Série 12

1 Chiffrer et déchiffrer

a) Pour chiffrer un message composé de lettres majuscules de A à Z, on utilise le système de substitution suivant. À chaque lettre de l'alphabet, on fait correspondre une autre lettre, par exemple :

$$A \to K, \quad B \to H, \quad C \to D, \quad D \to F, \quad E \to A, \quad F \to P, \quad \text{etc.}$$

On suppose ici que chaque lettre est utilisée une et une seule fois, i.e., qu'il y a une correspondance univoque entre l'alphabet d'origine et celui utilisé pour le chiffrement.

Une attaque par force brute de ce système permet de déchiffrer un message en une heure en testant toutes les substitutions possibles. Combien d'heures cette même attaque nécessitera-t-elle pour déchiffrer un message écrit avec un alphabet de 28 lettres et chiffré avec la même méthode ?

b) Supposons qu'une clé K d'une longueur de 20 bits soit utilisée pour chiffrer un message binaire d'une longueur sensiblement plus grande (on ne spécifie pas ici le système de chiffrement utilisé). Supposons également qu'avec une attaque par force brute avec un ordinateur donné, il soit possible de trouver la clé K (et donc de déchiffrer le message) en 5 minutes. Si maintenant une clé K' deux fois plus longue est utilisée pour chiffrer le message, combien de temps sera nécessaire pour déchiffrer le message avec une même attaque par force brute, si on dispose d'un ordinateur cent fois plus puissant que le premier (i.e., un ordinateur effectuant cent fois plus d'opérations par seconde) ?

2 One-Time Pad

a) Alice souhaite envoyer à Bob le message binaire suivant en utilisant un chiffrement par clé à usage unique (*one-time pad*) avec l'opération XOR ($\oplus$) :

$$M = 11010011$$

La clé (également connue de Bob) est :

$$K = 10111001$$

Calculez le message chiffré C qu'Alice envoie. Vérifiez ensuite que Bob, en appliquant la même opération $C \oplus K$, retrouve bien le message original M.

b) Alice veut maintenant envoyer le mot `CRYPTO` à Bob, mais en utilisant cette fois l'addition modulaire (mod 26) avec la convention A= 0, B= 1, . . ., Z= 25. Sa clé (de même longueur que le message) est :

$$K = \texttt{SECRET}$$

Calculez le message chiffré C qu'Alice envoie. Indiquez la formule utilisée par Bob pour déchiffrer.

c) Eve, malicieuse, sait qu'Alice est paresseuse et utilise toujours la *même* clé K pour chiffrer ses messages. Elle intercepte deux messages chiffrés C_1 et C_2 (chiffrés avec XOR). Que vaut $C_1 \oplus C_2$ en fonction des messages clairs M_1 et M_2 ? En quoi ceci aide-t-il Eve à retrouver M_1 et M_2 ?

3 Protocole de Diffie-Hellman

a) Alice et Bob souhaitent se mettre d'accord sur une clé secrète commune K en communiquant uniquement sur un canal public. Ils se mettent d'abord d'accord publiquement sur le nombre premier $P = 23$ et la base $Q = 5$. Puis Alice choisit le nombre secret $N_A = 6$ et Bob choisit le nombre secret $N_B = 15$.

• Quels nombres N_{QA} et N_{QB} Alice et Bob s'échangent-ils sur le canal public ?

• Quelle est la clé secrète commune K obtenue à la fin du protocole ? Vérifiez qu'Alice et Bob arrivent bien à la même valeur.

• Eve intercepte P, Q, N_{QA} et N_{QB}. Que doit-elle faire pour retrouver K, et pourquoi est-ce difficile en pratique (avec un grand nombre premier P) ?

b) Au cours, nous avons vu comment 2 personnes peuvent parvenir à se mettre d'accord sur une clé secrète K en communiquant uniquement sur un canal public, si on fait l'hypothèse que *l'exponentiation modulo P (avec P un grand nombre premier) est une opération à sens unique*, ce qui veut dire la chose suivante :

"Même en connaissant les valeurs de P, N_1 et N_3 (compris entre 1 et $P-1$) satisfaisant la relation $N_1^{N_2} \pmod P = N_3$, il est très difficile de retrouver la valeur de N_2."

Proposez un protocole similaire permettant à 3 personnes (Alice, Bob et Charlie) de se mettre d'accord sur une clé secrète commune K, tout en ne communiquant que sur un canal public.

4 Chiffrement RSA

Alice souhaite mettre en place une paire de clés RSA. Elle choisit les deux nombres premiers $p = 3$ et $q = 11$.

a) Calculez $n = p \cdot q$ et $\varphi(n) = (p-1)(q-1)$.

b) Alice choisit l'exposant public $e = 3$. Vérifiez que ce choix est valide (i.e., que $1 < e < \varphi(n)$ et $\gcd(e, \varphi(n)) = 1$). Calculez ensuite l'exposant privé d, c'est-à-dire l'entier $1 < d < \varphi(n)$ tel que $e \cdot d \equiv 1 \pmod{\varphi(n)}$. Quelle est la clé publique d'Alice ? Quelle est sa clé privée ?

c) Bob souhaite envoyer à Alice le message $m = 4$. Calculez le message chiffré c que Bob envoie sur le canal public.

d) Montrez qu'Alice retrouve bien le message $m = 4$ en appliquant sa clé privée à c.

5 Questions d'examens passés

a)

Concernant le protocole d'échange de clés de Diffie-Hellman, quelles affirmations sont **vraies** ? (Plusieurs réponses peuvent être correctes.)

- ☐ La sécurité du protocole repose sur la difficulté calculatoire de résoudre le problème du logarithme discret.
- ☐ Pour une sécurité maximale, les clés privées secrètes N_A et N_B doivent être plus grandes que le module premier P.
- ☐ Le protocole est vulnérable à une attaque de l'homme du milieu (*man-in-the-middle*) si un attaquant peut intercepter et modifier les clés publiques échangées.
- ☐ La sécurité du protocole exige que la base Q soit gardée secrète entre les deux parties.

b)

La sécurité du protocole d'échange de clé Diffie-Hellman repose sur la difficulté de factoriser de grands nombres entiers.

- ☐ VRAI
- ☐ FAUX

c)

Parmi les propositions suivantes concernant le hachage (stockage de mots de passe), les signatures numériques et la cryptographie asymétrique, cochez *toutes* celles qui sont correctes.

- ☐ Ajouter un sel aléatoire propre à chaque utilisateur (`hash(salt + mot_de_passe)`) empêche qu'on puisse déduire qu'un même mot de passe est utilisé par plusieurs comptes.
- ☐ Une signature numérique se crée avec la clé privée du signataire et se vérifie à l'aide de sa clé publique.
- ☐ Pour assurer la confidentialité d'un message, on le chiffre avec la clé *privée* du destinataire.
- ☐ Le sel utilisé pour le hachage des mots de passe doit rester secret et ne jamais être stocké en clair.

d)

En utilisant RSA, vous souhaitez protéger une information que vous envoyez à un ami dont la clé publique est $(17,\ 77)$ et la clé privée est $d = 41$. Votre clé publique est $(11,\ 65)$ et votre clé privée est $d = 23$.

A. En utilisant les lettres m et c pour le message en clair et chiffré respectivement, expliquez précisément chaque étape de la communication (en partant du message en clair jusqu'au moment où votre ami récupère le message en clair).

B. Vous souhaitez envoyer le message $m = 19$ à votre ami. Vous le chiffrez puis l'envoyez. Votre ami déchiffre le message reçu et obtient la valeur 12. Donnez une possible erreur qui entraînerait cette conséquence. Justifiez votre réponse.

Note : quelques valeurs de $a^b \bmod c$ (classées par a, b, c) :

$19^{11} = 34 \bmod 65$	$19^{17} = 34 \bmod 77$	$19^{23} = 19 \bmod 33$	$19^{23} = 34 \bmod 65$
$19^{29} = 58 \bmod 65$	$19^{41} = 12 \bmod 77$	$34^{11} = 19 \bmod 77$	$34^{17} = 12 \bmod 77$
$34^{23} = 11 \bmod 65$	$34^{29} = 58 \bmod 65$	$34^{41} = 19 \bmod 77$	$34^{23} = 19 \bmod 65$