Master Eii

Fiche Algorithme de Diffie-Hellman

Alice et **B**ob veulent echanger une clef secrète à utiliser dans un cryptosystème classique.

1. Ils choisissent ensemble un premier p assez grand et un générateur g de $(\mathbb{Z}/p\mathbb{Z})^*$. Ces informations sont *publiques*.
2. Alice choisit au hasard $a \in \{2, \ldots, p-1\}$ et elle calcule $A = g^a$. Alice rend public A.
3. Bob choisit au hasard $b \in \{2, \ldots, p-1\}$ et il calcule $B = g^b$. Bob rend public B.
4. Tous les deux calculent $C = g^{ab} = (g^a)^b = (g^b)^a$, qui sera leur clef secrète.

Dans la communication on a transmis seulement A et B.
Si un intrus,**C**harles veut connaître C, il devrait résoudre le *problème de Diffie-Hellmann*:

$$p \text{ premier, } g \text{ générateur de } (\mathbb{Z}/p\mathbb{Z})^*, g^a, g^b \text{ donnés,}$$
$$\Rightarrow \text{calculer } g^{ab}$$

On conjecture que ce problème est équivalent au problème du logarithme discret:

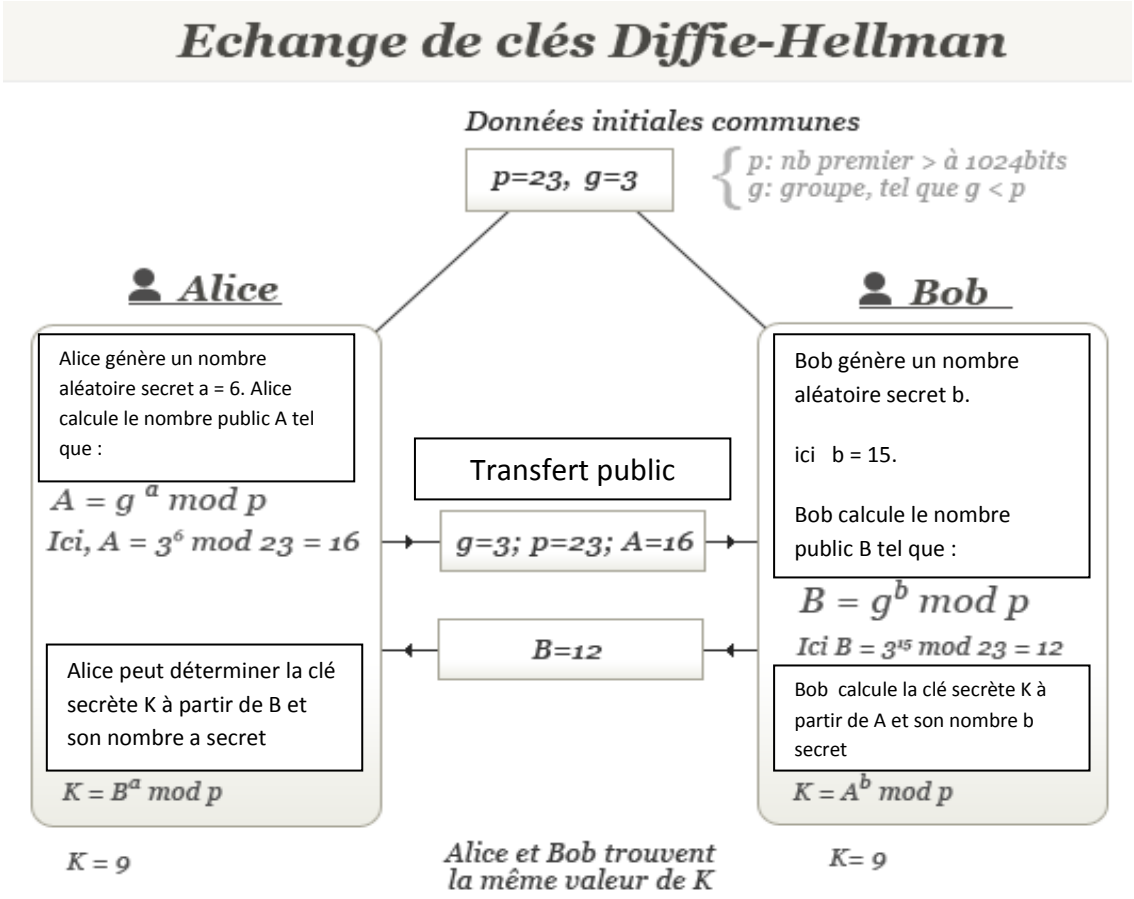
$$p \text{ premier, } g \text{ générateur de } (\mathbb{Z}/p\mathbb{Z})^*, a = g^x \text{ donnés,}$$
$$\Rightarrow \text{calculer } x$$

Pour ce dernier problème on ne connait pas d'algorithme polynomial,

Master Eii

Fiche Algorithme de Diffie-Hellman

APPLICATION 1 :



APPLICATION 2 :

Chez Alice	Publique (internet)	Chez Bob
	On choisit un nombre premier arbitraire commun: p = 419 On choisit un nombre aléatoire commun inférieur à p: g = 7	
Alice choisit un nombre aléatoire secret: Ax = 178		Bob choisit un nombre aléatoire secret: Bx = 344
Ay = 7^{178} modulo 419 = 208		By = 7^{344} modulo 419 = 49
Ay = 208	→	Ay = 208
By = 49	←	By = 49
s = 49^{178} modulo 419 = 107		s = 208^{344} modulo 419 = 107
	← échange de données chiffrées avec s →	