# 1 Fonction de Chaum, Van Heijst et Pfitzmann

## 1.1 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 $c$.

## 1.2 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.

## 1.3 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.

# 2 Devoir maison

## 2.1 Fonction de hachage

1. Rappelez les trois propriétés que doit vérifier une fonction de hachage.
2. Soit $f$ la fonction $x \to x^2 \mod N$. Quelle propriétés vérifie $f$ ?
   Soit $g : \{0,1\}^* \to \{0,1\}^n$ que l'on suppose résistante à la collision. Soit $h : \{0,1\}^* \to \{0,1\}^{n+1}$ définie par
   - $h(x) = 1|x$ si $x$ est de longueur $n$.
   - $h(x) = 0|g(x)$ sinon

   Quelle propriétés vérifie $h$ ?
3. Quels autres implications ou non-implications pouvez-vous trouver.
4. Soit $h : \{0,1\}^* \to \{0,1\}^n$. On suppose que pour un élément $m$ aléatoire, la probabilité d'avoir une valeur donnée $h(m)$ est de $\frac{1}{2^n}$ (l'espace d'arrivée est équiprobable). Donner une attaque pour chaque propriété de $h$ ainsi que sa complexité.

## 2.2 Utilisation de couplages, variante sur Diffie-Hellman

Soit $G$ et $G_T$ deux groupes cycliques de même cardinal $q$ et $g$ un générateur de $G$. Soit $e$ une fonction $G \times G \to G_T$ bilinéaire : $e(g^a, g^b) = e(g, g)^{ab}$ pour tout $a, b \in \mathbb{Z}/q\mathbb{Z}$. On suppose que la fonction $e$ peut être calculée en temps polynomial.

1. Montrer que pour tout $a \in \mathbb{Z}/q\mathbb{Z}$, $e(g^a, g) = e(g, g^a) = e(g, g)^a$.
2. Montrer que le problème décisionnel de Diffie-Hellman (connaissant $g^a$, $g^b$ et $g^c$, déterminer si $g^{ab} = g^c$) peut être résolu en temps polynomial dans $G$.
3. En se basant sur le protocole d'échange de clef Diffie-Helmann, créez un protocole d'échange de clef à trois personnes. Chaque personne envoie un seul message à chacune des deux autres personnes et tous les messages sont envoyés simultanément.
   Quelle est l'hypothèse de complexité sous-jacente à ce protocole ?

# 3 Examen deuxième session 2021

## 3.1 Questions courtes

1. Le masque de Véran consiste à ajouter une chaîne de caractère aléatoire à un message. Quels sont les avantages et inconvénients de ce système ?
2. Soit $N$ un entier fixé. On tire aléatoirement des entiers dans $\{1, ...N\}$. Combien faut-il de tirages pour que la probabilité de tirer deux entiers identiques soit supérieure à $\frac{1}{2}$ ?
3. Quelle est la différence entre la cryptographie à clef publique et la cryptographie à clef privée ?

## 3.2 Algorithme pas de bébé - pas de géant

Soient $G$ un groupe cyclique d'ordre $n$ et g un générateur de $G$. On pose $b = \lceil \sqrt{n} \rceil$.

1. Soit $h$ un élément de $G$. Montrer qu'il existe $(q; r) \in \{0, ..., b-1\}^2$ vérifiant $g^{bq}h = g^r$.
2. En déduire un algorithme donnant le logarithme discret d'un élément de $G$ en base $g$ de complexité $O(\sqrt{n})$.
3. Quel est l'espace en mémoire nécessaire à l'exécution de cet algorithme ?
4. Supposons $G = (\mathbb{Z}/31\mathbb{Z})^*$. Calculer le logarithme discret de 15 en base 3 par cette méthode.

## 3.3 Signature RSA

On considère le protocole de signature suivant :

- KeyGen $\rightarrow (pk = (N, e), sk = d)$
- Sign$(m, d) = \sigma = m^d \mod N$
- Verif$(pk, m, \sigma) = 1$ si $m = \sigma^e \mod N$

1. Montrer que le protocole est correct i.e. que Verif(Sign$(m, d) = 1$ pour tout message $m$.
2. Montrer que ce protocole ne résiste pas à une forge existentielle dans un attaque sans message, i.e. un attaquant peut générer un couple $(m, \sigma)$ valide.
3. Supposons que $N = 437$ et $e = 17$. Connaissant les deux couples $(m_1, \sigma_1) = (100, 156)$ et $(m_2, \sigma_2) = (2, 257)$, signez le message $m = 200$.