Introduction au Protocole de Diffie-Hellman

Riyad Derguini

22 janvier 2025

Qu'est-ce que le protocole de Diffie-Hellman ?

Le protocole de Diffie-Hellman (DH) est un algorithme cryptographique qui permet à deux parties (par exemple, Alice et Bob) de générer une **clé secrète partagée** sur un canal de communication non sécurisé. Cette clé peut ensuite être utilisée pour chiffrer leurs échanges.

Principe de base

Le protocole repose sur une idée simple mais ingénieuse :

- Alice et Bob se mettent d'accord sur deux nombres publics : un nombre premier p et une base g.
- Chacun génère une **clé privée secrète** (Alice : a, Bob : b).
- Ils calculent leurs **clés publiques** respectives en utilisant g et leurs clés privées, puis les échangent.
- En combinant la clé publique de l'autre avec leur propre clé privée, Alice et Bob obtiennent la **même clé secrète partagée**.

Pourquoi est-ce sécurisé ?

La sécurité du protocole repose sur la difficulté du **problème du logarithme discret** :

- Il est facile de calculer $g^a \mod p$ à partir de a, mais il est très difficile de retrouver a à partir de $g^a \mod p$.
- Même si un attaquant intercepte les clés publiques, il ne peut pas calculer la clé secrète partagée sans connaître les clés privées.

Applications

Le protocole de Diffie-Hellman est utilisé dans de nombreux systèmes de sécurité, notamment :

— **SSH** : Pour établir des connexions sécurisées.
— **TLS/SSL** : Pour sécuriser les communications sur Internet (HTTPS).
— **VPN** : Pour chiffrer les échanges entre un utilisateur et un réseau privé.

Illustration du protocole

Voici un schéma simplifié pour mieux comprendre le protocole de Diffie-Hellman :

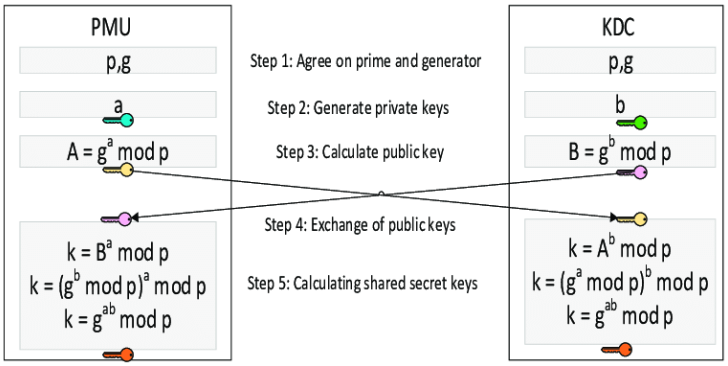

FIGURE 1 – Illustration du protocole de Diffie-Hellman