# Série d'exercices du module protocoles cryptographiques

## ***Exercice1 : QCM***

**Question 1 :** Quel service de sécurité permet de vérifier l'identité des utilisateurs en se basant sur leurs caractéristiques biométriques, telles que les empreintes digitales ou la reconnaissance faciale ?

a) Pare-feu
b) Cryptographie
c) Authentification biométrique
d) VPN

**Question 2 :** Quelle est la principale utilisation de la cryptographie asymétrique (ou à clé publique) ?
a) Chiffrer des données pour les stocker en toute sécurité
b) Chiffrer des données pour les transmettre en toute sécurité
c) Générer des empreintes digitales de données
d) Signer numériquement des messages pour l'authentification

**Question 3 :** Quelle technologie de sécurité permet de chiffrer une communication sur un réseau non sécurisé, comme Internet, en créant un tunnel crypté entre deux points de terminaison ?
a) Certificat numérique
b) VPN (Virtual Private Network)
c) Antivirus
d) Pare-feu

**Question 4 :** Quelle est la principale fonction d'une fonction de hachage cryptographique ?
a) Chiffrer des données
b) Vérifier l'intégrité des données
c) Stocker des mots de passe
d) Générer des clés secrètes

**Question 5 :** Quel algorithme de hachage est souvent utilisé pour stocker de manière sécurisée les mots de passe dans une base de données ?
a) SHA-256
b) MD5
c) bcrypt
d) AES

**Question 6 :** Quel service de sécurité permet de contrôler et de filtrer le trafic réseau entrant et sortant pour protéger un réseau informatique contre les menaces ?
a) Pare-feu
b) VPN
c) Cryptographie
d) Antivirus

**Enseignant :** Sofiane AISSANI **Contact :** sofiane.aissani@univ-ubs.fr

**Question 7 :** Quel est l'objectif principal d'un certificat numérique dans le contexte de la sécurité Internet ?

a) Stocker des informations d'identification
b) Authentifier un utilisateur
c) Chiffrer des données
d) Vérifier l'identité d'un site Web

**Question 8 :** Quelle technologie de sécurité est conçue pour prévenir, détecter et supprimer les logiciels malveillants, tels que les virus et les chevaux de Troie, sur un ordinateur ?

a) Pare-feu
b) VPN
c) Antivirus
d) Authentification à deux facteurs

**Question 9 :** Quel type de clé est utilisé en cryptographie asymétrique pour chiffrer les données ?

a) Clé secrète
b) Clé publique
c) Clé privée
d) Clé de session

**Question 10 :** Quelle technologie de sécurité permet d'authentifier un utilisateur en utilisant quelque chose qu'il sait (comme un mot de passe) et quelque chose qu'il a (comme un jeton ou une carte à puce) ?

a) Pare-feu
b) VPN
c) Authentification à deux facteurs
d) Certificat numérique

## ***Exercice 2 : Vérification d'intégrité des fichiers***

**Partie 1 : Création d'un Service de Vérification d'Intégrité**

- Génération de l'Empreinte (Hachage) : Développez un programme permettant de générer une empreinte (hash) d'un fichier. Enregistrez cette empreinte pour une utilisation ultérieure.

**Partie 2 : Vérification de la Méthode**

- Détaillez le processus de vérification d'intégrité en expliquant comment l'empreinte est générée et comment elle peut être utilisée pour déterminer si un fichier a été altéré. Documentez ces explications dans un fichier.

**Partie 3 : Vérification de l'Intégrité du Fichier**

- Envoyez les fichiers nécessaires ainsi que l'empreinte (hash) générée à un autre étudiant. Celui-ci devra vérifier l'empreinte du fichier reçu. Ensuite, il décidera s'il souhaite ou non modifier ce fichier avant de transférer les éléments nécessaires à un troisième étudiant, qui devra détecter toute éventuelle altération.

**Partie 4 : Recherche de Collisions dans SHA-1**

- Recherchez des exemples de deux fichiers ayant la même empreinte (collision) en utilisant l'algorithme SHA-1, et expliquez ce qu'est une collision.

**Partie 5 : La** Signature de l'empreinte résoudra-t-elle le problème des collisions détectées ?

## ***Exercice 3:***

**Objectif :** Les étudiants apprendront à créer un environnement de sécurité en utilisant des certificats numériques pour authentifier les serveurs et les clients.

**Matériel requis :**

- Logiciels de virtualisation (VirtualBox, VMware, ou Docker)
- Serveur virtuel
- Deux machines clientes virtuelles
- Logiciel de gestion de certificats (OpenSSL)

**Travail à faire :**

**Partie 1 : Configuration de l'environnement virtuel :**

- Configurez un serveur virtuel et deux machines clientes virtuelles.
- Assurez-vous que les machines clientes peuvent communiquer avec le serveur.

**Partie2 : Génération de clés et de certificats :**

- Sur le serveur, utilisez OpenSSL pour générer une paire de clés (clé privée et clé publique) pour le serveur.
- Créez un certificat numérique auto-signé pour le serveur en utilisant la clé privée.

**Partie3 : Distribution du certificat :**

- Copiez le certificat du serveur sur les deux machines clientes.
- Sur chaque machine cliente, utilisez OpenSSL pour générer une paire de clés et un certificat pour chaque client.

**Partie4 : Échange de certificats :**

- Les machines clientes envoient leurs certificats au serveur.
- Le serveur envoie son certificat aux deux machines clientes.

**Partie5 : Vérification des certificats :**

- Sur chaque machine cliente, utilisez OpenSSL pour vérifier la validité du certificat du serveur.

- Sur le serveur, utilisez OpenSSL pour vérifier la validité des certificats des deux machines clientes.

**Résultats :** Remettre un rapport qui documente toutes les étapes de l'exercice.

## ***Exercice 4:***

**Question1 :** Quel est le but du protocole Otway-Rees ?

1. $A \dashrightarrow B : M,A,B,\{N_a,M,A,B\}_{kas}$
2. $B \dashrightarrow S : M,A,B,\{N_a,M,A,B\}_{kas},,\{N_b,M,A,B\}_{kbs}$
3. $S \dashrightarrow B : M ,\{N_a,K_{ab}\}_{ka},\{N_b, K_{ab}\}_{kbs}$
4. $B \dashrightarrow A: M,\{N_a,K_{ab}\}_{kas}$

**Question2 :** Les sequences d'etapes de communication suivantes sont-elles des traces valides du protocole ?

**Sequence1 :**

1.1. $A \dashrightarrow I(B) : M,A,B,\{N_a,M,A,B\}_{kas}$

1.4. $I(B) \dashrightarrow A: M,\{N_a, M,A,B\}_{kas}$

**Séquence2 :**

1.1. $A \dashrightarrow I(B) : M,A,B,\{N_a,M,A,B\}_{kas}$

2.1. $I(A) \dashrightarrow B : M,A,B,\{N^1_a,M,A,B\}_{kas}$

2.2. $B \dashrightarrow I(S) : M,A,B,\{N^1_a,M,A,B\}_{kas},\{N^2_b,M,A,B\}_{kbs}$

1.4. $I(B) \dashrightarrow A: M,\{N_a, M,A,B\}_{kas}$

**Sequence3 :**

1.1. $A \dashrightarrow I(B) : M,A,B,\{N_a,M,A,B\}_{kas}$

2.1. $I(A) \dashrightarrow B : M,A,B,\{N^1_a,M,A,B\}_{kas}$

2.2. $B \dashrightarrow I(S) : M,A,B,\{N^1_a,M,A,B\}_{kas},\{N^2_b,M,A,B\}_{kbs}$

3.2 . $I(B) \dashrightarrow S : M,A,B , \{N^1_a,M,A,B\}_{kas},\{N^2_b,M,A,B\}_{kbs}$

*3.3.* $S \dashrightarrow I(B) : M,\{N^1_a,K_{ab}\}_{kas} , \{N^2_b, K_{ab}\}_{kbs}$

1.4. $I(B) \dashrightarrow A: M,\{N_a, M,A,B\}_{kas}$

**Question3 :** Chque etudiant propose une sequence à 3 niveaux qu'il remettra à deux camarades, ceux ci vont dire si la sequence est valide.

## ***Exercice 5:***

Quel est l'objectif du protocole de woo et Lam suivant :

Comment peut-on prouver qu'il contient une faille ?

Trouver une attaque contre ce protocole.

1. $A \longrightarrow B : A$
2. $B \longrightarrow A : N_b$
3. $A \longrightarrow B : \{N_b\}_{kas}$
4. $B \longrightarrow S : \{A, \{N_b\}_{kas}\}_{kbs}$
5. $S \longrightarrow B : \{N_b\}_{kbs}$

## ***Exercice6 (faille de fraicheur)***

Soit le protocole de Needham Shroeder suivant :

Quel est l'objectif du protocole de Needham Shroeder suivant :

Montrer que ce protocole contient une faille de fraicheur. (On suppose que l'intrus possède une clé $K'_{ab}$ générée lors d'une session précédente, et du message 3 : $\{K'_{ab}, A\}K_{bs}$)

1. $A \longrightarrow S : A,B,N_a$
2. $S \longrightarrow A : \{N_a,B, K_{ab}, \{K_{ab},A\}_{Kbs}\}_{kas}$
3. $A \longrightarrow B : \{K_{ab},A\}_{Kbs}$
4. $B \longrightarrow A : \{N_b\}_{kab}$
5. $A \longrightarrow B : \{N_b\text{-}1\}_{kab}$

## ***Exercice7 (Faille d'oracle)***

Soit le défi protocolaire à trois passes suivant avec la propriété suivante pour la fonction de cryptage $\{\{m\}_{K1}\}_{K2}=\{\{m\}_{K2}\}_{K1}$

1. $A \longrightarrow B : \{m\}_{Ka}$
2. $B \longrightarrow A : \{\{m\}_{Ka}\}_{kb}$
3. $A \longrightarrow B : \{m\}_{Kb}$

Trouver une trace d'exécution qui démontre une faille d'oracle.

## ***Exercice 8 ( faille d'association)***

Soit le protocole suivant ;

1. $A \longrightarrow S : A,B,N_a$
2. $S \longrightarrow A : S,\{S,A,N_a,K_b\}K^{-1}{}_s$

Quel est le but de ce protocole ? Trouver une attaque.

## ***Exercice 9 ( faille de type)***

Trouver une attaque exploitant une faille de type dans le protocole d'Otway-Rees

## ***Exercice 10(faille d'implantation)***

On considère le défi à trois passes de l'exercice 7, avec un algorithme cryptographique f qui verifie les propriétés suivantes :

F est binaire, ses arguments sont une clé K et le message M

F est commutative

F est associative

0 est l'element neutre de F

F(x,x)=0

Trouver une attaque qui exploite une faille d'implantation.

## ***Exercice11 (Vérification formelle avec la logique BAN)***

En utilisant la logique BAN, démontrer que le protocole Kerberos vérifie les propriétés pour lesquels il a été conçu.

## ***Exercice 12 : (Projet sur la vérification automatique)***

**Titre du Projet : Comparaison de deux outils de Vérification Automatique de Protocoles**

**Objectif :** Le projet vise à se familiariser avec les outils de vérification automatique de protocoles cryptographiques, vous choisissez deux vérificateurs automatiques vous les présentez, vous démontrez leur utilisation, et vous les comparez en citant leurs avantages et inconvénients.

**Étapes du Projet :**

1. **Recherche et Choix de l'outil :** Choisissez deux outils de vérification automatique. justifier votre choix.
2. **Présentation de l'Outil :** inclure son histoire, son objectif, sa méthodologie, sa plateforme de fonctionnement (Linux, Windows, etc.), et ses principales fonctionnalités.
3. **Exemple d'Utilisation :** Les étudiants devront créer un exemple de protocole cryptographique (peut être un protocole existant ou fictif) et utiliser l'outil pour vérifier la sécurité de deux exemples pour chaque outil (au minimum). Vous expliquez comment vous avez configuré et exécuté l'outil pour analyser les protocoles.
4. **Avantages et Inconvénients et comparaisons:** Comparer les deux outils choisis et discuter les avantages et inconvénients de chaque outil.

**Enseignant :** Sofiane AISSANI **Contact :** sofiane.aissani@univ-ubs.fr

**Livrables du Projet :**

1/ Un rapport contenant

- Présentation de l'outil de vérification automatique de protocoles.
- Document détaillant l'exemple d'utilisation de l'outil sur un protocole.
- Rapport d'évaluation des avantages et inconvénients de l'outil.

2/ Les fichiers nécessaires pour l'exécution de vos exemples (Les mettre dans des fichiers au lieu de les taper directement dans l'interface de l'outil choisi)

**Enseignant :** Sofiane AISSANI **Contact :** sofiane.aissani@univ-ubs.fr