?