

Cryptographie – TD8

Jérémy Briffaut

Jean-Christophe Deneuville

<jeremy.briffaut@insa-cvl.fr>

<jean-christophe.deneuville@insa-cvl.fr>

Lundi 1er octobre 2018

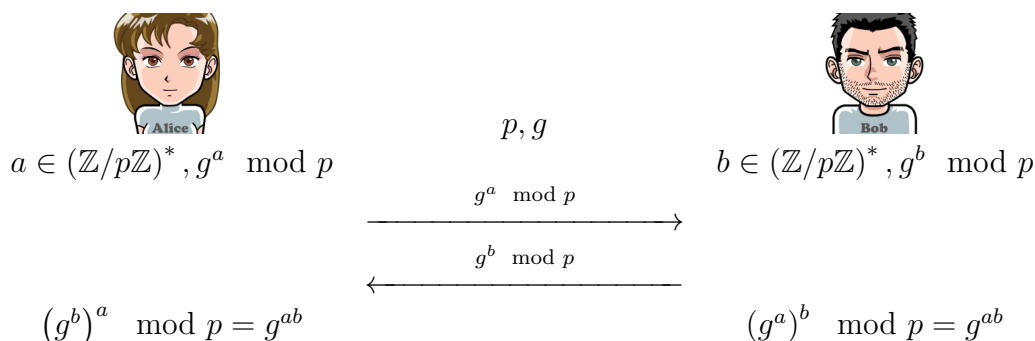
En cas de doute, référez-vous au cours 5, slides 61 à 65.
Téléchargez et décompressez l'archive TD8.zip.

Rappels de cours. 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.

Protocole (simple) de Diffie-Hellman (échange de clé) [1]

Paramètres publics :

- p un (grand) nombre premier
- g un générateur du groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^*$



Exercice 1 Protocole de Diffie-Hellman

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 est la même que la valeur K générée par Bob.
3. Montrez, à l'aide d'un attaquant Charlie, 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.zip sur le serveur enseignement, implanter le protocole DH. Afficher du côté client et serveur la valeur K obtenu.

7. Utilisez la valeur K obtenue et les fonctions suivantes de la librairie cryptographique 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 int datalength, unsigned  
↪ int mode);
```

Exercice 2 Librairie cryptographique

Ajouter la fonction les fonctionnalités de client et serveur à votre bibliothèque.

Exercice 3 Facultatif (bonus)

En utilisant votre réponse à la Question 4, implémentez une solution résistante aux attaques de type MITM.

Références

- [1] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6) :644–654, 1976.