Réponses

Sommaire

Algorithme discret

Définition

G un groupe cyclique d'ordre *n* engendré par *g*. Tous *x* ∈ G peut s'écrire: $x = g^{\alpha}$ avec $0 \leq \alpha < n$ α noté $\log_g(x)$ est le log discret de *x* en base *g*

Si G est un groupe de point appartenant à une courbe élliptique(courbe non singulière), sur un corp fini, le meilleur algorithme pour calculer le logarythme discret est le pgcd étendu.

En résumé le logarythme discret permet de retrouver x dans une équation du type:

$a^x = b \bmod p$

Il est la base de tous les moyens de cryptage à clé publique aujourd'hui utilisé.

Ex1

1. Nous allons détailler le protocole Diffie-Hellman. Il permet d'échanger un clé secrète entre deux personnes sans avoir au préalable de secret en commun. Il repose sur le logarithme discret.

Algo Diffie-Hellman

Pers1 et Pers2 génèrent ensemble deux nombres:

- p (un nombre premier)
- g (un nombre aléatoire < p)

Pers1 choisit un nombre a (aléatoire) et calcule $g^a \bmod p$. Ce qui donne Ax.

Pers2 choisit un nombre b (aléatoire) et calcule $g^b \bmod p$. Ce qui donne By.

Ils échangent alors leurs résultats respectifs.

Pers1 calcule la clé secrète s:

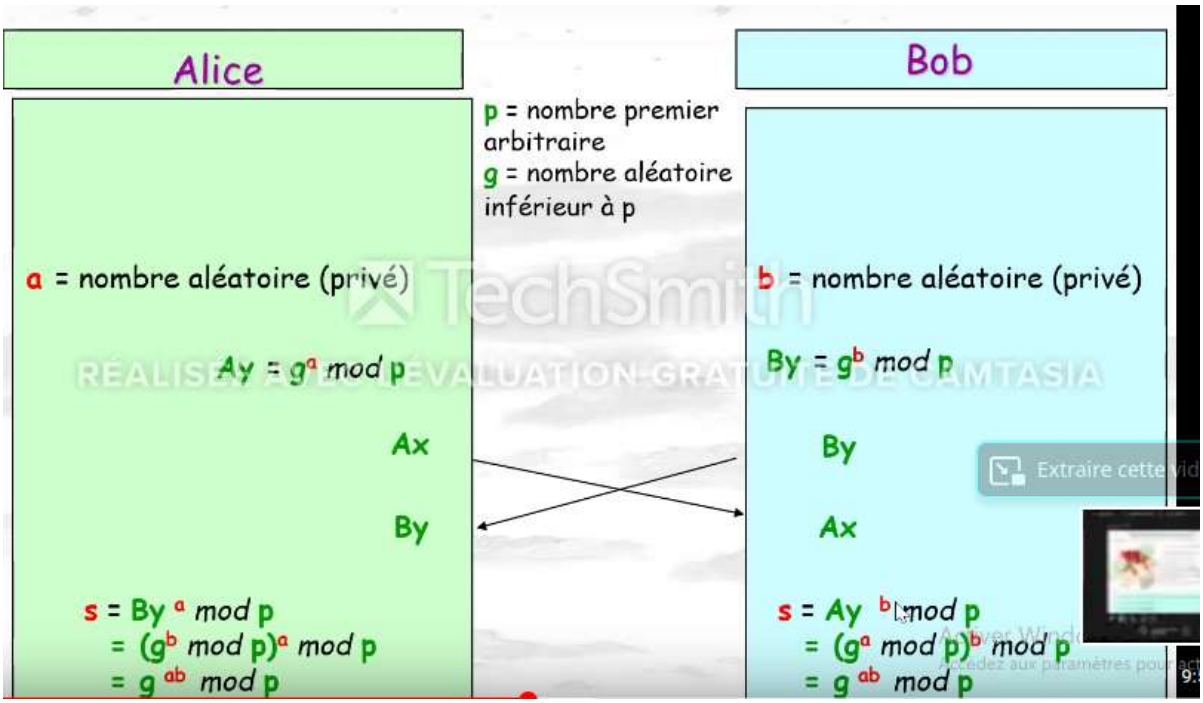
s = $By^a \bmod p$

Ce qui est égale à $(g^{ab}) \bmod p$

Pers2 calcule la clé secrète s:

s = $Ax^b \bmod p$ $(g^{ab}) \bmod p$

Ce qui est égale à $(g^{ab}) \bmod p$



Vulnérabilité

Man in the middle

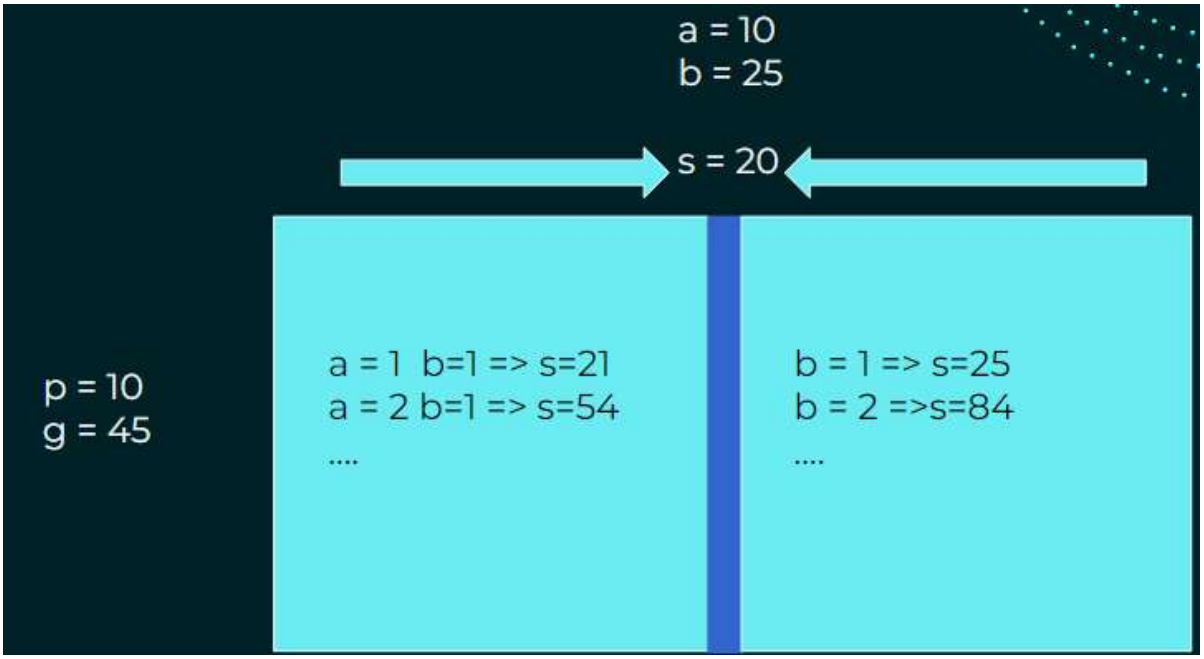
Ce protoole est vulnérable à une attaque man in the middle.
Une personne intersepte le message de Pers1 calcul un By et l'envoie à Pers1 (il se fait passer pour Pers2).
Puis il envoie le message de Pers1 à Pers2 (il se fait passer pour Pers1).
Ils pensent passer directement l'un à l'autre mais en réalité ils passent par l'intermédiaire.

Comme le logarithme discret est difficile à calculer, il est impossible de retrouver a ou b à partir de Ax ou By.

Il partage le problème du logarythme discret:
si on a la valeur de g, p et $g^a \bmod p$ on ne peut pas trouver la valeur de a

---

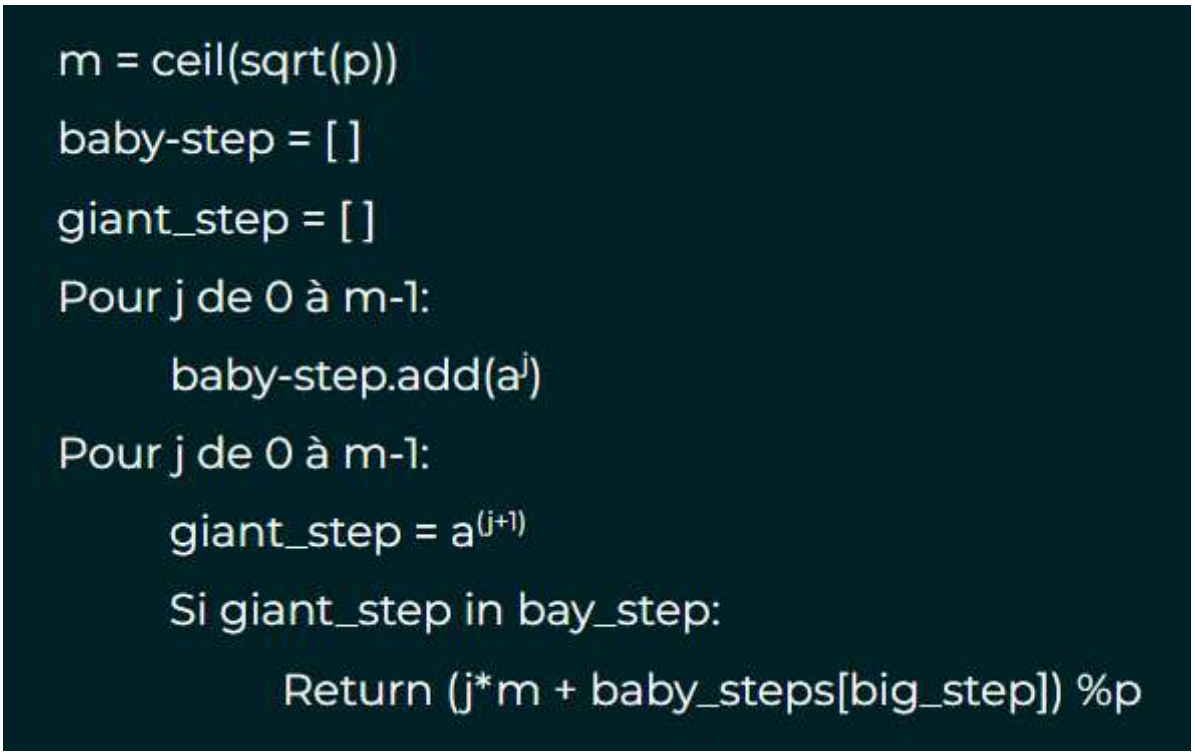
Meet in the middle



Meet int the middle est une attaque qui consiste à chercher les deux clés secrètes en même temps. Deux tableau sont construit: - un avec le calcul avec la clé secrète de Pers1 - un avec le calcul avec la clé secrète de Pers2 Une fois ces deux tableaux construit, on cherche l'intersection et on trouve la clé secrète.

Baby step giant step

Algorithme



Cette attaque est un algorithme de meet in the middle.