Algèbre et Cryptographie à Clef Publique

Des premières solutions Asymétriques

Yann Rotella

UVSQ - Université Paris-Saclay

26 mars 2026

Plan du Cours

Cryptographie asymétrique

Algèbre

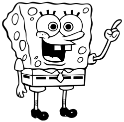
L'échange de clefs de Diffie et Hellman

Le cryptosystème d'ElGamal

CRYPTOGRAPHIE SYMÉTRIQUE

On suppose que Alice et Bob possèdent un secret commun appelé la clef notée k

$$k \in \mathcal{K}, m \in \mathcal{M}$$
$$E : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$$
$$E_k(m) = E(k, m) = c \Longrightarrow$$



$$k \in \mathcal{K}, c \in \mathcal{C}$$
$$D : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$$
$$D_k(c) = D(k, c) = m$$

✍ Comment se prémunir contre un attaquant actif ?

On a vu comment garantir la confidentialité, l'authenticité et l'intégrité dans le cas symétrique.

Cryptographie Symétrique

Problème

Les personnes doivent se partager une clef secrète et ce de manière sécurisée...

- C'est pratique si on est proche...
- Comment renouveler les clefs ?
- Exemple : le téléphone rouge (avec un masque jetable)

Cryptographie asymétrique

Algèbre
- Groupes
- Ordres et groupes engendrés
- Le théorème de Lagrange

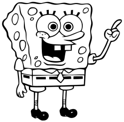
L'échange de clefs de Diffie et Hellman
- Problèmes algorithmiques

Le cryptosystème d'ElGamal
- IND-CPA Rappel
- Réduction du cryptosystème

Cryptographie Asymétrique

Bob possède une clef publique (pk_B - public) et une clef privée (sk_B - secret)

$$pk_B \in \mathcal{P}_k, m \in \mathcal{M}$$
$$Enc : \mathcal{P}_k \times \mathcal{M} \to \mathcal{C}$$
$$Enc_{pk_B}(m) = Enc(pk_B, m) = c \qquad \Longrightarrow$$



$$sk_B \in \mathcal{S}_k, c \in \mathcal{C}$$
$$Dec : \mathcal{S}_k \times \mathcal{C} \to \mathcal{M}$$
$$Dec_{sk_B}(c) = Dec(sk_B, c) = m$$

Avec ce type de cryptographie, on va pouvoir réaliser des échanges de clefs

✍ Donner la définition d'un groupe commutatif

DÉFINITION (GROUPE CYCLIQUE)

Soit $(G, \times)$ *un groupe.* $(G, \times)$ *est un groupe cyclique si tous les éléments de l'ensemble* G *sont engendré par un élément de* G*.*
Dit autrement, $(G, \times)$ *est cyclique si*

$$\exists g \in G, \forall x \in G, \exists n \in \mathbb{Z}, x = g^n$$

Propriété (Sous-groupe engendré)

Soit $(G,\times)$ *un groupe. Pour tout* $x \in G$*, on note* $< x >$ *l'ensemble engendré par l'élément* x *:*

$$< x >= \{x^i, i \in \mathbb{Z}\}.$$

Alors, $< x >$ *est un sous-groupe de* G*.*

✍ Rappeler la définition d'un sous-groupe.

✍ Montrer la propriété.

Définition (Générateur)

Soit $(G,\times)$ *un groupe. On appelle générateur de* G *tout élément* $g \in G$ *qui engendre seul* G*, i.e.* $g \in G$ *est un générateur si et seulement si*

$$< g >= G.$$

Ordre d'un élément

Définition (Ordre d'un élément)

Soit $(G, \times)$ *un groupe fini (l'ensemble* G *est fini). Pour tout* x *dans* G*, on appelle ordre de* x*, noté* $\mathrm{ord}(x)$ *le cardinal du sous-groupe engendré par* x*. i.e.*

$$\mathrm{ord}(x) = | < x > |$$

- Si G est fini, comme $< x >$ est un sous-groupe de G pour tout x, l'ensemble est donc inclus dans G et est donc bien fini.

Théorème de Lagrange et divisibilité

Théorème (de Lagrange)

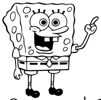
Soit $(G, \times)$ un groupe fini. Alors pour tout sous-groupe H de G, le cardinal de H divise le cardinal de G

- ✍ Preuve au tableau
- ✍ Que pouvez-vous dire sur les ordres des éléments dans un groupe ?
- ✍ Soit $x \in G$ avec G un groupe fini. Que vaut $x^{\mathrm{ord}(x)}$? Montrer le résultat.

L'ÉCHANGE DE CLEFS DE DIFFIE ET HELLMAN (1976)

$(G, \times)$ un groupe fini

$g \in G$ un générateur de G



$a \leftarrow_{\$} 0, \cdots, |G| - 1$

$Enc : \mathcal{P}_k \times \mathcal{M} \rightarrow \mathcal{C}$

$b \leftarrow_{\$} 0, \cdots, |G| - 1$

$$\xrightarrow{A = g^a}$$

$B^a = g^{ab}$

$A^b = g^{ba}$

- Si tout se passe bien, Alice et Bob partagent à la fin du protocole la même valeur g^{ab}.
- Mais est-ce que tout se passe bien ?
- ✍ Si Eve ne fait qu'écouter qu'est-ce qu'elle connaît ?

Problèmes algorithmiques associés

Soit $(G, \times)$ un groupe cyclique et soit g un générateur.

Problème (du Logarithme Discret)

Connaissant $h \in G$, trouver $a \in \mathbb{Z}$ tel que $h = g^a$.

Problème (CDH - Computational Diffie-Hellman)

Connaissant (g, g^a, g^b), calculer la valeur g^{ab}.

Problème (DDH - Decisional Diffie-Hellman)

Connaissant (g^a, g^b), distinguer g^{ab} de g^c pour c aléatoire.

Quel groupe G choisir ?

Fait : on peut montrer que si G n'a pas de propriété « particulière », alors tout algorithme qui « casse » le problème du logarithme discret nécessite $\Omega(\sqrt{|G|})$ opérations (Victor Shoup, 1997).

- Mais...

✍ Quel est le premier groupe fini auquel on peut penser ?

✍ Il va falloir trouver autre chose...

✍ Corps finis (hors programme), de petite ou grande caractéristique (avec la loi de multiplication).

Le cryptosystème d'ElGamal (1984)

Génération de clefs :

- Un groupe $(G, \cdot)$, un générateur g de G, avec $n = |G|$
- clef privée : $sk \in \mathcal{S}_k = \{0, \ldots, n-1\}$ tirée aléatoirement
- clef publique : $pk = g^{sk} \in \mathcal{P}_k = G$
- $\mathcal{M} = G$
- $\mathcal{C} = G \times G$

Chiffrement :

$$\begin{aligned} Enc : G \times G &\to G \times G \\ (pk, m) &\mapsto (m \cdot pk^r, g^r) = (m \cdot g^{rsk}, g^r) \end{aligned}$$

où r est une valeur tirée aléatoirement dans $\mathbb{Z}/n\mathbb{Z}$.

Déchiffrement :

$$\begin{aligned} Dec : \mathbb{Z}/n\mathbb{Z} \times (G \times G) &\to G \\ (sk, (c_1, c_2)) &\mapsto c_2 \cdot c_1^{-sk} \end{aligned}$$

Le cryptosystème d'ElGamal (1984)

Chiffrement :

$$\begin{aligned} Enc : G \times G &\to G \times \mathbb{Z}/n\mathbb{Z} \\ (pk, m) &\mapsto (m \cdot pk^{r}, g^{r}) = (m \cdot g^{rsk}, g^{r}) \end{aligned}$$

où r est une valeur tirée aléatoirement dans $\mathbb{Z}/n\mathbb{Z}$.

Déchiffrement :

$$\begin{aligned} Dec : \mathbb{Z}/n\mathbb{Z} \times (G \times \mathbb{Z}/n\mathbb{Z}) &\to G \\ (sk, (c_1, c_2)) &\mapsto c_2 \cdot c_1^{-sk} \end{aligned}$$

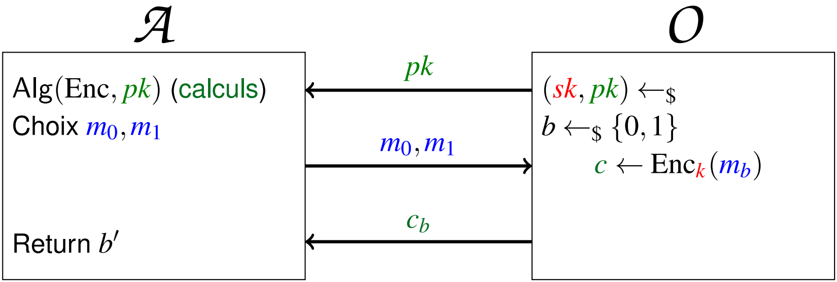
✍ Vérifier que le chiffrement est correct.

IND-CPA EN ASYMÉTRIQUE

L'adversaire $\mathcal{A}$ connaît Enc. La clef secrète k est tirée aléatoirement.

L'adversaire connaît la clef publique !

L'adversaire est limité en **calculs**.



ElGamal est IND-CPA sous DDH

$\mathcal{A}$		$\mathcal{O}$
Alg(Enc, pk) (calculs)	$\xleftarrow{pk}$	$(sk, pk) \leftarrow_{\$}$
Choix m_0, m_1	$\xrightarrow{m_0, m_1}$	$b \leftarrow_{\$} \{0,1\}$ $c \leftarrow \mathrm{Enc}_k(m_b)$
Return b'	$\xleftarrow{c_b}$	

$$Enc : G \times G \to G \times \mathbb{Z}/n\mathbb{Z}$$

$$(pk, m) \mapsto (m \cdot pk^r, g^r) = (m \cdot g^{rsk}, g^r)$$

$$Dec : \mathbb{Z}/n\mathbb{Z} \times (G \times \mathbb{Z}/n\mathbb{Z}) \to G$$

$$(sk, (c_1, c_2)) \mapsto c_2 \cdot c_1^{-sk}$$

✍ Preuve au tableau de ElGamal est IND-CPA sous DDH

Conclusions et perspectives

- Un bon choix de groupe permet de réaliser de la cryptographie asymétrique
- Rappels de théorèmes sur les groupes à connaître
- Échange de clefs (Diffie-Hellman), chiffrement asymétrique (ElGamal)
- Toujours nécessité d'aléa dans le chiffrement (IND-CPA)
- Réductions à DDH ou CDH

Problème

ElGamal n'est pas sûr à chiffrés choisis (il n'est pas IND-CCA) - cf TD