Attaque du système de cryptage d'El Gamal

Plan :

I/ Présentation du problème et des algorithmes.

II/ Un outil indispensable : les tables de hachage.

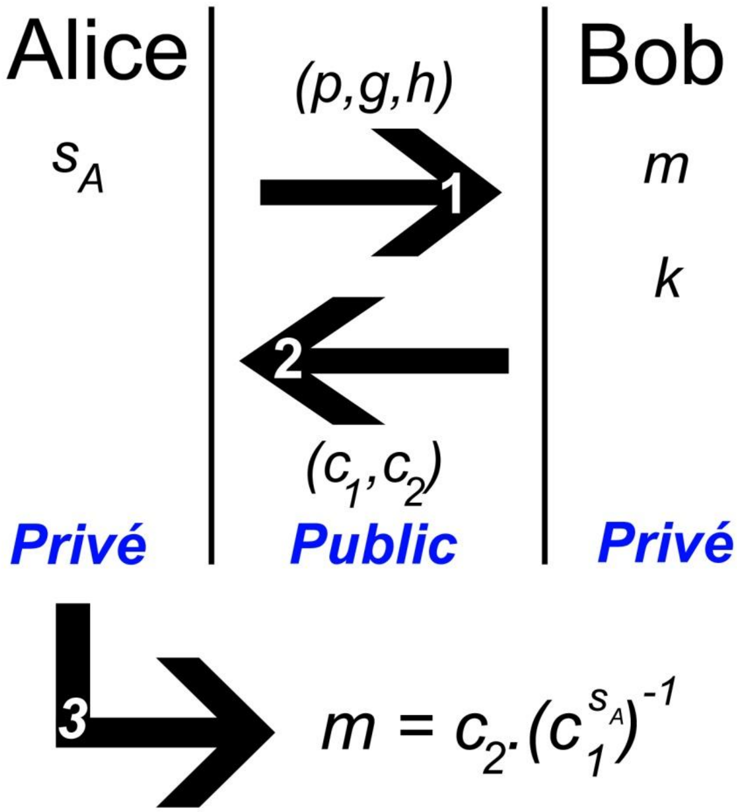
III/ Efficacité et limites de l'algorithme de Shank.

I/ a) a) Crypto-système d'El Gamal et problème du logarithme discret.

Propriété 1 : Pour p un nombre premier, $\left(\left(\mathbb{Z}/p\mathbb{Z}\right)^*, .\right)$ est un groupe.

De plus, ce groupe est cyclique, c'est-à-dire qu'il existe ∝ tel que :

$$\left(\mathbb{Z}/p\mathbb{Z}\right)^* = \{\propto^0, \propto^1, \dots, \propto^{p-2}\}$$



p nombre premier.

g générateur de G = $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$

$h = g^{s_A}$

$c_1 = g^k$ et $c_2 = m.h^k$

$h^k = g^{k.s_A} = {c_1}^{s_A}$

$c_2.({c_1}^{s_A})^{-1} = m.h^k.(h^k)^{-1} = m$

Définition 1 : Soit G un groupe cyclique d'ordre *p* dont la loi est notée multiplicativement, soit *g* un élément générateur de G et *y* un élément de G. On appelle logarithme discret le plus petit entier *k* tel que :

$$y = g^k$$

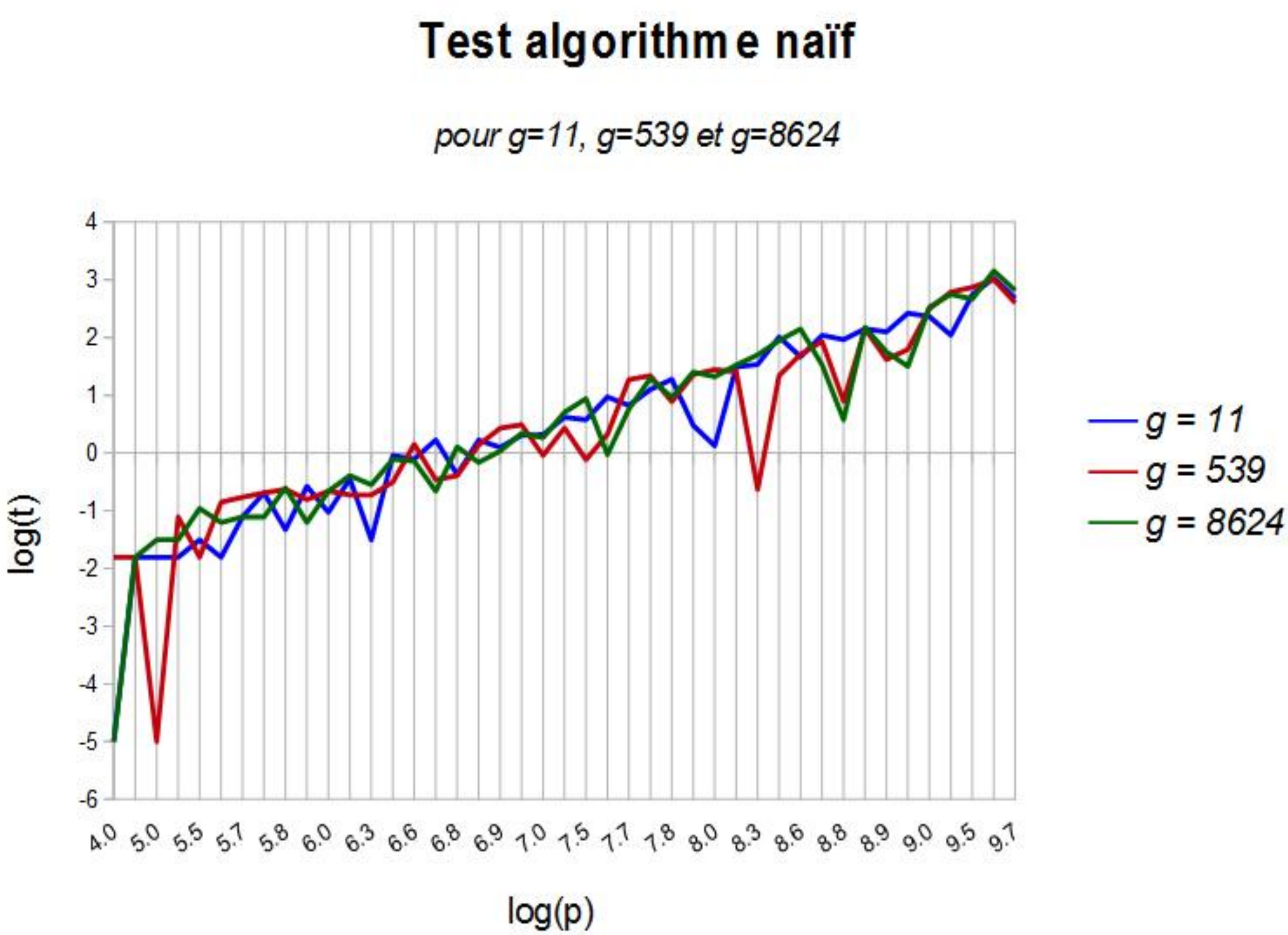
I / b) Algorithme naïf.

Principe : On calcule les puissances successives de *g* jusqu'à tomber sur *y.*
→ g^0, g^1, g^2, …, *y* .

→ Complexité en $O(p)$.

→ Construction d'une liste de valeurs de p à tester :
- *Problème 1 :* méthode de recherche d'éléments générateurs pas assez efficace.
- *Problème 2 :* exponentiations trop importantes.

Tests pour $\mathrm{y} = 647$et $\mathrm{g} \in \{11; 539; 8624\}$ selon p :



I / c) Une méthode plus efficace : Algorithme de Shank.

Exemple : $p = 19$, $g = 2$ et $y = 18$.

1: $n = 5$ $(E(\sqrt{p})+1)$

2: Baby-step

2^0	1
2^1	2
2^2	4
2^3	8
2^4	16

3: 2^5 | $32=13$

$1=13\times3-19\times2$

$(2^5)^{-1} = 3$

Algo. étendu Euclide

4: Giant-step

18×3^0	18
18×3^1	$54=16$

5: $18\times(2^{-5})^1=2^4$

$k=5\times1+4=9$

	Naïf	**Shank**
Espace	$O(1)$	$O(\sqrt{p})$
Temps	$O(p)$	$O(\sqrt{p})$

Comment stocker les données ? ➔ Tables de hachage

II / a) Définition d'une table de hachage.

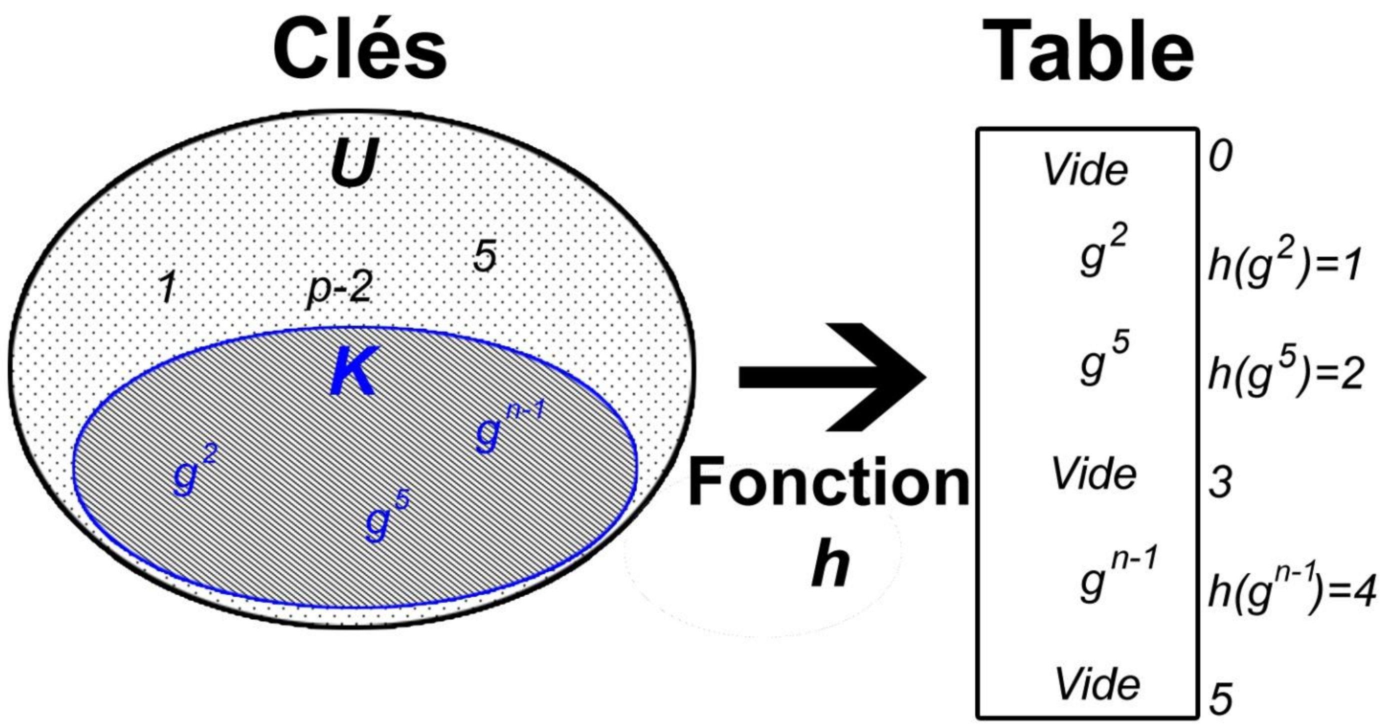
«Univers des clés» : $U = \{0, \dots, p-1\}$

Ensemble des clés de *U* qu'on va stocker : $K = \{g^0 mod\ p, \dots, g^{n-1} mod\ p\}$

Définition 2 : On définit une **table de hachage** comme un tableau de taille l dont la case numéro i (nommée **alvéole**) est :

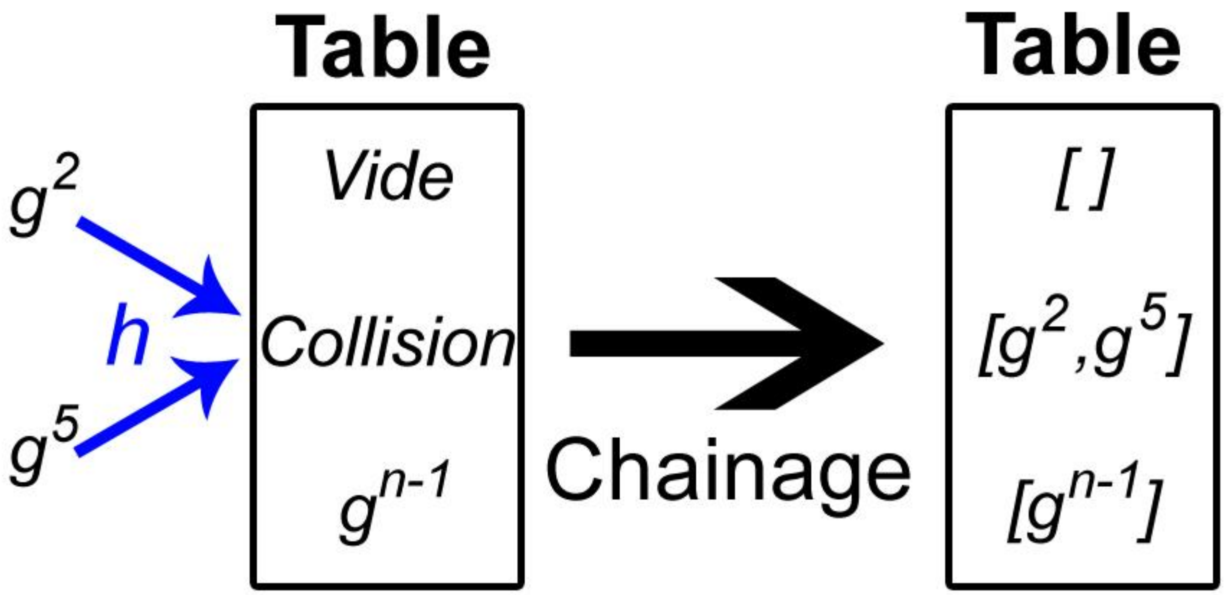
- Soit vide.
- Soit contient un élément $z \in U$ tel que $h(z) = i$.

L'application $h: U \to [\![0; l-1]\!]$ est appelée **fonction de hachage**.



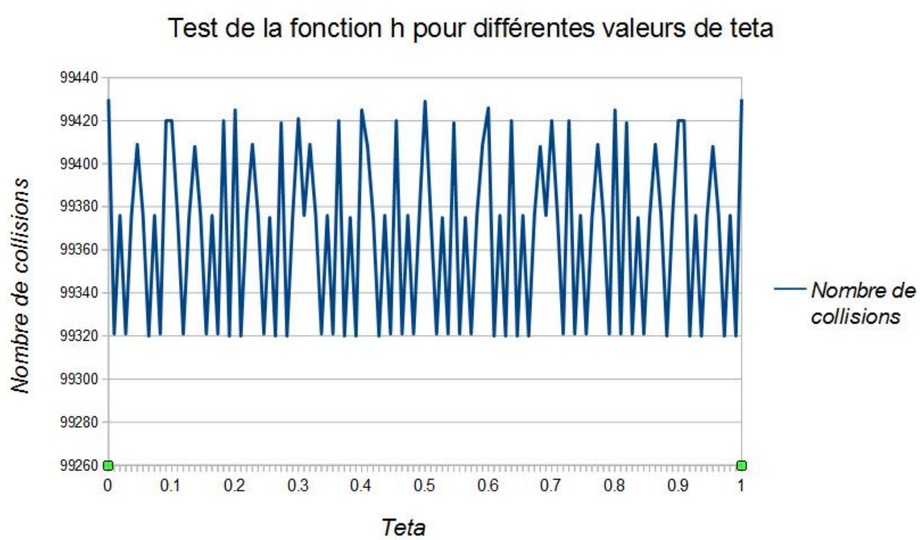
II / b) Gestion des collisions par chainage.

Définition 3: Soit $(u, v) \in U^2$. On dit qu'il y a « collision » si $u \neq v$ et $h(u) = h(v)$.



II / c) Etude d'une fonction de hachage.

Fonction de hachage : $h: x \to \lfloor ((x \times \theta) \bmod 1) \times l \rfloor$ avec $\theta \in [0; 1]$.



Théoriquement :

$$\theta_{optimal} = \frac{\sqrt{5} - 1}{2}$$

$$\approx 0.6180339887498949$$

III / Efficacité et limites de l'algorithme de Shank.

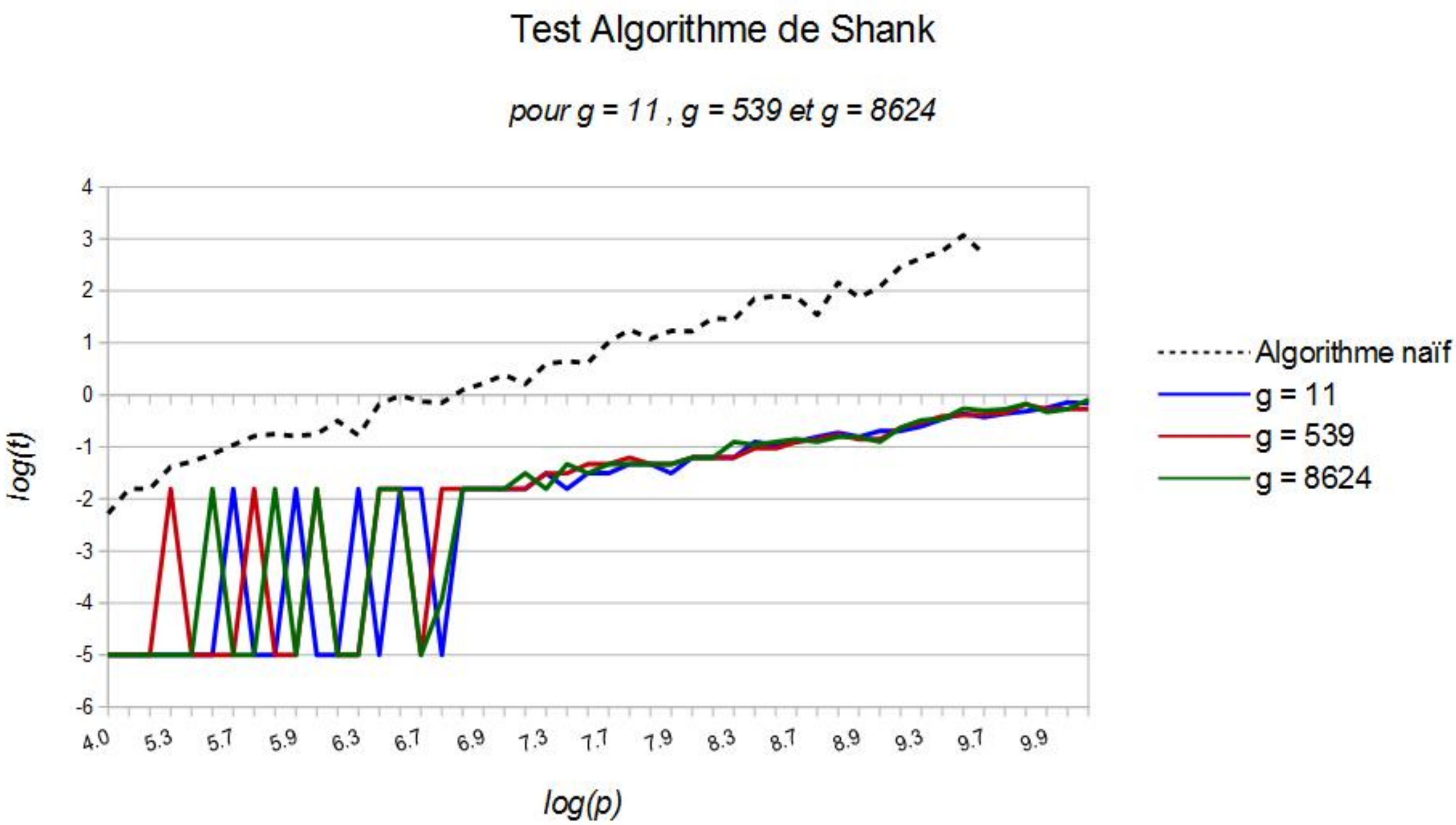


Table de hachage pour $y = 647$, $g = 539$ et $p = 10000103$: