Exercices
Semaine 11

Cours Turing

1 Chiffrement de Diffie-Hellman-Merkle

a) Ecrivez une fonction en Python qui prenne un nombre entier $n \geq 1$ en entrée et génère en sortie un nombre K compris entre 0 et (26**n)-1 avec l'algorithme de Diffie-Hellman-Merkle.

Notes : - Vous jouez ici à la fois les rôles d'Alice et de Bob ! Vérifiez juste à la fin de votre algorithme que ces deux-là ont bien calculé le même nombre K.

- Idéalement, le nombre K devrait se situer entre 26**(n-1) et (26**n)-1 (cf. partie b), mais l'algorithme de Diffie-Hellman-Merkle ne peut pas garantir ceci à 100%,

b) Transformez ensuite ce nombre K en une liste de n nombres compris entre 0 et 25 (également appelée "clé K" ci-dessous).

c) Implémentez ensuite le système de clé à usage unique pour chiffrer un message M de longueur n avec la clé K (pour ce faire, transformez d'abord le message M en une suite de n nombres compris entre 0 et 25). Vérifiez que votre système fonctionne en déchiffrant le message avec la même clé K.

Note : Comme déjà fait précédemment, nous travaillons ici avec les nombres entre 0 et 25 (et l'addition modulo 26), plutôt que de travailler avec les bits 0 et 1 (et l'opération XOR).

2 Racine carrée d'un nombre en arithmétique modulaire

Définition : Soit N un nombre entier et C un autre nombre entier compris entre 1 et $N-1$. On dit que M est une *racine de C modulo N* si $M^2 \pmod{N} = C$.

La racine d'un nombre n'existe pas toujours en artithmétique modulaire. Dans ce qui suit, on s'intéresse au cas particulier où $N = P$ est nombre premier.

a) Vérifier par des tests que si $P > 2$ est un nombre premier, alors $C^{(P-1)/2} \pmod{P} = 1$ ou $P-1$, pour tout nombre entier C compris entre 1 et $P-1$.

Note : Remarquez que le petit théorème de Fermat est une conséquence de ceci !

Le *critère d'Euler* dit que C admet une racine modulo P si et seulement si $C^{(P-1)/2} \pmod P = 1$.

b) Dans les cas où C et P satisfont le critère d'Euler *et aussi* $P \pmod 4 = 3$, trouver une formule pour le nombre M tel que $M^2 \pmod P = C$, et vérifier par des tests que ceci fonctionne.

Indication : Par le critère d'Euler, M existe si et seulement si $C^{(P-1)/2} \pmod P = 1$, et donc dans ce cas, $C^{(P+1)/2} \pmod P = C$, et vu que $P \pmod 4 = 3$, on en déduit que...

3 Fonction à sens unique de Rabin

Dans cet exercice, nous allons voir que la calcul de la racine carrée d'un nombre entier modulo N est plus compliqué pour un nombre N qui n'est pas un nombre premier, et que ceci peut même servir à définir une fonction à sens unique.

Supposons donc que $N = P \cdot Q$, avec P et Q premiers tels que $P \pmod 4 = 3$ et $Q \pmod 4 = 3$.

Dans ce cas, si on connaît seulement la valeur de N, mais pas celle de P et Q. il n'y a pas d'algorithme efficace qui permette, étant donné un nombre C compris entre 1 et $N-1$, de calculer (s'il existe) le nombre M tel que $M^2 \pmod N = C$.

Par contre, si on connaît les valeurs de P et Q, il est alors possible de calculer la racine carrée de C modulo N. Voici l'algorithme :

- calculer successivement M_P, la racine de C modulo P, ainsi que M_Q, la racine de C modulo Q (en utilisant à chaque fois l'exercice 2).

- puis les nombres entiers X_P et X_Q tels que $X_P \cdot P + X_Q \cdot Q = 1$; ceci peut se faire grâce à l'algorithme d'Euclide étendu :

`https://www.techiedelight.com/fr/extended-euclidean-algorithm-implementation/`

- les racines M de C modulo N seront alors les quatre nombres suivants :

$$R_1 = (X_P \cdot P \cdot M_Q + X_Q \cdot Q \cdot M_P) \pmod N \quad R_2 = N - R_1$$
$$R_3 = (X_P \cdot P \cdot M_Q - X_Q \cdot Q \cdot M_P) \pmod N \quad R_4 = N - R_3$$

Cette fonction à sens unique est utilisée dans le *cryptosystème de Rabin*, qui fonctionne ainsi :

- Bob choisit deux grands nombres premiers P et Q, calcule $N = P \cdot Q$ et envoie N à Alice.

- Pour envoyer un message M, Alice envoie le message chiffré $C = M^2 \pmod N$.

- Vu que Bob connaît les valeurs des nombres P et Q, il peut déchiffrer le message M en utilisant l'algorithme ci-dessus (*NB :* reste à identifier la bonne racine parmi les quatre !).

- Tandis que si Eve intercepte le message chiffré C, mais connaît seulement la valeur de N, elle ne sait pas comment faire autrement pour décrypter le message M que de tester toutes les possibilités, ce qui prend trop de temps (et rappelez-vous aussi que factoriser N est une opération a priori difficile, donc Eve ne connaît ni P ni Q).