Exercices
Semaine 11

Cours Turing

1 Un autre système cryptographique ?

Voici une autre proposition se basant sur l'idée du one-time pad pour permettre à Alice et Bob de s'échanger un message secret, alors qu'Eve écoute tout :

1. Pour transmettre un message M, Alice utilise une clé K_1 de même longueur que M, calcule $C_1 = M \oplus K_1$ et envoie le message chiffré C_1 à Bob.
2. Bob reçoit le message C_1 et lui ajoute une autre clé K_2 de même longueur : $C_2 = C_1 \oplus K_2$, et renvoie C_2 à Alice.
3. Alice reçoit C_2, lui soustrait sa clé K_1 (ce qui revient à faire une addition) : $C_3 = C_2 \oplus K_1$, et renvoie C_3 à Bob.
4. Finalement, Bob reçoit C_3, lui soustrait sa clé K_2 et déchiffre ainsi le message M d'Alice.

Voici maintenant la question pour vous : est-ce que ce système fonctionne ? et est-il sûr à 100% ?

2 Fonction à sens unique de Rabin

Le but de cet exercice est d'explorer la fonction à sens unique de Rabin. Dans tout ce qui suit, M fait référence au message qu'Alice veut envoyer à Bob, et C à la version chiffrée de celui-ci.

a) Dans une première partie, vous allez d'abord écrire un programme qui teste si, étant donné un nombre premier P, un autre nombre C compris entre 0 et $P-1$ est un carré modulo P, i.e., s'il existe un nombre M tel que $C = M^2 \pmod{P}$.

- une première possibilité est de le faire naïvement, en testant tous les nombres M possibles pour une valeur de C en entrée ;

- une deuxième possibilité est d'utiliser le *critère d'Euler*, qui dit que la réponse est positive si et seulement si $C^{(P-1)/2} \pmod{P} = 1$

Testez ces deux algorithmes et comparez leur efficacité.

b) Dans cette deuxième partie, on se donne toujours un nombre premier P, qui vérifie de plus la condition $P \pmod{4} = 3$ (par exemple, $P = 7$, $P = 19$ ou encore $P = 43$, mais pas $P = 41$).

Ecrivez un programme qui trouve, si elle existe, la racine modulo P d'un nombre C, i.e., le nombre M compris entre 0 et $P-1$ tel que $M^2 \pmod P = C$.

Indication : Par le critére 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...

Si Alice utilise le message chiffré $C = M^2 \pmod P$, avec P un nombre premier (même grand), Bob pourra déchiffrer celui-ci, mais Eve aussi (car rappelez-vous que le nombre P doit être public) : il faut trouver autre chose...

c) Dans cette troisième partie, on se donne un nombre $N = P \cdot Q$, avec P et Q premiers et tels que $P \pmod 4 = 3$ et $Q \pmod 4 = 3$.

Alice envoie maintenant le message chiffre $C = M^2 \pmod N$. L'affirmation ici est que si Bob connaît les valeurs des nombres P et Q, il va être capable de déchiffrer le message M (voir plus bas), tandis que si Eve intercepte le message chiffré C, mais connaît seulement la valeur de N, elle ne sait pas comment faire pour décrypter le message M (et rappelez-vous aussi que factoriser N est une opération a priori difficile, donc Eve ne connaît ni P ni Q).

Ecrire un programme qui calcule successivement :

- M_P, la racine de C modulo P, ainsi que M_Q, la racine de C modulo Q (en utilisant à chaque fois la partie b).

- 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/`

- le message M sera alors l'un des quatre nombres suivants :

$R_1 = (X_p \cdot P \cdot M_Q + X_Q \cdot Q \cdot M_P) \pmod N$

$R_2 = N - R_1$

$R_3 = (X_p \cdot P \cdot M_Q - X_Q \cdot Q \cdot M_P) \pmod N$

$R_4 = N - R_3$

3 Protocole d'échange de clé de Diffie-Hellman-Merkle avec trois personnes

Au cours, nous avons vu comment deux personnes, Alice et Bob, peuvent parvenir à se mettre d'accord sur une clé secrète K en communiquant uniquement sur un canal public, tout en évitant qu'Eve puisse décrypter la clé K. Dans cet exercice, on vous propose de réfléchir à un protocole similaire permettant à trois personnes, disons Alice, Bob et Charlie, de se mettre d'accord sur une clé secrète commune K, tout en ne communiquant que sur un canal public.