Université Mohammed V **Année Universitaire 2021/22**
Faculté des Sciences de Rabat Master IPS ; Module :SI
Département d'Informatique **Prof : Mme F.Omary**

Série de TD
(Hachage & signature)

Exercice :1

Soient p et q deux nombres premiers tels que : q divise p-1 et le problème du logarithme discret dans Z_p^* soit difficile.

Soit $\alpha \in Z_p^*$ une racine q^e de 1 modulo p.

On définit $\beta \equiv \alpha^a \bmod p$ où :

$0 \leq a \leq q-1$

Soit h : $\{0,1\}^* \rightarrow Z_q$ une fonction de hachage sûre.

Pour un nombre aléatoire secret k, $1 \leq k \leq q-1$ et K l'ensemble formé par la clé publique et la clé privé. On définit la signature d'un document x par :

$$Sig_K(x, k) = (\gamma, \delta) \text{ Où:}$$

$$\gamma = h(x // \alpha^k)$$

et

$$\delta = k + a\gamma \bmod p$$

1) **Comment peut-on construire α ?**
2) **Définir une clé publique et une clé privé pour le schéma de signature ci-dessus.**
3) **Comment peut-on vérifier la signature du document x ?**

4) **Application :**

On prend q=101 et p= 78q+1 = 7879

Hypothèse : 3 est un élément primitif dans (Z_{7879}^*) .

1) **construire α**
2) **Prendre a=75**
3) **Définir la clé publique et la clé privé.**
4) **On suppose que Alice veuille signer le message x et qu'elle choisisse k=50, déterminer la signature correspondant à ces paramètres.**
   (Indication : On suppose que $h(x // \alpha^k) = 96$
5) **Vérifier bien cette signature.**

Exercice 2

Comment peut-on vérifier que la signature d'El Gamal a été construite correctement ?

1) Monter que $\mathbf{A^r r^s \equiv g^{(H(M))} \bmod p}$
2) Que fait Bob pour vérifier l'authenticité du document en question ?

Exercice3

On note (Z//2Z/) par F et par F m l'ensemble des chaînes de m bits pris dans F .

Soit, f : $F^m \rightarrow F^m$ une fonction quelconque. On propose g comme fonction de hachage à itérer, définie comme suit :

On a g : $F^{2m} \rightarrow F^m$ telle que pour une chaîne x de 2m bits, découpée en 2 blocs $\mathbf{X}_h$ et $\mathbf{X}_l$,on ait $g(x)=g(x_h//x_l)=f(x_h \oplus x_l)$

Montrer que g n'est pas résistante à la seconde préimage.