TD 3 : Chiffrements asymétriques

Exercice 1 (Chiffrement RSA *).
Soient $p = 3$ et $q = 11$ deux nombres premiers.

1. Calculez n et $\Phi(n)$.
2. Soit $e = 7$, chiffrez le message $M = 2$.
3. Calculez la clé secrète d et déchiffrez $C = 3$.
4. Trouvez et démontrez une propriété homomorphique sur RSA.

Exercice 2 (Exemple de clé partagée Diffie-Hellman). Alice et Bob souhaitent convenir ensemble d'une clé secrète pour chiffrer leurs futures communications, sans pour autant prendre le risque de se rencontrer. Ils vont pour cela utiliser le protocole de Diffie-Hellman pour établir une clé partagée, détaillé ci-dessous.
Alice et Bob ont accès à deux nombres publics : un nombre premier $p = 11$ et un nombre compris entre 2 et $p - 1$, appelé générateur et noté g. Dans cet exercice, on prend $g = 2$. Le nombre premier p est en théorie très grand pour assurer la sécurité.
Alice tire un entier aléatoire a compris entre 2 et $p - 1$, et Bob tire un entier aléatoire b compris entre 2 et $p - 1$. Ici on prend $a = 3$ et $b = 4$. Le protocole de Diffie-Hellman pour échanger une clé fonctionne comme suit :

1. Alice envoie à Bob : le reste A de la division de g^a par p (c'est un entier compris entre 0 et $p - 1$)
2. Bob envoie à Alice : le reste B de la division de g^b par p

Alice et Bob calculent ensuite un nombre commun K : ce nombre est le reste de la division de $(B)^a$ par p (pour Alice), qui est aussi égal au reste de la division de $(A)^b$ par p (pour Bob).
Ils échangent ensuite des messages chiffrés avec cette clé partagée K.

- Calculez la clé DH partagée par Alice et Bob.

Exercice 3 (Attaque sur Diffie Hellman *). Alice et Bob utilisent le protocole de Diffie Hellman pour convenir d'une clé partagée (voir exercice précédent).
Un intrus a accès aux nombres A et B échangés par Alice et Bob. Cependant, lorsque p et g sont très grands, le temps de calcul nécessaire pour découvrir la valeur de a à partir des valeurs de p, g et A, même avec les meilleurs ordinateurs, est beaucoup trop long pour que cela soit envisageable.

- Saurez-vous imaginer comment un intrus, qui peut lire, intercepter ou modifier les messages échangés entre Alice et Bob, peut déchiffrer toutes leurs futures communications ?

Exercice 4 (Température *). Un thermomètre connecté mesure la température entre 35°C et 41°C au dixième de degré près. Les températures sont chiffrées par une clé publique RSA avec une clé de 4096 bits et envoyées aux utilisateurs. Comment un intrus peut-il apprendre les températures en ne connaissant que la clé publique ?

Exercice 5 (El Gamal *). On rappelle que le schéma de chiffrement El Gamal fonctionne de la manière suivante : soit M un message et r un élément aléatoire de $\{1, \dots, p-1\}$, on a :

$$c = (c_1, c_2) \text{ avec } c_1 = g^r \mod p \text{ et } c_2 = M \cdot h^r \mod p$$

où $(g, p, h = g^x \mod p)$ est la clé publique du destinataire construite à partir d'un élément secret x tiré aléatoirement dans $\{1, \dots, p-1\}$. L'élément x est la clef privée.
Rappel : p est un (grand) nombre premier et g est un générateur de $\mathbb{Z}/p\mathbb{Z}$, mais vous n'avez pas besoin de ces propriétés dans l'exercice.

Pour déchiffrer un message c on a :

$$M \equiv c_2 \cdot c_1^{-x} \mod p$$

1. Soit $x = 2$ et $(p, g) = (5, 3)$, calculez h et déchiffrez $c = (4, 2)$.
   Rappel : $c_1^{-x} \mod p = (c_1^x)^{-1} \mod p = (c_1^{-1})^x \mod p$
2. Vérifiez (par un calcul) que le message trouvé à la question précédente donne bien le chiffré c en prenant $r = 2$.
3. Rappelez le problème du logarithme discret.
4. Montrez que si l'on sait résoudre le logarithme discret alors on sait déchiffrer le chiffrement d'Elgamal.

Exercice 6. * Bellare Rogway
On considère deux fonctions de hachage G et H et une fonction à sens unique (OWF) f :
$G\colon \{0,1\}^{k_0} \to \{0,1\}^{k_1}$, $H\colon \{0,1\}^{k_0+k_1} \to \{0,1\}^{k_2}$ et $f\colon \{0,1\}^{k_0} \to \{0,1\}^{k_3}$.
Le chiffré par le système Bellare & Rogaway d'un message $x \in \{0,1\}^{k_1}$ vaut :

$$c = f(r) \| (x \oplus G(r)) \| H(x \| r)$$

où r est un mot binaire aléatoire de longueur k_0.
Trouvez l'algorithme de déchiffrement, sachant que vous avez accès à la fonction inverse f^{-1}.

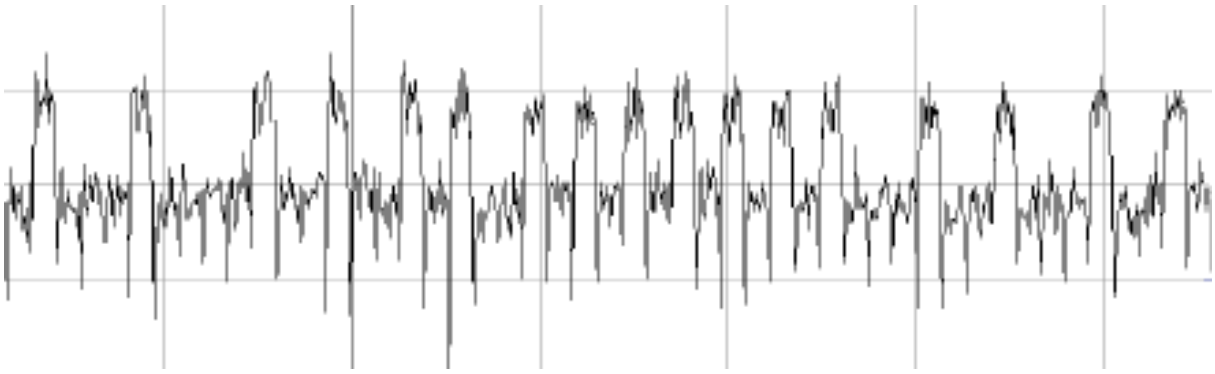
Exercice 7 (Power Attack sur la signature RSA). On rappelle l'algorithme *Square and Multiply* :

Input : a, d, n
Output : $a^d \mod n$
Convert d to binary $k_s k_{s-1} \dots k_1 k_0$
$b \leftarrow 1$
for $i = s, i >= 0, i$- **do**
  $b \leftarrow b \cdot b \mod n$
  if $k_i = 1$ **then**
    $b \leftarrow b \cdot a \mod n$
return b.

1. Exécutez l'algorithme Square and Multiply à la main pour calculer $a^d \mod n$ avec $s = 4$, $a = 2$, $d = 11$, et $n = 21$.

2. En utilisant un appareil approprié, on peut mesurer la consommation d'électricité d'un processeur qui effectue une signature RSA à l'aide de la clé privée d.

   Sachant qu'une multiplication modulaire consomme plus qu'une élévation au carré modulaire, déterminez la valeur en binaire de la clé privée d (32 bits), en utilisant la trace ci-dessous du calcul d'une signature.



3. Déterminez la valeur de la clé privée en hexadécimal.

Exercice 8 (Attaques de RSA **).

1. Soit un chiffré c, vous avez accès à un oracle de chiffrement et de déchiffrement qui déchiffre tous les message sauf c. Comment retrouver le message chiffré par c ?
2. Alice a une clé RSA, avec $N_1 = pq$. Elle génère une autre clé avec un autre premier r, et utilise $N_2 = qr$. Comment casser les deux clés d'Alice ?