Sécurité des données TD 4

Exercise 1 Message confidentiel et authentifié.
Comment Bob peut envoyer à Alice, en se basant sur le protocole RSA, un message chiffré et signé ? Les données publiques et privées de Alice et Bob sont dans le tableau ci-dessous.

	privé	publique
Alice	d_A	e_A, n_A
Bob	d_B	e_B, n_B

Exercise 2 Suite exo 1.
Bob doit envoyer un message confidentiel et authentifié à Alice, mais ne dispose que d'un canal public. Il utilise le protocole suivant :

Alice engendre les clés et envoie sa clé publique à Bob

Bob engendre les clés et envoie sa clé publique à Alice

Bob produit son message, le signe avec sa clé privée, et le chiffre avec la clé publique d'Alice

Alice reçoit le message, le déchiffre avec sa clé privée, et vérifie que la signature colle avec la clé publique de Bob.

Les fonctions dont Alice et Bob dispose sont :

	privé	publique
Alice	$D_A(C) : C \to C^{d_A} \mod n_A$	$E_A(C) : C \to C^{e_A} \mod n_A$
Bob	$D_B(C) : C \to C^{d_B} \mod n_B$	$E_B(C) : C \to C^{e_B} \mod n_B$

Q Quelle est la faiblesse de ce protocole ? Comment peut-on le rendre sûr ?

Correction : *Dans ce schéma qui semble à première vue parfait, il y a un élément crucial qui n'a pas été pris en compte, et ce dès le début : Bob (resp. Alice) n'a aucune certitude qu'il parle bien à Alice (resp. Bob). Un attaquant, disons Charlie, peut alors se créer lui aussi une paire de clés publique / privée. Il intercepte la clé publique de Bob et envoie la sienne à Alice, sans laisser transiter celle de Bob. De même il intercepte la clé publique d'Alice et envoie la sienne à Bob. Dans toute la suite des échanges, il peut déchiffrer les messages qu'il reçoit (puisque chiffrés avec sa clé publique), et les rechiffrer pour le bon destinataire, sans que ces deux là ne se rendent compte de rien. Cette attaque est appelée l'attaque* de l'homme au milieu *ou man in the middle en anglais*

Pour l'éviter, il faut par exemple que les clés publiques soient certifiées par une tiers authorité, ou que Bob et Alice trouvent un autre moyen de vérifier leurs clés publiques (attestées par un autre correspondant en lequel ils ont confiance au préalable, vérification occulaire derrière un écran etc).

Exercise 3
Un groupe de n personnes souhaite utiliser un système cryptographique pour s'échanger deux à deux des informations confidentielles. Les informations échangées entre deux membres du groupe ne devront pas pouvoir être lues par un autre membre.

1. Quel est le nombre minimum de clefs symétriques nécessaires ?
2. Quel est le nombre minimum de clefs asymétriques nécessaires ?
3. Donner les raisons pour lesquelles ce groupe utilise finalement un système hybride pour le chiffrement ?

Exercise 4 Hachage cryptologique.
On considère l'application suivante du hachage cryptographique. On suppose que h est une fonction de hachage cryptographique que tout le monde (Alice, le serveur, l'espion, ...) connaissent.

- Alice choisit un nombre g
- elle calcule $h(g)$, $h(h(g)) \ldots, h(h(h(h(h(h(h(h(h(h(h(g))))))))))) = h^{11}(g)$
- elle transmet (supposons qu'elle tape directement cette valeur sur le clavier du serveur) $h^{11}(g)$ au serveur qui le stocke tel quel.

L'espion, de son côté, peut espionner tout ce qui passe sur le réseau. Il souhaite se connecter à distance au serveur en se faisant passer pour Alice.

1. Pour s'authentifier à distance, Alice transmet $h^{10}(g)$ au serveur. Est-ce un authentification solide ?
2. Pour s'authentifier à distance une deuxième fois, Alice transmet $h^{10}(g)$ au serveur. Est-ce un authentification solide ?
3. Proposez un algorithme d'authentification sûr qui s'appuie sur les résultats de la question 1 et qui résiste à un espion qui peut lire (mais pas modifier) tout ce qui passe sur le réseau. La seule fonction cryptographique que votre algorithme est autorisé à utiliser est le fonction h.

Exercise 5 Dans $\mathbb{F}_{23}$, les 6 participants $P_1, P_2, \ldots, P_6$ se sont vus attribués les secrets suivants :

$$P_1 : 6,\ P_2 : 19,\ P_3 : 8,\ P_4 : 19,\ P_5 : 6 \text{ et } P_6 : 15.$$

- Retrouvez le seuil t de ce schéma
- Retrouvez le secret.

$$\varsigma\mathrm{I} + x\varepsilon + {}_{\mathcal{C}}x\mathrm{II} = (x)f$$

Exercise 6 Dans $\mathbb{F}_{17}$, les 7 participants P_1 ,P_2, $\cdots$,P_7 veulent partager le secret $s = 13$. Distribuez le secret s entre les 7 participants avec un seuil $t = 4$.