# 1 Réduction de Pollig-Hellman

Soit $G$ un groupe d'ordre $pq$ avec $p$ et $q$ premiers entre eux. Soit $g$ un générateur de $G$ et $h \in G$. En utilisant l'identité de Bezout montrer comment calculer le logarithme discret de $h$ en complexité $O(\sqrt{\max\{p,q\}})$.

# 2 Protocole d'encryption d'El-Gamal

## 2.1 Description de protocole

Alice choisit un groupe $G$ cyclique d'ordre $q$ dans lequel l'hypothèse décisionnelle de Diffie-Hellman est vérifiée et $g$ un générateur de $G$. Elle tire un élément $x$ aléatoirement dans $\{0, 1, .., q-1\}$ et calcule $h = g^x$. Elle publie la clef publique $pk = (G, g, h)$ et conserve la clef secrète $sk = x$.
Pour envoyer un message $m$, Bob tire un élément $r$ aléatoirement dans $\{0, 1, .., q-1\}$. Il calcule $c_1 = g^r$ et $c_2 = m.h^r$ et envoie comme chiffré $c = (c_1, c_2)$.

1. Comment Alice retrouve t-elle le message $m$ à partir du chiffré ?
2. Rappeler l'hypothèse décisionnelle de Diffie-Hellman.
3. Si l'hypothèse n'est pas vérifiée, comment un attaquant peut-il retrouver le message ?

## 2.2 Sécurité du protocole

On suppose que l'on est en possession d'un algorithme $\mathcal{A}$ qui déchiffre une instance d'El-Gamal avec une probabilité $p$. On veut se servir de cette algorithme pour résoudre le logarithme discret dans $G$.

1. A partir de l'algorithme $\mathcal{A}$ construire un algorithme qui, sur une instance $(g^a, g^b, g^c)$ renvoie si $ab = c$ avec une probabilité $p'$.
2. En supposant que $c = ab$ avec une probabilité $\frac{1}{2}$, quel est la probabilité de succès de cet algorithme ?

## 2.3 Propriété d'homomorphisme

1. Montrer qu'en connaissant le chiffré d'un message $m$ il est possible de chiffrer le message $2m$.
2. Connaissant le chiffrer de deux messages $m_1$ et $m_2$, peut-on chiffrer $m_1 + m_2$ ? Et $m_1 \times m_2$ ?

# 3 Composition de fonctions

Soit $H_1 : \{0,1\}^n \to \{0,1\}^m$ et $H_2 : \{0,1\}^m \to \{0,1\}^l$ deux fonctions de hachage avec $n > m > l$. Est-ce que $H$ définie par $H(x) = H_2(H_1(x))$ est une fonction de hachage ?

# 4 Fonction de Chaum, Van Heijst et Pfitzmann

## 4.1 Préliminaires mathématiques.

Soit $p$ un nombre premier. Un élément $x$ de $\mathbb{Z}/p\mathbb{Z}^*$ est un générateur si tous les éléments de $\mathbb{Z}/p\mathbb{Z}^*$ sont des puissances de $x$ (modulo $p$). Dans ce cas, si $x^i = x^j \mod p$, alors $i = j \mod p - 1$.
Lemme de Gauss : Si $a$ divise $bc$ et que $a$ est premier avec $b$, alors $a$ divise $c$.

## 4.2 Description de la fonction

Considérons un (grand) nombre premier $q$, choisi de telle sorte que $p = 2q + 1$ est premier lui aussi. On prend aussi deux générateurs de $\alpha$ et $\beta$ du groupe $\mathbb{Z}/p\mathbb{Z}^*$. La fonction de hachage prend en entrée deux nombres $x$ et $y$ dans l'intervalle $\{0, ..., q-1\}$ et calcule : $H(x, y) = \alpha^x \beta^y \mod p$.

1. Supposons que $q$ s'écrive sur $n$ bits. Quelle sont les tailles (en bits) de l'entrée de $H$ et de sa sortie ?
2. Quelle est (en fonction de $n$) la complexité asymptotique du calcul de $H$ ?
3. Comment faire pour hacher des messages plus long sans augmenter la taille de $q$ ?
4. Comme on a supposé que $\alpha$ était un élément primitif, alors on sait qu'il existe $\lambda$ tel que $\beta = \alpha^\lambda \mod p$. Si $\alpha$ et $\beta$ nous sont imposés, déterminer $\lambda$ revient à résoudre un problème algorithme usuel en cryptologie à clef publique. Lequel ?
5. Ce problème est-il facile à résoudre, pour de grandes valeurs de $p$ ?
6. Montrez que si on connaît la valeur de $\lambda$, alors on peut facilement forger des collisions pour la fonction.

## 4.3 Résistance aux collisions

On a donc vu que si on connaît le logarithme discret de $\beta$ en base $\alpha$, alors on peut fabriquer des collisions. L'objectif des questions suivantes est de montrer la réciproque : si on arrive à trouver une seule collision, on est capable de calculer le logarithme discret de $\beta$.

1. Expliquez pourquoi cela garantit la résistance aux collisions de la fonction de hachage.

2. Supposons qu'on ait une collision sur $H$, c'est-à-dire deux paires $(x, y) \neq (u, v)$ telles que $H(x, y) = H(u, v)$. Justifiez qu'on a alors : $\alpha^{x-u} = \beta^{v-y} \mod p$.

3. Justifiez qu'on a :
$$\lambda(v - y) - (x - u) = 0 \mod p - 1$$

4. . On pose $d = PGCD(z - y, p - 1)$. Rappelons que c'est le plus grand entier (positif) qui divise à la fois $z-y$ et $p-1$. En utilisant le fait que $z$ et $y$ sont strictement inférieurs à $q$, montrez que $d$ est strictement inférieur à $q$ (on peut supposer que $z - y > 0$).

5. En utilisant le fait que $d$ divise $p - 1$ et le lemme de Gauss, justifier que $d$ vaut soit 1, soit 2.

6. Dans le cas où $d = 1$, justifiez qu'il y a une seule valeur de $\lambda$ possible, et trouvez comment on peut la calculer facilement.
   Le cas où $d = 2$ est plus pénible, car l'équation en $\lambda$ a deux solutions, et il est plus difficile de les calculer. C'est néanmoins possible, et on peut tester laquelle des deux solutions réalise effectivement $\beta = \alpha^{\lambda}$. On peut donc calculer le logarithme de $\beta$ dans tous les cas.