HAI709I - Fondements cryptographiques pour la sécurité

Cours 9 - Échange de clés et révolution de la clé publique

Rocco Mora

24 Novembre, 2025

Université de Montpellier – Faculté des Sciences
M1 informatique, parcours Algo, IASD, Imagine

Distribution des clés et problèmes connexes

Cryptographie à clé privée : garantir la confidentialité et l'intégrité pour deux parties communiquant via un canal non sécurisé, en supposant qu'elles partagent une clé secrète.

Comment partager la clé secrète au départ ?

Le recours à un canal sécurisé pour distribuer les clés présente des limites :

Scénario 1 : dans une grande entreprise, chaque paire d'employés doit communiquer de manière sécurisée

$\longrightarrow$ difficile de partager une clé entre deux employés situés dans des villes différentes

$\longrightarrow$ pour chaque nouveau employé, une clé pour tout autre employé doit être partagée

$\longrightarrow$ s'il y a N employés, chaque employé doit gérer et stocker $N - 1$ clés

$\longrightarrow$ quelques clés peuvent être stockées sur un hardware sécurisé (par exemple, une carte à puce), plus difficile s'il y a un grand nombre de clés

Distribution des clés et problèmes connexes

Cryptographie à clé privée : garantir la confidentialité et l'intégrité pour deux parties communiquant via un canal non sécurisé, en supposant qu'elles partagent une clé secrète.

Comment partager la clé secrète au départ ?

Le recours à un canal sécurisé pour distribuer les clés présente des limites :

Scénario 2 : Dans les systèmes ouverts (achats sur Internet, e-mails), les canaux sécurisés ne sont pas du tout possibles.

Résumé des problèmatiques :

1. **Distribution des clés**
2. **Stockage et gestion des clés**
3. **Inapplicabilité** de la cryptographie à clé privée **aux systèmes ouverts**

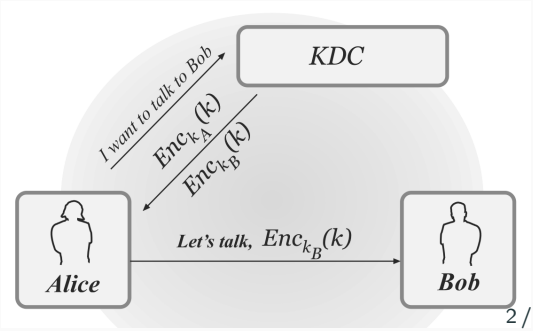
Centre de distribution des clés (KDC)

Centre de distribution des clés : [🇬🇧 Key-distribution center (KDC)]

entité à laquelle tout le monde fait confiance (par exemple, l'administrateur système d'une grande entreprise) qui aide toutes les parties à partager des clés

$\longrightarrow$ lorsqu'une nouvelle partie rejoint le réseau, le KDC partage une clé avec elle. Ensuite, le KDC génère une clé pour chaque ancienne partie et les partage.

Cela peut être fait en ligne/à la demande : le KDC partage une clé secrète avec chaque partie. Si Alice souhaite communiquer avec Bob, elle envoie un message authentifié au KDC. Le KDC échantillonne une clé de session aléatoire et la partage avec Alice et Bob, en la chiffrant avec les clés secrètes correspondantes pour Alice et Bob.



Avantages et inconvénients d'un KDC

+ Chaque partie n'a besoin de stocker qu'une seule clé à long terme. Seul le KDC stocke de nombreuses clés et doit être conservé dans un endroit sécurisé et bénéficier de la meilleure protection possible contre les attaques réseau
+ Lorsqu'une nouvelle partie rejoint le réseau, les anciennes parties n'ont pas besoin de configurer une nouvelle clé, seule la KDC doit le faire.
− Une attaque contre la KDC compromet complètement le système
− si la KDC est hors service, les communications sécurisées sont temporairement impossibles

De nombreux protocoles utilisent en pratique le KDC pour la distribution sécurisée des clés, par exemple le **protocole Needham-Schroeder** au cœur de **Kerberos**

→ problèmes supplémentaires lorsque l'attaquant n'est pas seulement un espion, mais peut interférer activement avec le protocole

La révolution de la cryptographie à clé publique

Whitfield Diffie et **Martin Hellman** ont observé en 1976 que les phénomènes asymétriques peuvent être utilisés pour dériver des protocoles interactifs pour un échange de clés sûr sur un canal non sécurisé.

644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

***Abstract*—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to**

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by send-

Protocole d'échange de clés

Contexte : Alice et Bob exécutent un protocole proba. Π et produisent deux clés k_A, k_B

$\longrightarrow$ **Propriété de correction :** $k = k_A = k_B$

Expérience d'échange de clés $\mathtt{KE}^{eav}_{\mathcal{A},\Pi}(n)$

1. 2 parties qui connaissent 1^n exécutent le protocole Π. Les messages envoyés par les 2 parties sont contenus dans une transcription $\mathtt{tr}$. Chaque partie génère une clé k.
2. Un bit uniforme b est choisi. Si $b = 0$, on fixe $\bar{k} = k$, sinon $\bar{k} \in \{0,1\}^n$ est choisi uniformément au hasard.
3. $\mathcal{A}$ reçoit $\mathtt{tr}$ et $\bar{k}$, et produit un bit b'.
4. Le résultat de l'expérience est 1 ($\mathcal{A}$ réussit) si $b' = b$, 0 sinon.

Sécurité EAV

Un protocole d'échange de clés Π est EAV-sûr si, pour tous les PPT $\mathcal{A}$, il existe une fonction négligeable $\mathtt{negl}$ telle que

$$\Pr(\mathtt{KE}^{eav}_{\mathcal{A},\Pi}(n) = 1) \leq \frac{1}{2} + \mathtt{negl}(n).$$

Le protocole d'échange de clés de Diffie-Hellman

Soit $\mathcal{G}$ un algorithme de génération de groupe en temps polynomial.

Protocole d'échange de clés de Diffie-Hellman

Entrée commune : le paramètre de sécurité 1^n.

Le protocole :

1. Alice obtient $(\mathbb{G}, q, g)$ à partir de $\mathcal{G}(1^n)$.
2. Alice choisit un $x \in \mathbb{Z}_q$ uniforme et calcule $h_A := g^x$.
3. Alice envoie $(\mathbb{G}, q, g, h_A)$ à Bob.
4. Bob reçoit $(\mathbb{G}, q, g, h_A)$. Il choisit un nombre uniforme $y \in \mathbb{Z}_q$ et calcule $h_B := g^y$. Bob envoie h_B à Alice et génère la clé $k_B := h_A^y$. Alice reçoit h_B et génère $k_A := h_B^x$.

Vérification de la propriété de correction :

$$k_B = h_A^y = (g^x)^y = g^{xy} = (g^y)^x = h_B^x = k_A.$$

Hypothèse calculatoire correspondante

Quelle hypothèse de dureté est nécessaire pour le protocole d'échange de clés Diffie-Hellman ?

- **Logarithme discret :** si $\mathcal{A}$ peut le casser, il peut calculer x à partir de h_A, puis $k = k_A = h_B^x$. Mais il existe peut-être d'autres moyens d'obtenir k sans calculer explicitement x ou y.
  $\rightarrow$ nécessaire mais non suffisant
- **CDH :** La clé est exactement $\mathtt{DH}_g(h_A, h_B)$. Mais peut-être que $\mathcal{A}$ peut distinguer sans trouver la clé.
  $\rightarrow$ nécessaire mais non suffisant
- **DDH :** g^{xy} devrait être impossible à distinguer d'un élément uniforme, étant donné g, g^x, g^y.
  $\rightarrow$ nécessaire et suffisant

Théorème

Si le problème DDH est difficile par rapport à $\mathcal{G}$, alors le protocole d'échange de clés de Diffie-Hellman Π est EAV-sûr.

⚠Pour simplifier, nous prouvons l'indistinguabilité par rapport à un élément uniforme du groupe plutôt que par rapport à une chaîne de bits uniforme.

Preuve. Puisque $\Pr(b=0) = \Pr(b=1) = 1/2$, nous avons

$$\begin{aligned}
\Pr(\mathtt{KE}^{eav}_{\mathcal{A},\Pi}(n)=1) &= \frac{1}{2}\Pr(\mathtt{KE}^{eav}_{\mathcal{A},\Pi}(n)=1 \mid b=0) + \frac{1}{2}\Pr(\mathtt{KE}^{eav}_{\mathcal{A},\Pi}(n)=1 \mid b=1) \\
&= \frac{1}{2}\Pr(\mathcal{A}(\mathbb{G},q,g,g^x,g^y,g^{xy})=0) + \frac{1}{2}\Pr(\mathcal{A}(\mathbb{G},q,g,g^x,g^y,g^z)=1) \\
&= \frac{1}{2}\left(1-\Pr(\mathcal{A}(\mathbb{G},q,g,g^x,g^y,g^{xy})=1)\right) + \frac{1}{2}\Pr(\mathcal{A}(\mathbb{G},q,g,g^x,g^y,g^z)=1) \\
&= \frac{1}{2} + \frac{1}{2}\Pr(\mathcal{A}(\mathbb{G},q,g,g^x,g^y,g^z)=1) - \frac{1}{2}\Pr(\mathcal{A}(\mathbb{G},q,g,g^x,g^y,g^{xy})=1) \\
&\leq \frac{1}{2} + \left|\frac{1}{2}\left(\Pr(\mathcal{A}(\mathbb{G},q,g,g^x,g^y,g^z)=1)\right) - \frac{1}{2}\Pr(\mathcal{A}(\mathbb{G},q,g,g^x,g^y,g^{xy})=1)\right| \\
&\leq \frac{1}{2} + \mathtt{negl}(n).
\end{aligned}$$

□

Attaquants actifs

Nous avons uniquement prouvé la sécurité contre un espion, c'est-à-dire un attaquant passif.

Un adversaire actif (attaque man-in-the-middle) peut exécuter (honnêtement) le protocole avec Alice et Bob, obtenant respectivement k_A et k_B.

$\longrightarrow$ Alice et Bob ne peuvent pas détecter l'attaque.

$\Downarrow$

Forme de base du protocole Diffie-Hellman non utilisé dans la pratique

- Importance théorique : premier exemple où les techniques asymétriques et la théorie des nombres peuvent être utilisées pour surmonter les problèmes de distribution des clés.
- Le protocole de Diffie-Hellman est au cœur des protocoles standardisés d'échange de clés résistants aux attaques de type "man-in-the-middle", comme dans TLS.

Cryptographie à clé publique/asymétrique

Notion de **cryptographie à clé publique** introduite aussi par Diffie et Hellman :

Une partie qui souhaite communiquer en toute sécurité génère une paire de clés

1. une clé publique, qui est largement diffusée
2. une clé privée, qui est gardée secrète

Chiffrement à clé publique

- clé publique utilisée comme clé de chiffrement par une autre partie
- clé privée utilisée comme clé de déchiffrement par son propriétaire

Signature numérique

- clé publique utilisée comme clé d'authentification par une autre partie
- clé privée utilisée comme clé de vérification par son propriétaire

	Cryptographie à clé privée	**Cryptographie à clé publique**
Confidentialité	Chiffrement à clé privée	Chiffrement à clé publique
Authentification	MAC	Signature numérique