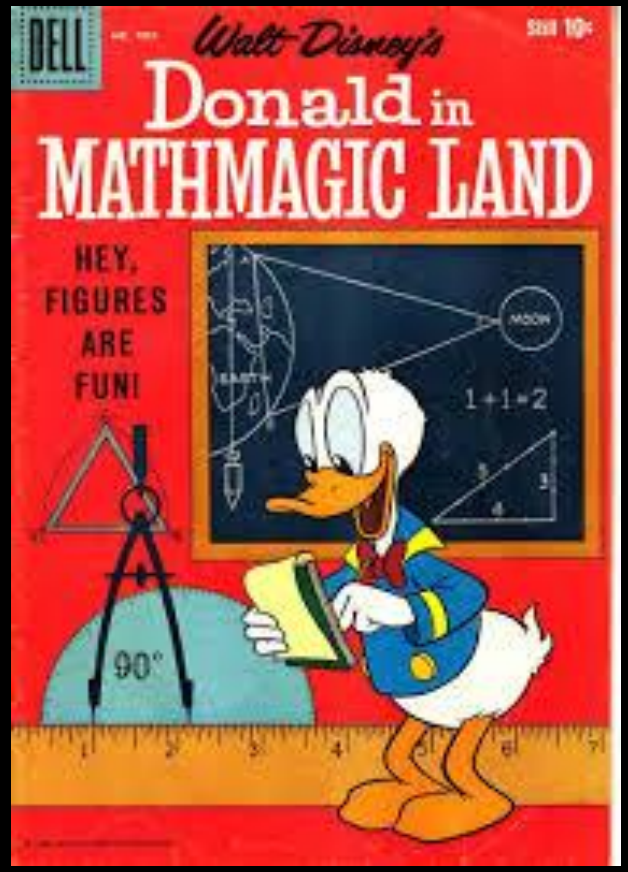
Et si les mathématiques étaient un pays ?

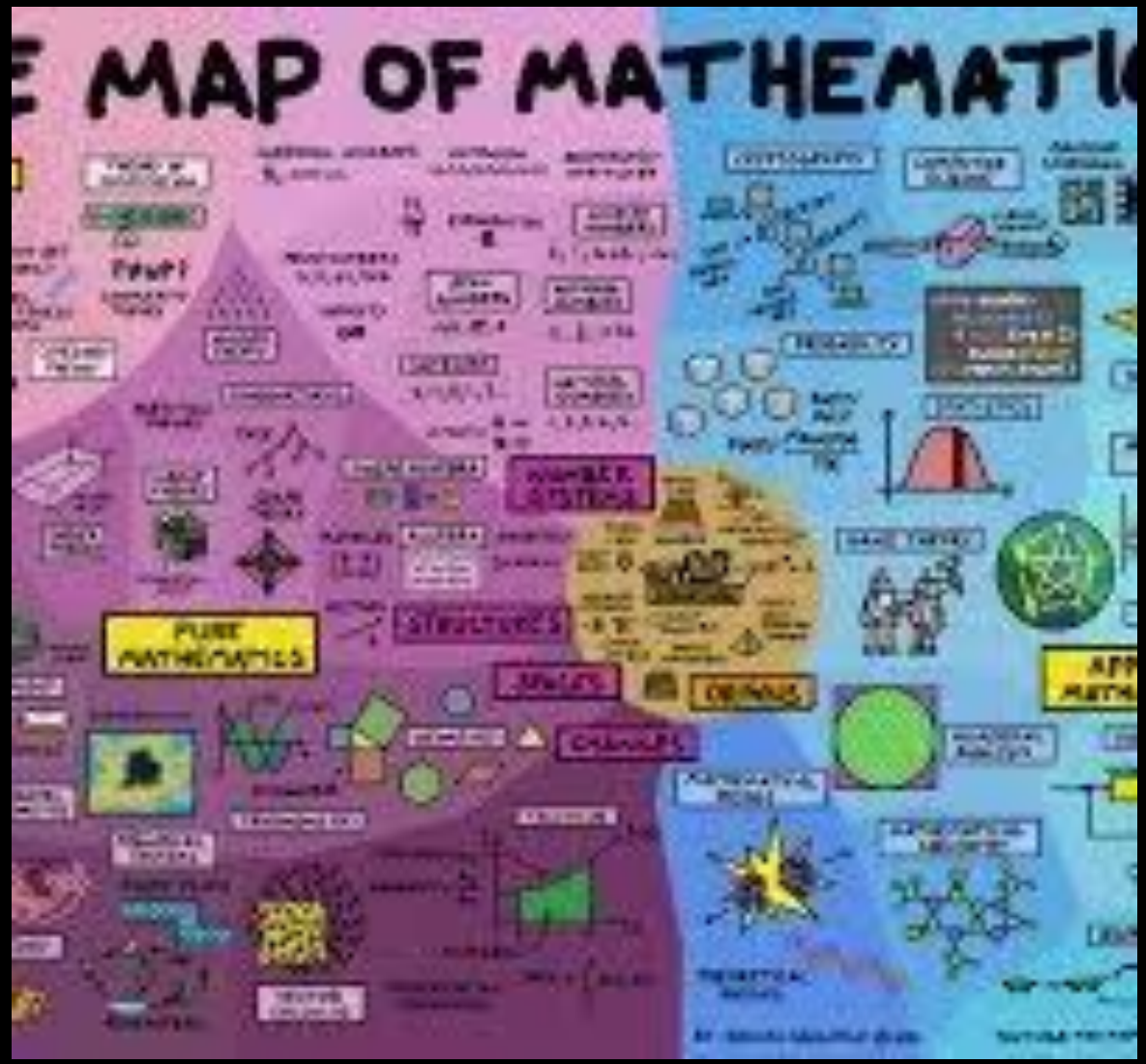
- Ou serait la cryptologie ?



Réponse possible (seulement pour l'amusement)

Dans la province de l’arithmétique, dans le district de l’algèbre, dans le voisinage de la théorie des nombres, il existe un village où les mystères sont cachés, où les trésors sont ensevelis, où les énigmes demeurent... C’est le village de la cryptologie.

Nous allons parlé d'une maison en particulier dans ce village : la maison du logarithme discret



Securité du chiffrement : Les buts

En ordre d'ambition(fort à faible)

Bris total: retrouvé la clé sécrete. Cela permettrait de déchiffrer tous les messages passés, présents et futurs.

Casser la notion de sens unique : trouvé le message original étant donnée le message chiffré c . Comment ?
 Reponse: Sans récupérer la clé, juste **inverser la fonction de chiffrement**.

Casser la notion de sécurié semantique : retrouver une information étant donnée le message chiffré c.Par exemple, l'adversaire decouvre que le message m fait parti d'un ensemble finis d'élement.

Moyen de l'adversaire

Moyens de l'adversaire

On a, par ordre décroissant de difficulté pour l'adversaire :

- **l'attaque à chiffré(s) seul(s)** : l'adversaire ne connaît que le chiffré (moyen le plus faible);
- **l'attaque à clair(s) connu(s)** : l'adversaire connaît un ou plusieurs (éventuellement un très nombre) couples clairs chiffrés;
- **l'attaque à clair(s) choisi(s)** : semblable à la précédente, mais pour laquelle l'adversaire peu sir les clairs
- **l'attaque à chiffré(s) choisi(s)** : l'adversaire obtient les déchiffrements correspondants.

Explication à l'aide d'exemple(pour les amateurs de soccer)

- Attaque à chiffré seul : c= 7789009 , cela à rapport avec un jouer de soccer aucune information de plus
- Attaque à clair connu : plusieurs couples clairs chiffrés.

-"`But de Saka à la 23e`" → chiffré en "`847293`"

-"`Carton rouge pour Ramos`" → "`732812`"

But: En accumulant ces paires, il tente de déduire le fonctionnement du chiffrement, pour décrypter d’autres messages.

Continuation ...

Attaque à clair choisi: L’adversaire peut **choisir un message clair** m et obtenir son chiffré c.

Il envoie volontairement à un système de chiffrement :

- `"But de Ronaldo"`
- `"But de Ronaldo à la 88e"`

Et il obtient les chiffrés correspondants.
Il utilise ces résultats pour **comprendre la structure du chiffrement** .

Continuation...

- Attaque chiffré(s) choisi(s)
- Exemple sport :
- Il envoie volontairement un chiffré inconnu, comme "934729", au système, et celui-ci lui renvoie :
  ➡️ "Blessure de Mbappé"
  Avec assez de tentatives, il peut reconstruire des messages sensibles ou casser la clé.

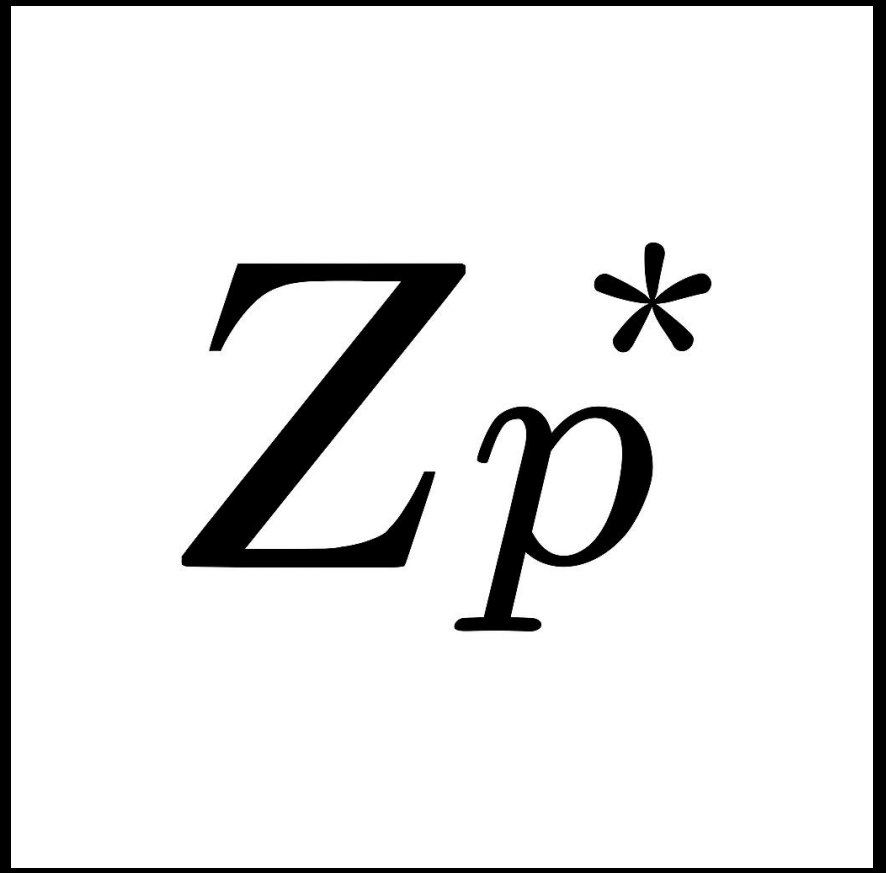
Le problème du logarithme discret

enoncé:

1. Le problème du logarithme discret

Soit $(G, \times)$ un groupe cyclique d'ordre n et g un générateur. $G = \{g, g^2, \ldots, g^{n-1}, g^n = 1\}$. Étant donné $h \in G$, le **problème du logarithme discret** consiste à retrouver x défini modulo n tel que $h = g^x$. On note $\log_g(h) = x$.

- Ici, nous nous interessons aux groupes cycliques pour lesquelles le problème du logarithme discret est difficile.



Au sujet de ce groupe en particulier(exemple)

Définition : Générateur de groupe

Un **générateur de groupe multiplicatif** de $\mathbb{Z}^*_p$ (le groupe des entiers modulo p premiers avec p) est un élément de ce groupe qui, lorsqu'il est élevé à différentes puissances, génère tous les autres éléments non nuls de $\mathbb{Z}^*_p$. Autrement dit, un générateur est un élément g tel que tous les éléments de $\mathbb{Z}^*_p$ peuvent être obtenus en élevant g à des puissances successives.

Exemple :

Si p=7, alors $\mathbb{Z}^*_7$ ={1,2,3,4,5,6}. Un générateur possible est g=3, car en élevant 3 à des puissances successives, on peut obtenir tous les éléments de $\mathbb{Z}^*_7$:

- $3^1 \equiv 3 \, mod(7)$
- $3^2 \equiv 2 \, mod(7)$
- $3^3 \equiv 6 \, mod(7)$
- $3^4 \equiv 4 \, mod(7)$
- $3^5 \equiv 5 \, mod(7)$
- $3^6 \equiv 1 \, mod(7)$

Application Cryptographique

L'echange de clefs de Diffie-Hellman(76)

Protocole interactif permettant à Alice et Bob d'echanger publiquement des informations et à la fin du protocole de connaitre une quantité qui pourra servir comme clef secrete pour faire du chiffrement

Description (1)

Pour cela Alice et Bob se mettent tout d'abord publiquement d'accord sur un groupe $(G, \times)$ cyclique d'ordre n et g un générateur.

- Ensuite Alice choisit un a aléatoire $1 < a < n$ et calcule $A := g^a$ et envoie cette quantité à Bob sur un canal public.
- Parallèlement Bob choisit un b aléatoire $1 < b < n$ et calcule $B := g^b$ et envoie cette quantité à Alice sur ce canal public.
- Alice calcule $B^a = g^{ab}$. Bob de son côté calcule $A^b = g^{ab}$. Cette quantité $C = g^{ab}$ sera leur secret commun.

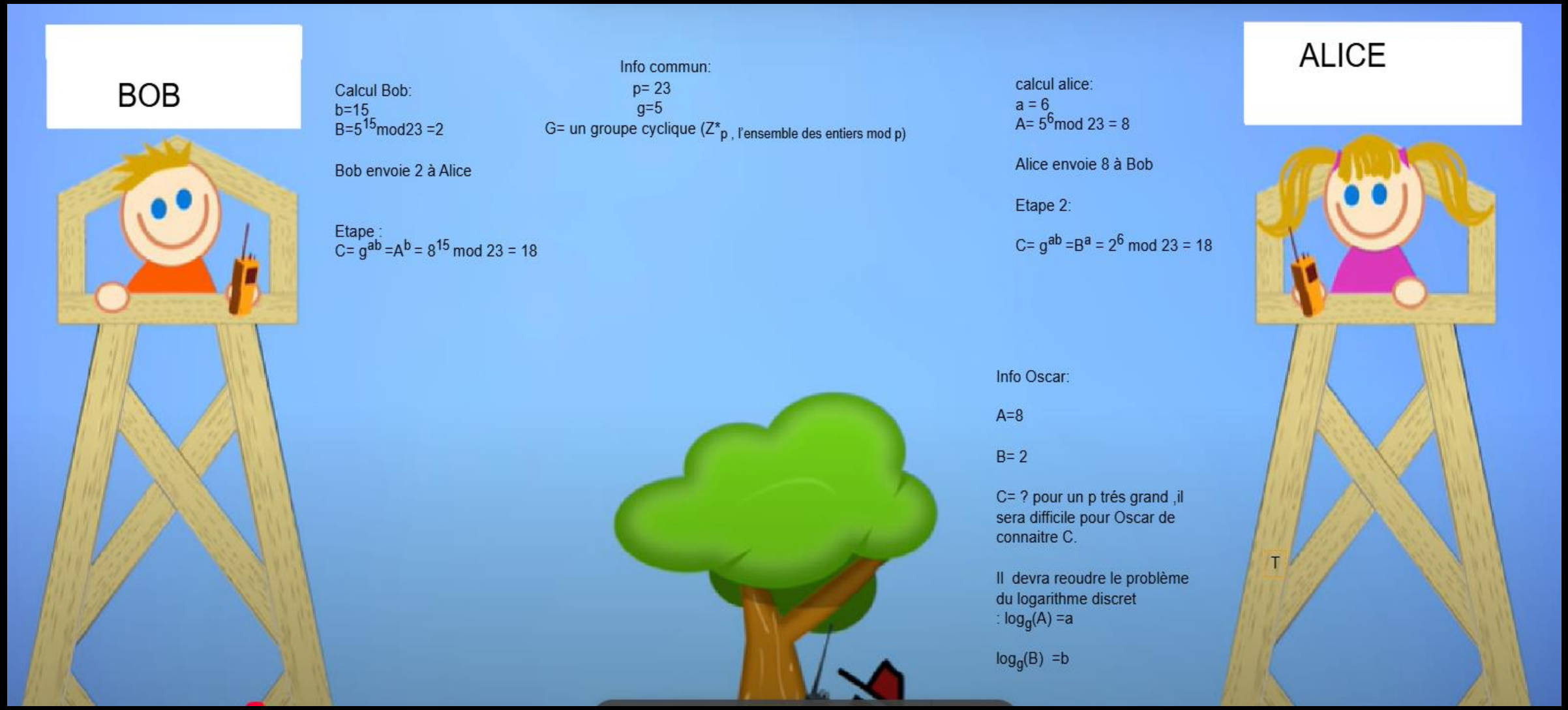
Description (2)

- Pour un hypothetique personnage malicieux oscar qui ecoute les echange entre Alice et Bob , il faudra resoudre le problème du logarithme discret :

commun.

Pour retrouver cette quantité, Oscar qui écoute les échanges entre Alice et Bob doit résoudre le problème suivant : étant donné $A, B \in G$ calculer $C \in G$ tel que $C = g^{ab}$ où a et b sont tels que $A = g^a$ et $B = g^b$. Ce problème est appelé **problème calculatoire de Diffie-Hellman**, et (A, B, C) est appelé un triplet Diffie-Hellman.

Exemple clé d'echange diffie-hellmann: petite histoire



Le chiffrement de Elgamal

C'est un chiffrement à clef publique qui peut se déduire de l'échange de clef Diffie-Hellman. Pour recevoir des messages Bob choisit un groupe $(G, \times)$ cyclique d'ordre n et g un générateur. Il choisit ensuite un x aléatoire $1 < x < n$ et calcule $h = g^x$.

Le triplet $K^B_{pub} = (n, g, h)$ constitue la clef publique de Bob, et $K^B_{priv} = x$ est sa clef privée.

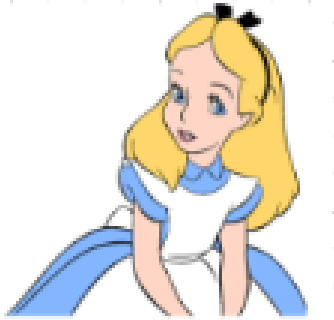
Pour envoyer un message $m \in G$ à Bob, Alice choisit r aléatoire $1 < r < n$, et calcule $\text{Chiff}_{K^B_{pub}}(m) := c := (c_1, c_2) = (g^r, mh^r) \in G \times G$.

Pour déchiffrer, Bob calcule $\text{Dechiff}_{K^B_{priv}}(c_1, c_2) := c_2 c_1^{-x}$.

Ce système de chiffrement est correct car si $(c_1, c_2) = (g^r, mh^r)$, $c_1^x = g^{rx} = h^r$ comme dans l'échange de clef Diffie-Hellman. Donc $c_2 c_1^{-x} = mh^r (h^r)^{-1} = m$.

Lien avec l'echange de clé de Diffie-hellman.

On peut montrer que casser la notion de sens unique est équivalent à résoudre un problème calculatoire Diffie-Hellman dans G, en effet (h, c_1, h^r) est un triplet Diffie-Hellman.



Alice

message
crypté

Bob

$K^b_{pub}=(n,g,h)$

$K^b_{pub}=$
(n,g,h)

connait

Scar

message

r tel que 1 <r <n

x tel que 1 <x <n

$K_{priv}= x$

message cripté=$(C_1,C_2)=(g^r,mh^r)$

Decryptage:$c_2 \cdot c_1^{-x}=m$

Preuve de decriptage

- $(C_1, C_2) = (g^r, mh^r)$
- $(C_2), (C_1)^{-x} = (m\, h^r)(g^r)^{-x}$
- $= (mh^r)\ (g^x)^{-r}$
- $= (m\, h^r)\ (h^{-r})$
- $= m\, h^r\, h^{-r}$
- $= m$

Algorithmes de calcul de Diffie-Hellman

Mention breve: Algorithme de Shanks (pas de bébé , pas de geant)

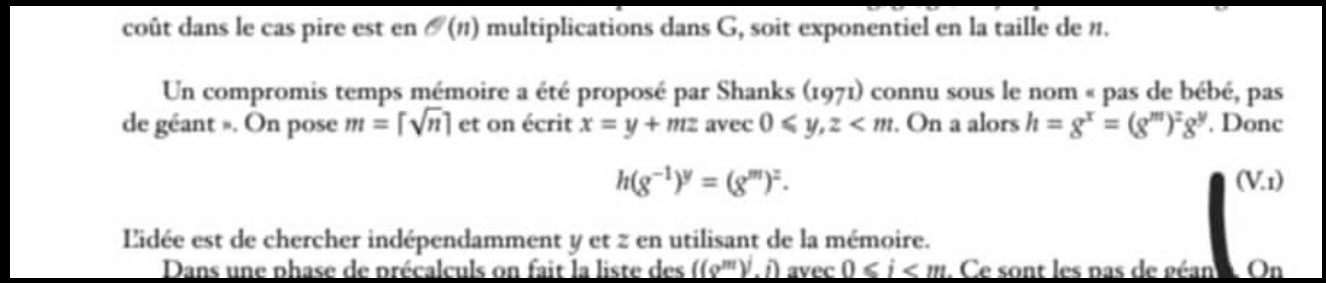
But: resolution du logarithme discret.

Trouver x tel que $g^x = h \bmod p$, où g,h appartiennent à $\mathbb{Z}^*_p$ où p est un nombre premier .

Une amelioration de O(n) multiplication dans G pour la recherche naïve à $O(n^{1/2})$.

Désavantage: utilise beaucoup la memoire .

Solution : methode probabiliste de Pollard(79) utilise trés peu de mémoire.



coût dans le cas pire est en $\mathcal{O}(n)$ multiplications dans G, soit exponentiel en la taille de n.

Un compromis temps mémoire a été proposé par Shanks (1971) connu sous le nom « pas de bébé, pas de géant ». On pose $m = \lceil \sqrt{n} \rceil$ et on écrit $x = y + mz$ avec $0 \leqslant y, z < m$. On a alors $h = g^x = (g^m)^z g^y$. Donc

$$h(g^{-1})^y = (g^m)^z. \quad \text{(V.1)}$$

L'idée est de chercher indépendamment y et z en utilisant de la mémoire.

Dans une phase de précalculs on fait la liste des $((g^m)^j, j)$ avec $0 \leqslant j < m$. Ce sont les pas de géant. On


Merci pour
votre attention