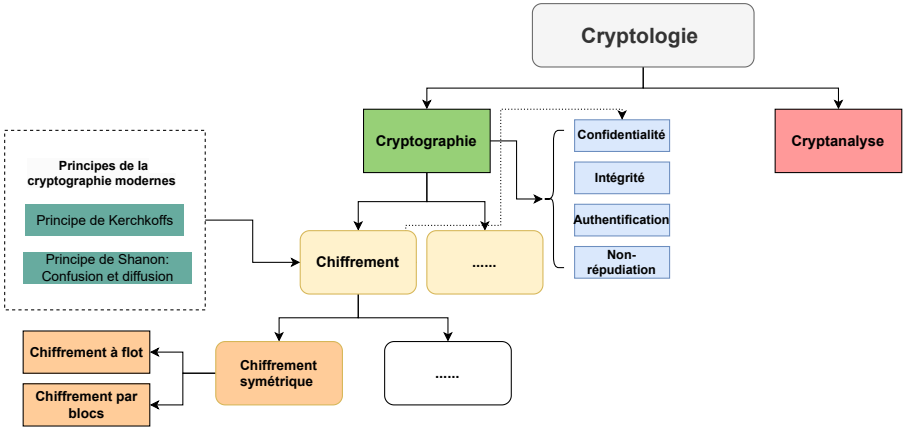
Initiation à la Cryptographie

Échange de clés Diffie-Hellman

February 24, 2025

Awaleh HOUSSEIN

Recap de deux posts précédents [1] [2]



[1] Premier post: https://www.linkedin.com/feed/update/urn:li:activity:7284685244455157761/

[2] Deuxième post: https://www.linkedin.com/feed/update/urn:li:activity:7292307076343578624/

Limitations des chiffrements symétriques

Rappel du chiffrement symétrique

- Efficace, rapide, idéal pour chiffrer de grandes quantités de données.
- Les deux parties doivent au préalable partager un **secret commun**, appelé **clé secrète**, pour chiffrer et déchiffrer les messages.

Problème: Comment partager cette clé secrète en toute sécurité ?

- **Transmettre la clé physiquement** (par courrier, en personne, etc.).
  - *Problème :* Si on peut transmettre la clé en sécurité, pourquoi ne pas transmettre directement le message ?
- **Sur un réseau non sécurisé ?** Transmettre la clé par internet ou par téléphone.
  - *Problème :* Risque d'interception par un tiers malveillant.

L’échange de clés Diffie-Hellman (1976)

Face aux limitations du partage de clés dans le chiffrement symétrique, une solution révolutionnaire a vu le jour en 1976 :

- **La révolution Diffie-Hellman :**
  - Whitfield Diffie et Martin E. Hellman publient un article intitulé *”New Directions in Cryptography”*[3].
  - Ils proposent une méthode entièrement nouvelle pour résoudre un problème fondamental : **l’échange de clé sécrète**.

- Cette méthode, appelée **échange de clés Diffie-Hellman**, permet à deux parties de générer une clé secrète commune **sans jamais l’échanger directement**.

[3] Whitfield Diffie and Martin E Hellman (1976). “New directions in cryptography”. In: Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman, pp. 365–390.

Pourquoi est-ce révolutionnaire ?

Une contribution majeure en cryptographie moderne

- **Avant Diffie-Hellman (1976) :**
  - Partage de clés nécessitant une transmission physique (risquée).
  - Confiance obligatoire dans un canal déjà sécurisé (rare sur internet).
- **Après Diffie-Hellman :**
  - Création d'un secret commun **sans contact préalable**.
  - Sécurité même sur des réseaux publics (ex : Wi-Fi, internet).
- **Prix et reconnaissance:**
  - L'article[4] est l'un des plus cités en informatique (24 000+ citations).
  - Prix Turing 2015 (équivalent du "Prix Nobel" en informatique) pour Diffie et Hellman.

[4] Whitfield Diffie and Martin E Hellman (1976). "New directions in cryptography". In: Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman, pp. 365–390.

Fonctionnement de l'échange de clés Diffie-Hellman (1/2)

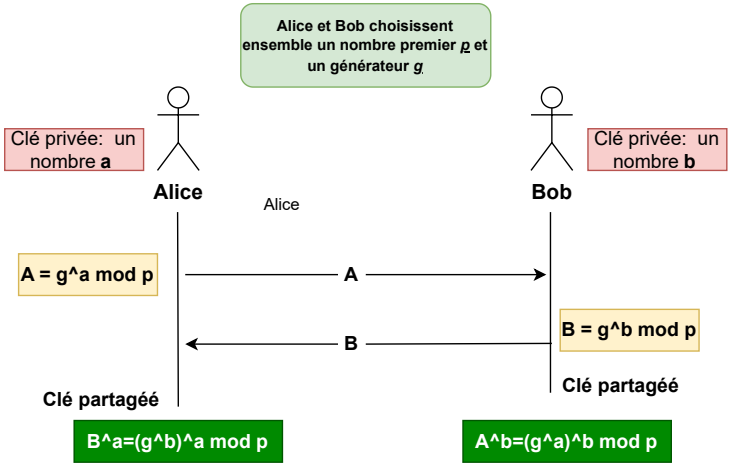
Étapes :

1. Alice et Bob choisissent ensemble :
   - Un nombre premier p.
   - Un générateur g du groupe multiplicatif $\mathbb{Z}/p\mathbb{Z}$.
2. Alice :
   - Choisit un nombre secret a.
   - Calcule $A = g^a \mod p$ et envoie A à Bob.
3. Bob :
   - Choisit un nombre secret b.
   - Calcule $B = g^b \mod p$ et envoie B à Alice.
4. Alice calcule la clé secrète : $K = B^a \mod p = (g^b)^a \mod p = g^{ab} \mod p$.
5. Bob calcule la clé secrète : $K = A^b \mod p = (g^a)^b \mod p = g^{ab} \mod p$.

Résultat :

Alice et Bob obtiennent la même clé secrète $K = g^{ab} \mod p$, sans jamais l'avoir échangée directement.

Fonctionnement de l'échange de clés Diffie-Hellman (2/2)



Fondements mathématiques et sécurité de Diffie-Hellman

Base mathématique

- Nombre premier p
- Opérations ($\times$, puissances) effectuées modulo p.
- Commutativité : $(g^b)^a = g^{ab} = (g^a)^b$.

Sécurité Problème du logarithme discret[a] :

- Calculer a depuis $g^a \mod p$
- Impossible en temps raisonnable.

[a] Vulnérable aux attaques quantiques (à détailler ultérieurement)

Exigences pratiques :

- p doit être grand (ex : 2048 bits, 600 chiffres).
- Renouvellement régulier p.
- Garantir que le logarithme discret reste insoluble en pratique. .

Vulnerable face à l'attaque de l'homme du milieu

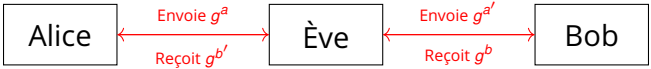


Figure: Ève intercepte/modifie les échanges entre Alice et Bob.

Déroulé de l'attaque

1. Ève intercepte g^a et g^b, les remplace par $g^{a'}$ et $g^{b'}$.
2. Alice calcule $K_1 = g^{ab'}$, Bob calcule $K_2 = g^{a'b}$.
3. Ève connaît K_1 et $K_2 \rightarrow$ Elle déchiffre/modifie tous les messages

Comment se protéger à l'attaque de l'homme du milieu ? (1/2)

1. Vérifier les identités

- Utiliser des **certificats numérique** (comme une carte d'identité numérique).
- Une organisation de confiance (ex : banque, état) garantit qu'Alice et Bob sont bien ceux qu'ils prétendent être.

→ *L'attaquant ne peut plus se faire passer pour eux.*

2. Signature numérique des échanges

- Alice et Bob ajoutent une **signature unique** à leurs messages.
- Analogie : Comme un tampon officiel sur un document important.

→ *L'attaquant ne peut pas falsifier les messages.*

Comment se protéger à l'attaque de l'homme du milieu ? (2/2)

3. Vérification finale de la clé

- Après l'échange, Alice et Bob comparent un code secret (ex : via un canal sécurisé).
- Si les codes ne correspondent pas : alerte d'une attaque !

→ *Une dernière vérification pour confirmer la sécurité.*

Résultat:

- Alice et Bob savent qu'ils communiquent entre eux.

  → *L'attaquant ne peut plus intercepter ou modifier les messages.*

Applications concrètes de Diffie-Hellman

Où utilise-t-on Diffie-Hellman ?

- **Échange de clés sécurisé** : Protocole TLS/SSL (cadenas HTTPS)[5].
- **Réseaux Privés** : VPNs (IPsec, OpenVPN)
- **Messagerie** : WhatsApp, Signal (établissement de clé E2EE) [6].
- **Wi-Fi Sécurisé** : Protocoles WPA2/WPA3 [7].
- **Accès distant** : Connexions SSH.

Pourquoi Diffie-Hellman ?

- Permet un échange de clé **sans contact préalable**
- Résistant à l'écoute passive (logarithme discret).

[5] RFC standard `https://www.rfc-editor.org/rfc/rfc5246#section-7.4.3`

[6] `https://dev.to/prismlabsdev/the-core-of-whatapp-and-signal-diffie-hellman-key-exchange-50fd`

[7] Pour plus de détails `https://wirelessgnan.wordpress.com/2020/08/31/keys-to-understanding-wpa3-sae-diffie-hellman-key-exchange-elliptic-curve-cryptography-and-dragonfly-key-exchange/`

À retenir

Chiffrement symétrique : Avantages & Limites

- **Forces** : Rapide - Idéal pour chiffrer gros volumes de données.
- **Faiblesse** : Probléme de partage de la clé secrète

Solution : Diffie-Hellman (1976) :

1. Alice et Bob choisissent un nombre **premier** p et un **générateur** g, qui sont publics.
2. Alice $\rightarrow$ Bob : $A = g^a \mod p$ (a secret).
3. Bob $\rightarrow$ Alice : $B = g^b \mod p$ (b secret).
4. Clé commune : $K = B^a = A^b = g^{ab} \mod p$

Résumé

- Échange de clés de Diffie-Hellman résout le problème du **partage de clés**.
- Sécurité basée sur le problème du **logarithme discret**.
- Nécessite **authentification** pour contourner *l'attaque du l'homme du milieu*.