# Cryptosystème ElGamal

Anca Nitulescu
anca.nitulescu@ens.fr

Ecole Normale Supérieure, Paris

Cours 4

# Protocole ElGamal

## ElGamal - Génération des clés

$\mathcal{KG}(\ell) = (\mathsf{pk}, \mathsf{sk})$

- Soit un premier p et le groupe cyclique $\mathbb{Z}_p^\star$
- Soit $g \in \mathbb{Z}_p^\star$ un élément d'ordre q, un diviseur de $(p-1)$.
- Soit une clé secrète $\mathsf{sk} = x$.
- Soit $y = g^x \pmod p$.

## clé publique

- $p$ et $g$ : paramètres publiques
- $\mathsf{pk} = y = g^x$ : clé publique

## clé secrète

- $\mathsf{sk} = x$
  exposant sécret

# Protocole ElGamal

## ElGamal - Chiffrement

$\mathcal{E}(\text{pk} = y, M) = (C, D)$

Pour un aléa $r$ on calcule une paire $(C, D)$ (le chiffré de $M$)

$$C = g^r \pmod{\text{p}}$$

$$D = M \cdot y^r \pmod{\text{p}}$$

## ElGamal - Déchiffrement

$\mathcal{D}(\text{sk} = x, (C, D)) = D \cdot C^{-x} \pmod{\text{p}}$.

# Protocole ElGamal

## ElGamal - Chiffrement

$\mathcal{E}(\text{pk} = y, M) = (C, D)$

Pour un aléa $r$ on calcule une paire $(C, D)$ (le chiffré de $M$)

$$C = g^r \pmod{\text{p}}$$

$$D = M \cdot y^r \pmod{\text{p}}$$

## ElGamal - Déchiffrement

$\mathcal{D}(\text{sk} = x, (C, D)) = D \cdot C^{-x} \pmod{\text{p}}$.

## Vérification

$$D \cdot C^{-x} = M\ y^r\,(g^r)^{-x} = M\,(g^x)^r\,(g^r)^{-x} = M \pmod{p}$$

# Emploi de ElGamal

## Avantages

- Tous les utilisateurs peuvent utiliser le même groupe $\mathbb{Z}_p^\star$ et le même $g$
- Possibilité de techniques d'exponentiation rapide
- Chiffrement randomisé nativement
- Meilleure sécurité basique

## Inconvénients

- Augmentation de la taille du chiffré
- Deux fois plus lent que RSA

# Efficacité de ElGamal

## ElGamal - coût

Le coût est celui de deux exponentiations modulaires :

- El Gamal est 2 fois plus lent que RSA.
- La taille des données chiffrées représente 2 fois celle des données en clair.

# Propriétés multiplicatives

## ElGamal -Attaque à chiffré choisi

Si $(C, D)$ est un chiffré de $M$, pour tout $A$, le couple $(C, A \cdot D)$ chiffre $A \cdot M$ :

$$C = g^r \pmod{\text{p}}$$
$$A \cdot D = A \cdot M \cdot y^r \pmod{\text{p}}$$

# Attaques ElGamal

## ElGamal avec le même aléa

**Ne jamais utiliser deux fois le même aléa !**

Si $M_1$ et $M_2$ sont chiffrés avec le même aléa $r$, alors :

$$(C_1, D_1) = (g^r, y^r M_1) \pmod{p}$$
$$(C_2, D_2) = (g^r, y^r M_2) \pmod{p}$$

d'où :

$$\frac{M_1}{M_2} = \frac{D_1}{D_2}$$

# Problème difficile

## Logarithme discret (DLOG)

**Définition** Soit $\mathbb{G}$ un groupe multiplicatif, $g \in \mathbb{G}$ et $y \in \langle g \rangle$ :

$$\log_g(y) = x \quad \text{où} \quad g^x = y$$

# Difficulté de ElGamal

## Réduction

La recherche de la clé privée $x$ à partir de la clé publique $y = g^x$ est équivalente au problème du logarithme discret (DLOG).

**ElGamal se réduit au logarithme discret !**

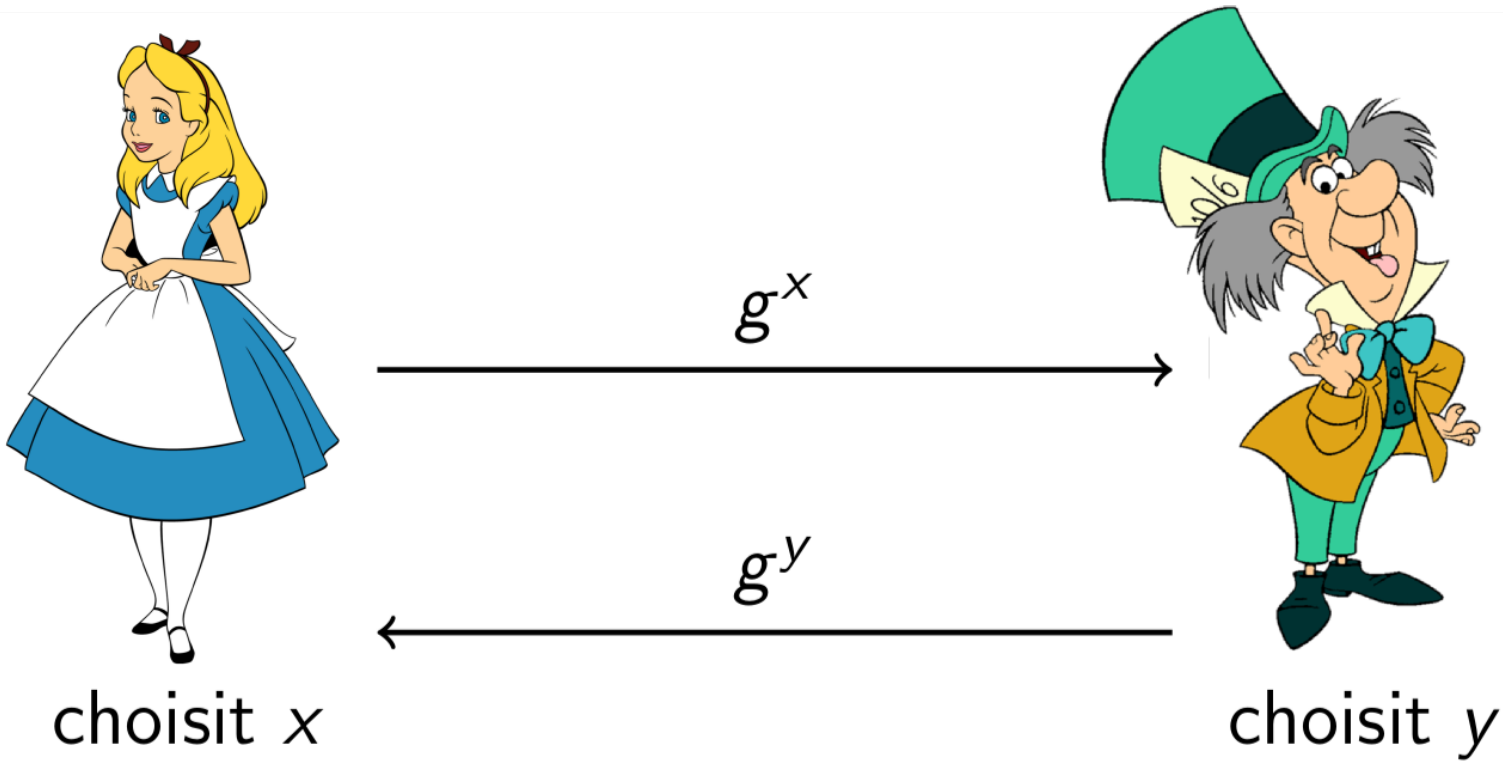
# Réduction de ElGamal

## En pratique

- Si le problème du logarithme est résolu polynomialement, alors El Gamal sera cassé.
- Le contraire est peut-être faux !
- Rien ne prouve qu'il n'est pas cassable par un autre moyen.

Le log discret est la seule méthode **connue** pour casser ElGamal.

# Echange de clé




clé commune $g^{xy}$

# Autres problèmes difficiles

Soit $\mathbb{G}$ un groupe multiplicatif cyclique, $\mathbb{G} = \langle g \rangle$ :

**Calculer Diffie-Hellman (CDH)**

Etant donnés $g$, $A = g^a$ et $B = g^b$,

Calculer $C = CDH(A, B) = g^{ab}$

**Décider si Diffie-Hellman (DDH)**

Etant donnés

$g$, $A = g^a$, $B = g^b$ et $C = g^c$ dans $\mathbb{G}$

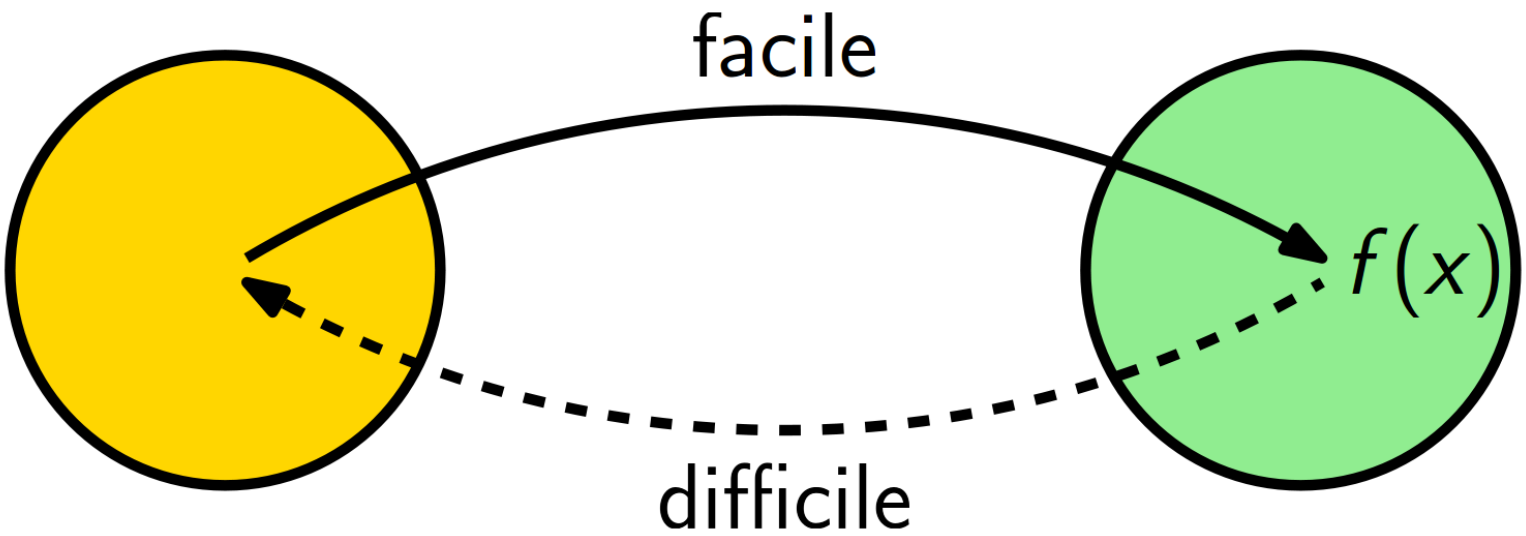
Décider si $C = g^{ab}$

# Réduction de Diffie-Hellman

## Attaquer Diffie-Hellman

- Si le problème **CDH** est résolu, alors l'attaquant peut calculer une clé Diffie-Hellman
- Si le problème **DDH** est résolu, alors l'attaquant peut distinguer entre une clé valide et une clé fausse

# Fonctions à sens unique



# Problèmes difficiles

Soit $\mathbb{G}$ un groupe multiplicatif cyclique, $\mathbb{G} = \langle g \rangle$ :

## Logarithme discret (DLOG)

Etant donnés $g \in \mathbb{G}$ et $X = g^x$,

Calculer $\log_g(X) = x$

## Calculer Diffie-Hellman (CDH)

Etant donnés $g$, $A = g^a$ et $B = g^b$,

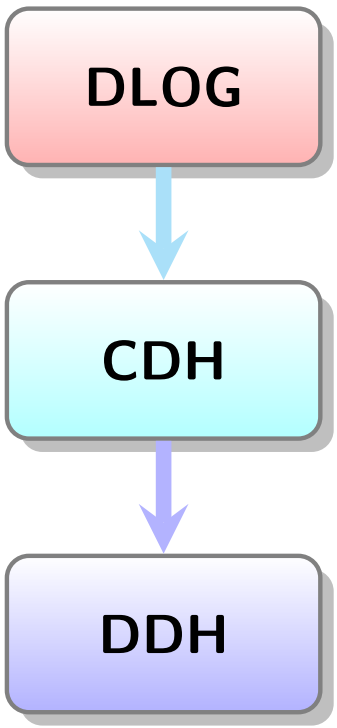
Calculer $C = CDH(A, B) = g^{ab}$

## Décider si Diffie-Hellman (DDH)

Etant donnés $g$, $A = g^a$, $B = g^b$ et $C = g^c$ dans $\mathbb{G}$

Décider si $C = g^{ab}$

# Hiérarchie




## CDH $<$ DLOG

Etant donnés $g$, $A = g^a$ et $B = g^b$,

- on calcule $b$ =DLOG($B$)
- on trouve $C = A^b = g^{ab}$

## DDH $<$ CDH

Etant donnés $g$, $A = g^a$, $B = g^b$ et $C = g^c$

- on calcule $CDH(A, B) = g^{ab}$
- on compare avec $C$