Contrairement à l'usage plusieurs questions de cet examen sont des questions ouvertes qui admettent plusieurs réponses. Vous devez justifier le choix de vos réponses et détailler les hypothèses que vous adoptez. Vous devez aussi choisir la précision et la longueur de vos réponses pour respecter le temps limité (deux heures) et pour traiter toutes les questions de manière équilibrée.

Exercice 1. Authentification du serveur par SSH.

1. Voici une tentative de connexion à un serveur SSH.

```
mimosa-coulbois> ssh ssh.logique.jussieu.fr
The authenticity of host 'ssh.logique.jussieu.fr (134.157.19.4)' can't be established.
RSA key fingerprint is 15:a5:c5:76:ad:69:f6:79:95:3a:c9:68:38:41:3e:8d.
Are you sure you want to continue connecting (yes/no)?
```

1.a. De combien de bits est constituée l'empreinte de la clé RSA du serveur `ssh.logique.jussieu.fr` ?

1.b. À votre avis, avec quel algorithme est calculée cette empreinte ?

1.c. Quelle est l'utilité de cette alerte, à quelles conditions est-elle efficace ?

2. Après avoir répondu `yes` à l'alerte ci-dessus le fichier `.ssh/known-hosts` contient la ligne :

```
ssh.logique.jussieu.fr,134.157.19.4 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAzZwAoDtHcumE
cnbpooB6cCCn1i5m314IyRqzTnqbrPiQrMeExml0rsfVNL4Zx2ySbp7n7Vs73pdn0XuJXyonAcoiGk9w
pyy0y/3Ew9bCFLPG4h7NHImmYzjzGoJ4s7+0ibt9Kfy1CGaJbkwc1F+qT+QI8MNx5HrJ+RFfeL99o15J
q/V9v/IosO1N9vtHd7TQxPphjynpPfh9gKqhjoP8cNQKU0zepAWCP5Io/VlwddpPvt97d3Boi8947WrQ
i9NDpQ135KYoUCTP15nQmuMpJ4WwANQjTXt3iW5jNcWFF+IhvM9Mca/T2kSYczP9D1nKoA8serBYG1m6
PA3WliMoUQ==
```

Le codage utilisé ici est base64, un des 64 caractères affichables du jeu ascii [`A-Z,a-z,0-9,+,/`] code le mot de 6 bits correspondant, chaque partie du message commence par 4 octets qui donnent la longueur (en octets) de la partie suivante. On a donc ici trois parties, la première est une chaine de caractère les deux suivantes des nombres :

```
ssh-rsa
0x23
0xCD 9C 00 A0 3B 47 72 E9 [...] 96 23 28 51 (en tout 256 octets)
```

2.a. Quel est l'algorithme cryptographique dont il est question ici ? Quelle est la taille de la clé du serveur `ssh.logique.jussieu.fr` ? Que représente le nombre 35=0x23 qui apparait ici ?

2.b. La taille de cette clé vous parait-elle bien choisie ?

2.c. La clé publique visible ici n'a pas de date d'expiration. Est-ce une faille de sécurité ?

Exercice 2. Authentification du client par yahoo!mail. Nous avons vu lors du premier TD que l'authentification du client par le serveur yahoo!mail se fait par le protocole `HTTP` et de la manière suivante :

1. le client demande la page de login au serveur ;
2. le serveur renvoie une page qui contient l'algorithme MD5 programmé en javascript ainsi qu'un nonce appelé ici `challenge` ;
3. le client envoie au serveur le nom de login et `md5(md5(motdepasse)||challenge)`.

1. Un espion qui a accès à toute la communication peut-il découvrir le mot de passe du client ?

2. Rappeler brièvement les propriétés de l'algorithme MD5. À quoi sert le double appel de la fonction MD5 ?

3. Un attaquant qui a accès à toute la communication peut-il avoir accès aux mèls du client ?

4. Le mot de passe d'un compte yahoo!mail fait au moins six caractères.

4.a. Avez-vous une chance de vous connecter à la place d'un autre utilisateur ?

4.b. Reprendre la question 1 en considérant l'attaque par force brute.

5. Serait-il plus raisonnable pour Yahoo!mail d'utiliser de la cryptographie à clé publique ? Est-ce possible en javascript ?

Exercice 3. On se réfère dans cet exercice au document du Secrétariat général de la Défense nationale reproduit en annexe.

1. À la section 5, quel est le lien discuté entre les protocoles SSL ou TLS et la sécurité ? Plus généralement quels sont les rapports entre la cryptographie et la sécurité des systèmes informatiques.

2. À la section 2, deux types d'algorithmes cryptographiques sont cités dans le fonctionnement du sous-protocole TLS Record. Donner des exemples de tels algorithmes ainsi que leurs propriétés principales.

3. 3.a. Que sont les « clés de session » mentionnées à la fin de la section 2 ? Quelle est une taille raisonnable pour de telles clés ?

3.b. Quelle(s) méthode(s) connaissez-vous pour négocier ces clés de session ?

3.c. Ces méthodes sont-elles vulnérables à l'attaque de l'« homme au milieu » ?

4. Ce document ne discute pas la taille des clés utilisées par les différents algorithmes utilisés par SSL ou TLS. Proposez une sixième section traitant ce problème.