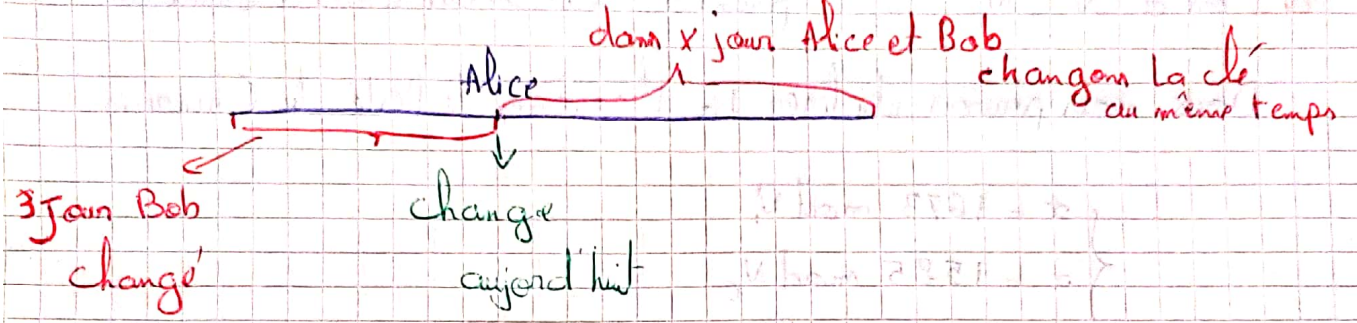
Série de révision

Exercice 1:



x est un multiple de 25
$x+3$ est un multiple de 31

$$\begin{cases} x \equiv 0 \bmod (25) \\ x+3 \equiv 0 \bmod (31) \end{cases}$$

$$\Leftrightarrow \begin{cases} x \equiv 0 \bmod (25) \\ x \equiv -3 \bmod (31) \end{cases}$$

Remarque : $\text{pgcd}(25, 31) = 1$

(Il existe) D'après le C.R.T il existe une solution unique $x =$

$$x = \sum_{i=1}^{2} a_i y_i M_i \bmod (25 \times 31)$$

$m_1 = 25 \quad m_2 = 31$

$M = m_1 \times m_2 = 775$

$M_1 = \frac{M}{m_1} = 31 \quad M_2 = \frac{M}{m_2} = 25$

$y_1 = M_1^{-1} [m_1] \qquad y_2 = M_2^{-1} [m_2]$

$y_1 = M_1^{-1} \bmod 25 \qquad y_2 = M_2^{-1} \bmod 31$

Algorithme d'Euclide Etendu

$\Rightarrow$ formule de Bezout pour calculer y_1 et y_2

$y_1 = 5 \bmod 25 \qquad y_2 = -4 \bmod 31$

$$x \equiv 0 \times 31 \times 5 + -3 \times -4 \times 25 \bmod (775)$$

$$x \equiv 300 \bmod (775)$$

Exercice 2:

a- on a N_1, N_2, N_3 sont premier entre eux deux à deux

Donc nous pouvons utiliser La théorème de Reste du Chinoi.

$$\begin{cases} x = 1673 \mod N_1 \\ x = 1525 \mod N_2 \\ x = 1032 \mod N_3 \end{cases}$$

Il existe une solution unique de $x = \sum_{i=1}^{3} a_i y_i M_i \mod(N_1 \times N_2 \times N_3)$

$$\begin{cases} M = 1673 \times 1525 \times 1032 \\ M_i = \frac{M}{m_i} \\ y_i = M_i^{-1} \mod(N_i) \end{cases}$$

$$x \equiv 820516\,3253 \times y_1 + 918923\,6725 \times y_2 + 645893\,8152 \times y_3 \mod N_1 N_2 N_3$$

Ce qui donne :

$$x \equiv 19851423906251 \mod 13600070353$$
$$\equiv 8921261224 \mod(N_1, N_2, N_3)$$

$$e_k(m) = m^3 \mod N_1 \equiv 1673 \mod N_1$$
$$e'_k(m) = m^3 \mod N_2 = 1525 \mod N_2$$
$$e''_k(m) = m^3 \mod N_3 = 1032 \mod N_3$$

$$m^3 = 8921261224 \mod(N_1 N_2 N_3)$$
$$N_1 \times N_2 \times N_3 = 13600070353$$

On a $0 < m < N_1$

$0 < m < N_2$

$0 < m < N_3$

$\Longleftrightarrow \quad 0 < \underset{X}{\underset{|||}{m^3}} < N_1 N_2 N_3 \}$

or x est aussi $< N_1 N_2 N_3$

d'où $m^3 = x \mod (N_1 . N_2 . N_3)$

$m = \sqrt[3]{x}$

Exercice 3

$$h(x) = \begin{cases} 1 // x & \text{Si } |x| < n \\ 0 // g(x) & \text{Sinon} \end{cases}$$

a – Supposons que h n'est pas résistante aux collisions.

Donc : Il existe (X, X') telque $X \neq X'$ et $h(X) = h(X')$

1er cas : Si $h(X)$ et $h(X')$ commance par ~~0~~ 1

c-à-d $h(x) = h(x') = ~~0//X~~ \; 1//X$

$= ~~0//X'~~ \; 1//X'$

d'où $X = X'$

contradiction avec le fait que $X \neq X'$

2ème cas : Si $h(x)$ et $h(x')$ commance par 0

c-à-d $h(x) = h(x') = 0//g(x)$

$= 0//g(x')$

$\Rightarrow g(x) = g(x')$

contradiction avec le fait que $g(x) \neq g(x')$ car g est un fonction résistante aux collision d'où $X \neq X'$

Conclusion : h est résistante aux collisions

b - Soit h une fonction résistante aux collision, Supposons que h n'est pas résistante à La seconde préimage.
il existe un x comme dont le haché est h(x)
Et que Il existe un $x' \neq x$ telque $h(x') = h(x)$
donc il existe un couple (x, x') telque $x \neq x'$ et $h(x) = h(x')$ ce qui est contradictoire au fait que h est résistante aux collision.

Exercice 4 :

a - $x \in [1, p-2]$

b - $m_1 \neq m_2$ On suppose qu'on va utiliser le même aléatoire K soit $S_1 = K^{-1}(H(m_1) - xn) \bmod (p-1)$

$S_2 = K^{-1}(H(m_2) - xn) \bmod (p-1)$

$\begin{cases} r_1 = g^k \bmod (p) \\ S_1 \end{cases}$ $\begin{cases} r_2 = g^k \bmod (p) \\ S_2 \end{cases}$

On can pourra calculer $S_2 - S_1 = K^{-1}H(m_2) - K^{-1}xn + K^{-1}H(m_1) + K^{-1}x$

$S_2 - S_1 = K^{-1}H(m_2) - K^{-1}H(m_1) \bmod (p-1)$

$S_2 - S_1 = K^{-1}(H(m_2) - H(m_1)) \bmod (p-1)$

La fonction d'hachage, m_1, m_2 est déja connue et Si $(H(m_2) - H(m_1))^*$ est inversible modulo $(p-1)$

$$(H(m_2) - H(m_1))^{-1} \cdot (S_2 - S_1) = K^{-1} \bmod (p-1)$$

Donc il va déduire K à partir K^{-1}, Et il pourra à partir de S_1 ou S_2 et déterminer La clé X Donc c'est la camp TOTAL.

⚠ Donc on est obliger de modifier K chaque fois dans La signature d'un menage dans Le chiffrement ElGamal (Signature)