Cours 7. Échange de clefs

HAI709I – Cryptographie

Bruno Grenet

Université de Montpellier – Faculté des Sciences

Introduction

Cryptographie basée sur des clefs

- Clef pour chiffrer / déchiffrer
- Clef pour authentifier / vérifier
- Clef pour hacher

Comment deux participant·e·s font-ils pour avoir une clef commune ?

Mauvaise solution

- Tout couple de participant·e·s partagent une clef commune
  - Si N participant·e·s, il faut N^2 clefs !
  - Pour partager une clef, les participant·e·s doivent se rencontrer

Une solution possible : les centres de distribution de clefs (KDC)

Idée

- Chaque participant·e possède une clef (secrète) en commun avec le KDC
- Si Alice veut parler à Bob :
  - Alice obtient une *clef de session* k chiffrée : $\mathrm{Enc}_{k_a}(k)$
  - Bob obtient la même clef temporaire chiffrée : $\mathrm{Enc}_{k_b}(k)$
  - Alice et Bob déchiffrent k puis l'utilisent pour communiquer

Avantages

- Chaque participant·e ne retient (sur le long terme) qu'une clef
- Chaque participant·e n'a besoin de rencontrer que le KDC, une seule fois

Inconvénients

- Le KDC est le point central de sécurité :
  - S'il est attaqué, toute la sécurité tombe
  - S'il est en panne, aucune communication n'est possible
- Ne fonctionne pas en *système ouvert* type Internet

La *bonne* solution : l'échange de clefs

Permettre à deux participant·e·s de se mettre d'accord sur une clef, à distance

Objectif

- Alice et Bob échangent des messages
- À la fin de l'échange, ils connaissent tous les deux une même clef k
- Un attaquant qui voit tous les messages n'a aucune information sur k

Est-ce que c'est possible ?

- L'attaquant voit autant qu'Alice et Bob ?
- Aucune information $\rightarrow$ sécurité calculatoire

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

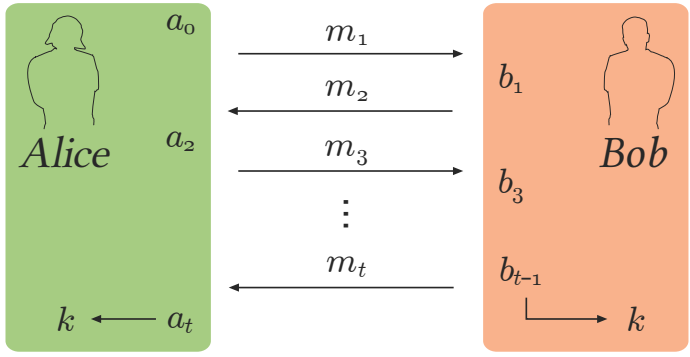
***Abstract*—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This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

I. Introduction

WE STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of me-

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 sending the key in advance over some secure channel such as private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.

Définition d'un protocole



Protocole d'échange de clef

- Public : messages $m_1, \ldots, m_t$; espace des clefs $\mathcal{K}$
- Privé : les a_i connus seulement d'Alice, les b_i seulement de Bob
- Protocole correct si Alice et Bob calculent la même clef $k \in \mathcal{K}$

Sécurité d'un protocole

Protocole d'échange de clefs sûr : étant donné $m_1, \ldots, m_t$, il est difficile de calculer k

Expérience d'échange de clefs

1. Simulation du protocole $\rightarrow$ messages $m_1, \ldots, m_t$ et clef $k \in \mathcal{K}$
2. Protocole : tire un bit b uniforme et renvoie $\hat{k} = k$ si $b = 1$ et $\hat{k}$ uniforme dans $\mathcal{K}$ sinon
3. Attaquant : étant donné $m_1, \ldots, m_t$ et $\hat{k}$, renvoie un bit b'

Succès de l'attaquant si $b' = b$

Définition

Un protocole d'échange de clef est sûr en présence d'une oreille indiscrète (EAV-sûr) si pour tout APP, $\Pr[b' = b] \leq \frac{1}{2} + \text{negl}(n)$

- $n = \log|\mathcal{K}|$
- APP : polynomial en n

1. Protocoles d'échange de clefs

2. Groupes cycliques et logarithme discret

3. Protocole de Diffie-Hellman

Groupes cycliques – générateurs

Rappel : sous-groupe engendré

Soit G un groupe (multiplicatif, fini) et $x \in G$. Le sous-groupe engendré par x est $G_x = \{x^n : n \geq 0\}$

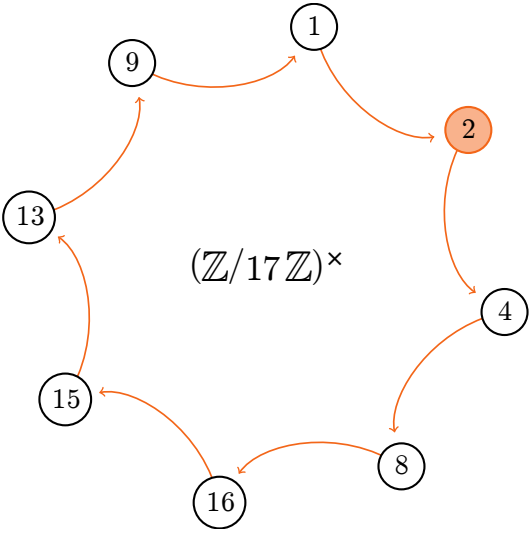
Définitions

- Un groupe G (multiplicatif, fini) est **cyclique** s'il existe x tel que $G_x = G$
- L'élément x est un **générateur** de G

Remarques

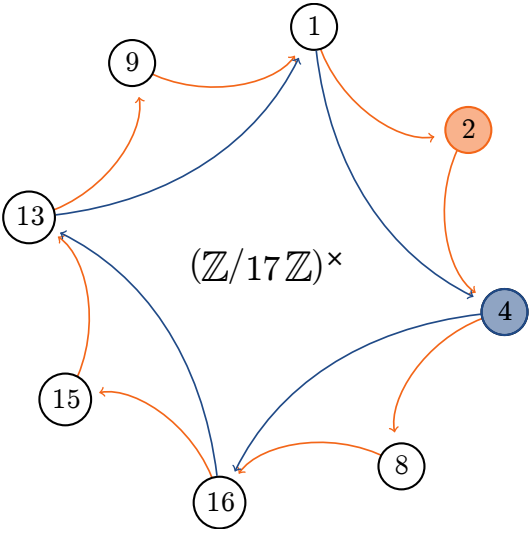
- x est un générateur de $G \iff$ l'ordre de x est $|G|$
- Pour tout x, G_x est un groupe cyclique, de générateur x
- Si p est premier $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p-1$ *admis*
- En général, $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique

Exemple



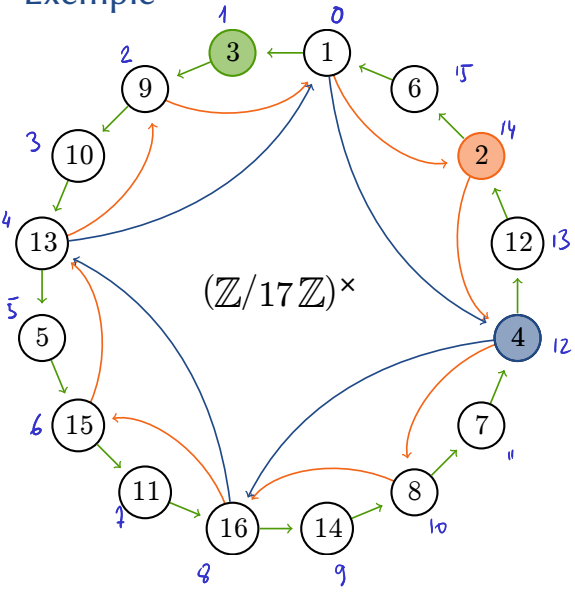
- 2 est d'ordre 8

Exemple



- 2 est d'ordre 8
- 4 est d'ordre 4

Exemple



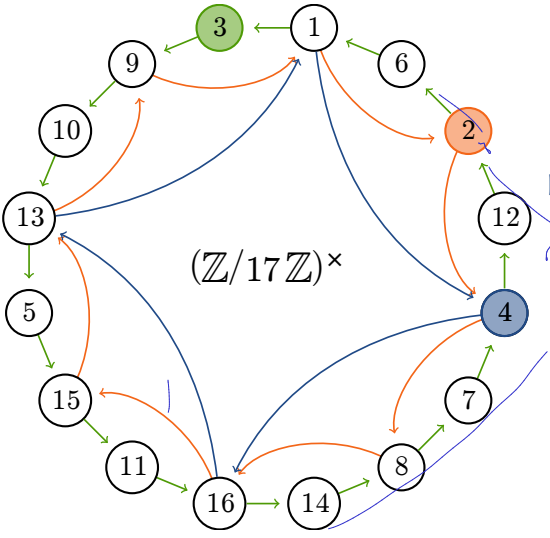
- 2 est d'ordre 8
- 4 est d'ordre 4
- 3 est d'ordre 16 $\rightarrow$ générateur

Bijection

$i \longleftrightarrow 3^i$

$(\mathbb{Z}/16\mathbb{Z}, +)$ $(\mathbb{Z}/17\mathbb{Z}^\times, \times)$

Exemple



- 2 est d'ordre 8
- 4 est d'ordre 4
- 3 est d'ordre 16 $\rightarrow$ générateur

Remarques

- Si G est cyclique, il possède plusieurs générateurs
  - g générateur $\Rightarrow g^{-1}$ générateur
  - Si $|G|$ est premier, tous les éléments $\neq 1$ sont générateurs
- Si g est générateur et k divise $|G|$, g^k est d'ordre $|G|/k$

Problème du logarithme discret

Propriété

- Soit G un groupe cyclique et g un générateur : pour tout $x \in G$, $\exists t$, $x = g^t$
- On peut fixer $0 \leq t < |G| \rightarrow t$ est unique
- $G = \{g^0, g^1, \ldots, g^{|G|-1}\}$

Définition

Le logarithme discret de x en base g est l'unique $t \in \{0, \ldots, |G| - 1\}$ tel que $x = g^t$

Le problème algorithmique

Entrée : Un groupe cyclique G avec un générateur g, et $x \in G$
Sortie : Le logarithme discret t de x en base g

$\mathbb{Z}/12\mathbb{Z}^\times \rightarrow$ 9 $\rightsquigarrow$ 2
3 12 $\rightsquigarrow$?13

Résolution du logarithme discret

Algorithme naïf

- Étant donné g et x, calculer $g^0, g^1, g^2, \ldots$ jusqu'à tomber sur $g^t = x$
- Complexité $O(t) = O(|G|)$ opérations dans G

Cas du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$

- Générateur g tel que $\text{PGCD}(g, n) = 1$ *dont* 1
- *Logarithme discret* de x en base g : entier t tel que $x = t \cdot g \bmod n$
- Algorithme : Inverser g *modulo* n et multiplier x par $g^{-1} \to O(\log^2 n) = O(\log^2 |G|)$

Quelques autres algorithmes

- « *Pas de bébé, pas de géant* » en $O(\sqrt{|G|})$ *cf* TD
- Pollig-Hellman : si p est le plus grand facteur premier de $|G| \to O(\sqrt{p})$
- Techniques de crible pour $((\mathbb{Z}/p\mathbb{Z})^\times, \times)$: $2^{O((\log p)^{\frac{1}{3}} (\log \log p)^{\frac{2}{3}})}$

Algorithmes, complexités et records de calculs *relativement* similaire à la factorisation

Hypothèses de difficulté

Hypothèse du logarithme discret pour le groupe G

Expérience : l'attaquant a accès à g, $x \in G$, et renvoie $t \in \{0, \dots, |G| - 1\}$
Succès de l'attaquant si $g^t = x$
Hypothèse : la probabilité de succès de tout APP est $\leq \mathrm{negl}(\log |G|)$

Hypothèse de Diffie-Hellman calculatoire (CDH) pour le groupe G

Expérience : l'attaquant a accès à g, x_1, $x_2 \in G$, et renvoie $y \in G$
Succès de l'attaquant si $y = g^{t_1 t_2}$ où $x_1 = g^{t_1}$ et $x_2 = g^{t_2}$
Hypothèse : la probabilité de succès de tout APP est $\leq \mathrm{negl}(\log |G|)$

Remarques

- APP : temps polynomial en $O(\log |G|)$
- CDH pour $G \Rightarrow$ Hyp. de log. discret pour G *cf contraposée*
- Hypothèses fausses pour $(\mathbb{Z}/n\mathbb{Z}, +)$ par exemple !
- $g^{t_1 t_2} = (g^{t_1})^{t_2} = (g^{t_2})^{t_1} \neq g^{t_1} g^{t_2}$

L'hypothèse de Diffie-Hellman *décisionnelle* (DDH)

Expérience de Diffie-Hellman pour le groupe G

1. Protocole :
   i. $k_1, k_2 \leftarrow_R \{0, \ldots, |G| - 1\}$
   ii. $(x_1, x_2, y) \leftarrow (g^{k_1}, g^{k_2}, g^{k_1 k_2})$ où $g =$ générateur de G
   iii. $b \leftarrow_R \{0, 1\}$
   iv. Si $b = 1 : \hat{y} \leftarrow y$
   v. Sinon : $\hat{y} \leftarrow_R G$
2. Attaquant : étant donné G, g, x_1, x_2 et $\hat{y}$, renvoie b'

Succès de l'attaquant si $b = b'$

Hypothèse DDH pour G

Pour tout APP, $\Pr[b = b'] \leq \frac{1}{2} + \text{negl}(\log |G|)$

Lien avec les autres hypothèses

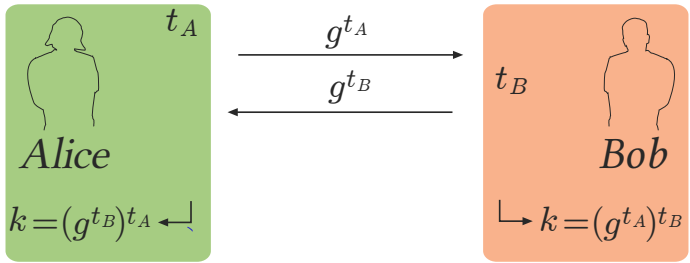
- Pour chaque G, DDH $\Rightarrow$ CDH $\Rightarrow$ logarithme discret

1. Protocoles d'échange de clefs

2. Groupes cycliques et logarithme discret

3. Protocole de Diffie-Hellman

Le protocole



Protocole de Diffie-Hellman

Entrée : Groupe G et générateur $g \in G$

1. Alice tire t_A uniformément dans $\{0, \ldots, |G| - 1\}$, calcule $h_A = g^{t_A}$ et envoie h_A à Bob
2. Bob tire t_B uniformément dans $\{0, \ldots, |G| - 1\}$, calcule $h_B = g^{t_B}$ et envoie h_B à Alice
3. Alice calcule $k_A = h_B^{t_A}$ et Bob calcule $k_B = h_A^{t_B}$

Propriété

Le protocole est correct : $k_A = (g^{t_B})^{t_A} = g^{t_A t_B} = (g^{t_A})^{t_B} = k_B$

Librement inspiré de : J. Katz, Y. Lindell. Introduction to modern cryptography. 3rd ed, CRC Press, 2021.

Sécurité du protocole de Diffie-Hellman

Théorème

Si l'hypothèse DDH est vérifiée pour G, alors le protocole de Diffie-Hellman est EAV-sûr

L'hypothèse DDH est exactement la définition d'EAV-sécurité spécialisée pour le protocole de Diffie-Hellman.

Remarques finales

50 nuances de Diffie-Hellman

- Le protocole DH est essentiellement le seul protocole d'échange de clefs
- Mais nombreux choix de groupe cyclique G : $(\mathbb{Z}/p\mathbb{Z})^\times$, courbe elliptique, isogénies

Vulnérabilité : attaque de l'« homme du milieu » (*man in the middle*)

- Charlie se place entre Alice et Bob
- Alice échange une clef k_A avec Charlie, croyant discuter avec Bob
- Bob échange une clef k_B avec Charlie, croyant discuter avec Alice
- Charlie peut alors intercepter, modifier, etc. tous les messages entre Alice et Bob

$\rightarrow$ Nécessite une *authentification* entre Alice et Bob

Où vivent les clefs ?

- *A priori* pour la cryptographie symétrique : $\mathcal{K} = \{0,1\}^n$ pour un certain n
- Échange de clef : $k \in G$, groupe cyclique de taille possiblement $\gg 2^n$

$\rightarrow$ Techniques de hachage pour obtenir la clef définitive

Conclusion

Protocoles d'échanges de clefs

- Suite de calculs et d'envois de messages pour qu'Alice et Bob partagent une clef
- Notion de sécurité : clef *indistinguable* d'un tirage uniforme

Groupes cycliques et logarithme discret

- Groupe cyclique : $G = \{g^0, g^1, \ldots, g^{|G|-1}\}$ pour un *générateur* g
- Logarithme discret : trouver t tel que $x = g^t$
  - Calcul en $O(\sqrt{|G|})$, voire env. $2^{O(\log(|G|)^{\frac{1}{3}})}$
- Hypothèses de difficulté :
  - Log. discret : pas de calcul en temps polynomial en $O(\log |G|)$
  - CDH : calcul de $g^{t_1 t_2}$ difficile depuis g^{t_1} et g^{t_2}
  - DDH : indistinguabilité entre $g^{t_1 t_2}$ et élément uniforme

Protocole de Diffie-Hellman

- Alice calcule $k = (g^{t_B})^{t_A}$ et Bob calcule $k = (g^{t_A})^{t_B}$
- Protocole sûr si hypothèse DDH vérifiée pour le groupe choisi