TD8 - Diffie-Hellman

Documentation

Diffie-Hellman est un protocole cryptographique qui permet à deux tiers de générer un secret partagé sans informations préalables l'un sur l'autre. Ce protocole repose essentiellement sur l'échange de valeurs publiques.

Principe de génération de clés de session :

1- p un grand nombre premier ; une base g.

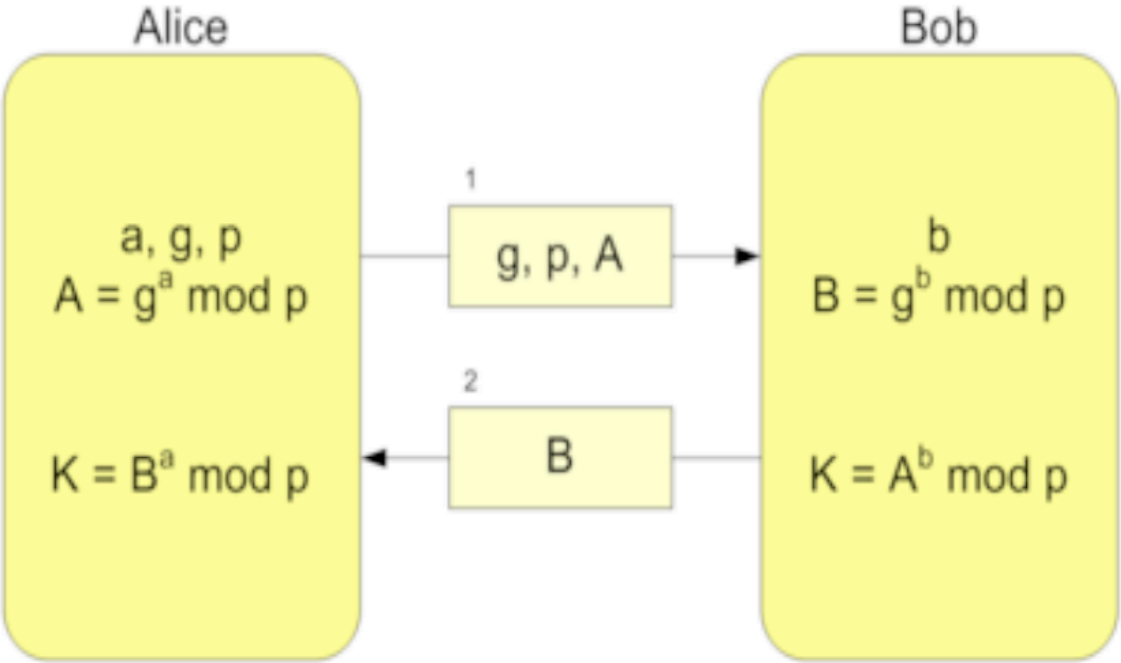
2- Alice choisit a, et calcule A = g^a mod p.

3- Bob choisit b

4- Alice envoie (g,p,A) à Bob.

5 - Bob calcule B = g^b mod p et l'envoi à Alice.

6- Alice calcule K=B^a mod p, et Bon calcule K=A^b mod p.



Exercices

1. Calculer les deux valeurs K en utilisant p=23, g=3, a=6, b=15.
2. Montrez que la valeur K générée par Alice et la même que la valeur K générée par Bob
3. Montrez, à l'aide d'un attaquant C, qu'il est possible de faire une attaque de type «Man-in-the-middle» entre Alice et Bob.
4. Proposez une amélioration de ce protocole permettant d'empêcher ce type d'attaque.
5. Dans quel autre protocole ce protocole est-il utilisé?
6. En utilisant le code client/serveur fourni dans l'archive TD8.tar.bz2 sur le serveur enseignement, implanter le protocole DH. Afficher du coté client et serveur la valeur K obtenu.
7. Utilisez la valeur K obtenue et les fonctions suivantes de la librairie crypt pour implanter un chiffrement symétrique. Vous échangerez alors un message HELLO entre le client et le serveur en vérifiant (avec wireshark) que la communication est bien chiffrée :

```
void des_setparity(char *key);
int ecb_crypt(char *key, char *data, unsigned datalen,
          unsigned mode);
```