Chiffrement à clef publique ou asymétrique

Pierre-Louis Cayrel

Université de Limoges, XLIM-DMI,
123, Av. Albert Thomas
87060 Limoges Cedex France
05.55.45.73.10
pierre-louis.cayrel@xlim.fr

Licence professionnelle Administrateur de Réseaux
et de Bases de Données
IUT Limoges

Sommaire

Cryptographie à clef publique

R.S.A.

DLP & Diffie-Hellman

El Gamal

Motivations

- Systèmes cryptographiques à clé secrètes
  - pratiquement sûrs
  - efficaces en termes de temps de calcul.
- Mais nouvelles interrogations :
  - Avant d'utiliser un système de chiffrement à clé secrète, comment convenir d'une clé ?
  - Comment établir une communication sécurisée entre deux entités sans échange préalable de clef ?

  $\Rightarrow$ Solution apportée par Diffie et Hellman (1976)
  - systèmes cryptographiques à clé publique

Cryptographie à clef publique

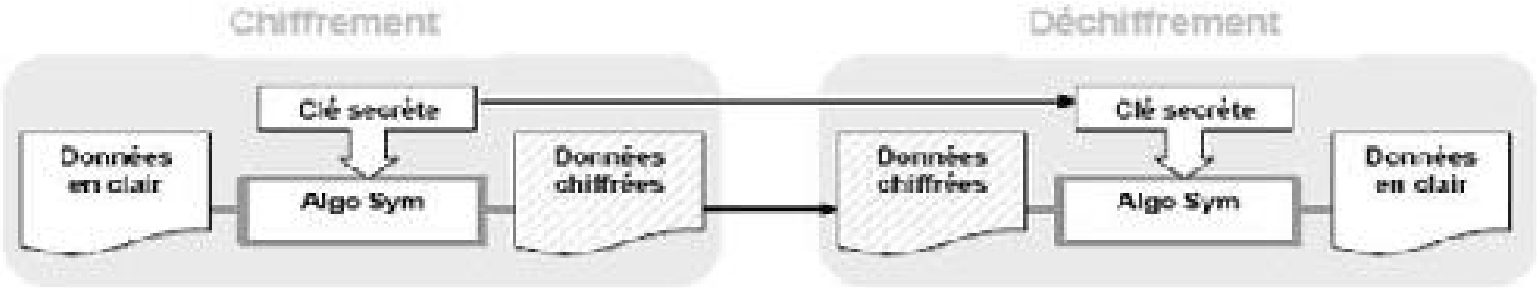


Fig.: La cryptographie symétrique

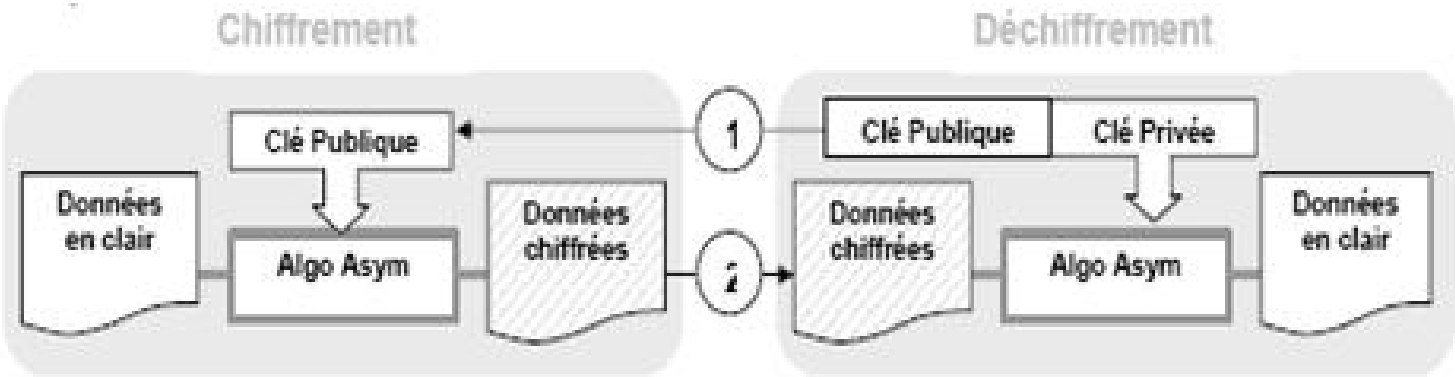


Fig.: La cryptographie asymétrique

Cryptographie asymétrique

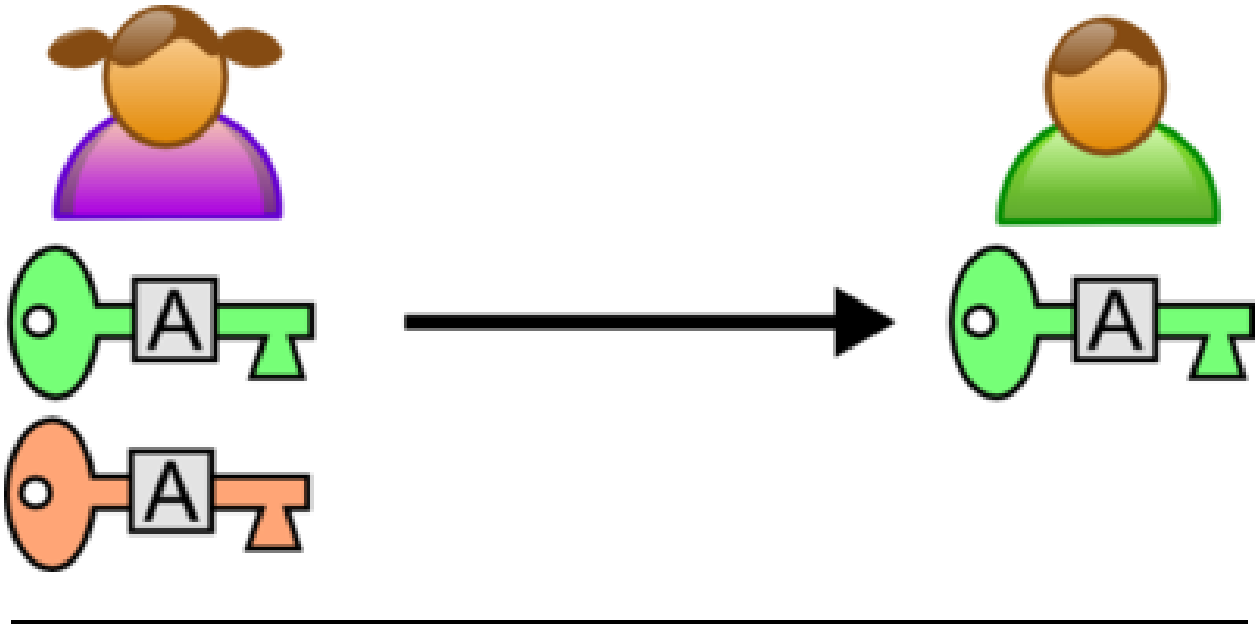


Fig.: La cryptographie asymétrique : Première Étape

Alice génère deux clés. La clé publique (verte) qu'elle envoie à Bob et la clé privée (rouge) qu'elle conserve précieusement sans la divulguer à quiconque.

Cryptographie asymétrique

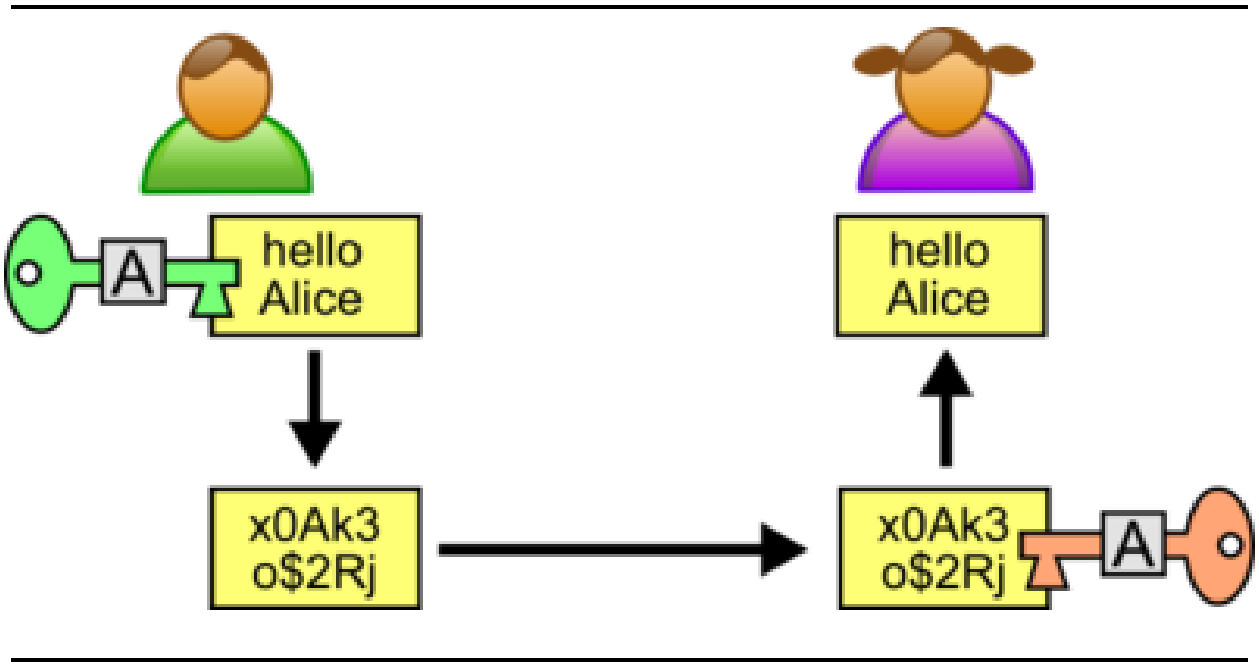


Fig.: La cryptographie asymétrique : Deuxième et Troisième Étape

Bob chiffre le message avec la clé publique d'Alice et envoie le texte chiffré. Alice déchiffre le message grâce à sa clé privée.

Cryptographie asymétrique

Fondée sur l'existence de fonctions à sens unique.
Il est simple d'appliquer cette fonction à un message, mais extrêmement difficile de retrouver ce message à partir du moment où on l'a transformé.

Déroulement

Bob souhaite pouvoir recevoir des messages chiffrés de n'importe qui.

- Il génère une valeur (clef publique) à partir d'une fonction à sens unique.
- Il diffuse la clef publique, mais garde secrète l'information permettant d'inverser cette fonction (clef secrète).

R.S.A.

Ronald Rivest, Adi Shamir et Leonard Adleman

Fig.: Ronald Rivest, Adi Shamir et Leonard Adleman, dans *A Method for Obtaining Digital Signatures and Public-key Cryptosystems* ont eu l'idée d'utiliser les anneaux $\mathbb{Z}/n\mathbb{Z}$ et le petit théorème de Fermat pour obtenir des fonctions trappes, ou fonctions à sens unique à brèche secrète.

R.S.A.

- C'est à l'heure actuelle le système à clef publique le plus utilisé (Netscape, la carte bancaire française, de nombreux sites web commerciaux).
- RSA repose sur le calcul dans les groupes $\mathbb{Z}/n\mathbb{Z}$, plus précisément sur l'exponentiation modulaire. Voici une description des principes mathématiques sur lesquels repose l'algorithme RSA.
- Il est toutefois important de remarquer que le passage des principes à la pratique requiert de nombreux détails techniques qui ne peuvent pas être ignorés, sous peine de voir la sécurité du système anéantie.

  Par exemple, il est recommandé d'encoder le message en suivant l'OAEP.

R.S.A.

Alice veut envoyer M à Bob.

- M un entier représentant un message.
- Bob choisit p et q deux nombres premiers et on note n leur produit.
- Bob choisit e un entier premier avec $p-1$ et $q-1$.
- On a $\varphi(n) = (p-1)(q-1)$ donc e est premier avec $\varphi(n)$ et on obtient (via Bézout) qu'il est inversible modulo $\varphi(n)$, i.e. il existe un entier d tel que $ed \equiv 1 \pmod{\varphi(n)}$.
- Le message chiffré sera alors représenté par :

$$C = M^e \pmod{n}$$

- Pour déchiffrer C, on calcule d l'inverse de $e \mod \varphi(n)$, ensuite on calcule $C^d \mod n$.

R.S.A.

- On a alors,

$$C^d \pmod{n} \equiv (M^e)^d \pmod{n} \equiv M^{ed} \pmod{n}$$

- Comme $ed \equiv 1 \pmod{\varphi(n)}$ par définition de modulo, on a

$$ed = 1 + k\varphi(n), \text{avec } k \in \mathbb{N}.$$

- D'où,

$$M^{ed} \pmod{n} \equiv M \cdot M^{k\varphi(n)} \pmod{n} \equiv M \cdot (M^{\varphi(n)})^k \pmod{n}$$

- Or si x est premier avec n; on a $x^{\varphi(n)} \equiv 1 \pmod{n}$, d'après le théorème d'Euler.
- Donc finalement, si le message M est premier avec n :

$$C^d \equiv M \pmod{n}.$$

R.S.A.

- Le cas où le message M n'est pas premier avec n est un peu plus compliqué mais le résultat reste le même :

$$C^d \equiv M \pmod{n}.$$

- (n, e) est appelé clef publique
- (n, d) est appelé clef privée.
- pour chiffrer, il suffit de connaître e et n.
- pour déchiffrer, il faut d et n, autrement dit connaître la décomposition de n en facteurs premiers.

Alice		Bob
M		
		choisit p et q e premier avec $p-1$ et $q-1$
		calcule $n = p \times q$ d tel que $ed \equiv 1 \pmod{\varphi(n)}$
	$\longleftarrow$	envoie (n, e) à Alice
calcule $C = M^e \pmod{n}$ et l'envoie à Bob	$\longrightarrow$	
		calcule $C^d \pmod{n}$ et en déduit M

Le cryptosystème RSA : Exemple

Prenons $p = 47$ et $q = 59$.

- On calcule $n = p.q = 47.59 = 2773$
- On choisit e, premier par rapport à $\phi(n)$. Ex : $e = 17$.
- On calcule alors, par l'algorithme d'Euclide étendu[1], d tel que $d.e = 1 \mod (p-1)(q-1)$, soit $d = 157$.

Clef publique : $(e, n) = (17, 2773)$
Clef privé : $d = 157$.

- Chiffrement du message $M = 01000010 = 66$:

$$C = M^e \mod n = 6617 \mod 2773 = 872$$

- Déchiffrement de C :

$$C^d \mod n = 872^{157} \mod 2773 = 66$$

[1] sous Maple : igcdex

RAPPEL : Exponentiation rapide modulaire

Exercice :
Calcul de $51447^{21} \mod 17$ (E)

Exponentiation rapide modulaire

$51447 = 3026 \times 17 + 5$ donc $(E) \equiv 5^{21} \mod 17$

1. Décomposition de 21 en binaire : $21 = 2^4 + 2^2 + 2^0$
2. Calcul de $\{5^{2^i} \mod 17\}_{0 \leq i \leq 4}$
   - $i = 0 : 5^{2^0} = 5 \mod 17$
   - $i = 1 : 5^{2^1} = 5^2 = 25 = 8 \mod 17$
   - $i = 2 : 5^{2^2} = 8^2 = 64 = 13 = -4 \mod 17$
   - $i = 3 : 5^{2^3} = (-4)^2 = 16 = -1 \mod 17$
   - $i = 4 : 5^{2^4} = (-1)^2 = 1 \mod 17$
3. On en déduit : $5^{21} = 5^{2^4} \times 5^{2^2} \times 5^{2^0} = 1 \times (-4) \times 5 = -20 = 14 \mod 17$

Le cryptosystème RSA : Exercice

Prenons $p = 29, q = 31$ et $e = 13$. Utilisé le protocole RSA pour chiffrer et déchiffrer $M = 123$

Le cryptosystème RSA : Exercice

- Les variables étant données, $p = 29, q = 31, e = 13, m = 123$;
- Nous calculons : $n = p \times q = 899$
- $(p-1) \times (q-1) = 840$
- $d = 517$ car $e \times d = 13 \times 517 = 8 \times (p-1) \times (q-1) + 1$
- Pour chiffrer,

$$c = 123^{13} \mod 899 = 402$$

- Et pour déchiffrer,

$$m = 402^{517} \mod 899 = 123$$

Sécurité du cryptosystème RSA

- Le vrai but de l'attaquant : découvrir le texte en clair !
- Calculer d à partir de $(n, e) \equiv$ factoriser n.
  - $\Leftarrow$: trivial (cf génération des clefs)
  - $\Rightarrow$: Soit $s = \max\{t \in \mathbb{N} : 2^t | ed - 1\}$. On pose $k = \frac{ed-1}{2^s}$. Alors, soit $a \in \mathbb{Z}$ est premier avec n.
    - l'ordre de a^k dans $\mathbb{Z}_n \in \{2^i; 0 \leq i \leq s\} (a^{\phi(n)} = 1 \mod n)$
    - si l'ordre de $a^k \mod p \neq$ l'ordre de $a^k \mod q$, alors

$$\exists t \in [0, s[/ 1 < pgcd(a^{2^t k} - 1, n) < n$$

    On a ainsi trouvé un facteur non trivial de n.
- (Résultat récent) : Casser RSA est équivalent à la factorisation de n [Coron2004].

Sécurité du cryptosystème RSA

- Limites actuelles de factorisation : $\approx$ 200 chiffres
- Record actuel[2] : RSA200 (200 chiffres décimaux)

  Bahr, Boehm, Franke and Kleinjung - 9 mai 2005.
- Si la clef secrète d est petite (de l'ordre de $n^{\frac{1}{4}}$) :
  - attaque utilisant l'algorithme des fractions continues (algorithme LLL)
  - permet de calculer d à partir de n et e.

[2] `http://www.loria.fr/~zimmerma/records/factor.html`

DLP & Diffie-Hellman

Merkle-Hellman-Diffie

DLP & Diffie-Hellman

Autre problème difficile : Discret Logarithme Problem

- **Definition** (Logarithme discret)

  Soit $G =< g >= \{g^i\}_{0 \leq i < n}$ un groupe monogène fini d'ordre n. Soit $h \in G$. Alors le logarithme discret de h en base g, noté $log_g h$, est l'unique entier x tel que $h = g^x (0 \leq x < n)$.

- DLP consiste alors à résoudre le problème suivant :

  Etant donné G, g, h, trouver $x = log_g h$.

- Exemple : $p = 97$ et $G = \mathbb{Z}/97\mathbb{Z} = 1, 2, ..., 96 = \{5^i\}_{0 \leq i < 96}$;
  $5^{32} = 35 \mod 97 \Rightarrow log_5 35 = 32$ dans $\mathbb{Z}/97\mathbb{Z}$.

Protocole d'échange de clefs de Diffie-Hellman

Alice et Bob veulent partager une clef secrète K. On suppose que les données $G, n = |G|$ et g sont publiques.

- Alice choisit un entier $1 \leq a \leq n-1$ au hasard.
- Alice calcule $A = g^a$ et l'envoie à Bob.
- Bob choisit un entier $1 \leq b \leq n-1$ au hasard.
- Bob calcule $B = g^b$ et l'envoie à Alice.
- Alice est en mesure de calculer B^a et Bob de calculer A^b. La clef commune est donc

$$K = g^{ab} = A^b = B^a.$$

Protocole d'échange de clé de Diffie-Hellman

Alice		Bob
génère a		génère b
$A = g^a \mod p$		$B = g^b \mod p$
	$A \longrightarrow$	
	$\longleftarrow B$	
(dispose de $[a, A, B, p]$)		(dispose de$[b, A, B, p]$
Clé secrète : $K = B^a \mod p$		Clé secrète : $K = A^b \mod p$

Protocole d'échange de clé de Diffie-Hellman

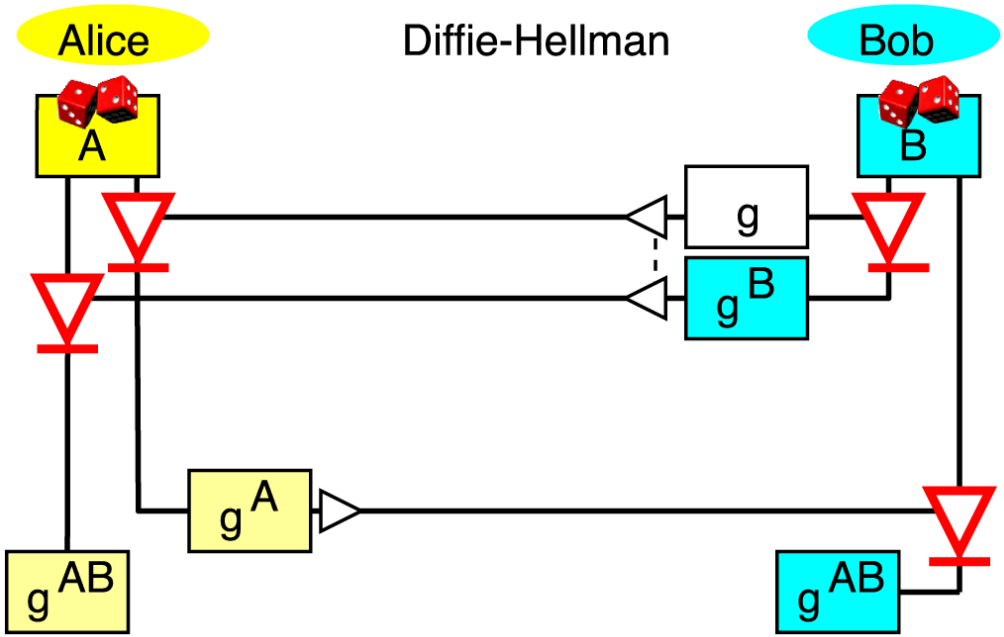


Fig.: `www.petworkshop.org/2004/talks/fairbrother/`

Protocole d'échange de clé de Diffie-Hellman (exemple)

1. Alice et Bob choisissent un nombre premier p et une base g. Dans notre exemple, $p = 23$ et $g = 3$
2. Alice choisit un nombre secret $a = 6$
3. Elle envoie à Bob la valeur $g^a \mod p = 3^6 \mod 23 = 16$
4. Bob choisit à son tour un nombre secret $b = 15$
5. Bob envoie à Alice la valeur $g^b \mod p = 3^{15} \mod 23 = 12$
6. Alice peut maintenant calculer la clé secrète :

$$(g^b \mod p)^a \mod p = 12^6 \mod 23 = 9$$

7. Bob fait de même et obtient la même clé qu'Alice :

$$(g^a \mod p)^b \mod p = 16^{15} \mod 23 = 9$$

Protocole d'échange de clé de Diffie-Hellman (exercice)

1. Supposons qu'Alice et Bob partagent $p = 233$ et $g = 45$:
2. si Alice choisit $a = 11$ et Bob $b = 20$, alors :
3. Quelle est leur clef secrète commune ?

Protocole d'échange de clé de Diffie-Hellman (corrigé)

$$g^a = 45^{11} \mod 233 = 147, g^b = 45^{20} \mod 233 = 195,$$

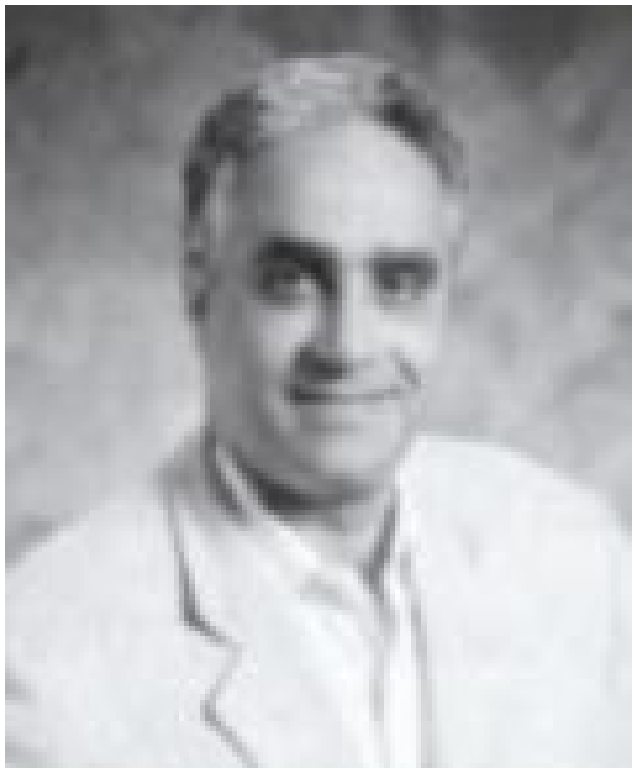
- $(g^b)^a \mod p = 195^{11} \mod 233 = 169$ et $(g^a)^b \mod p = 147^{20} \mod 233 = 169$.
- Alice et Bob disposent d'une clé privée commune : $k = 169$.

Sécurité de DH

- Problème de DH :
  - connaissant $G, g, A = g^a$ et $B = g^b$, calculer $K = g^{ab}$.
- A l'heure actuelle, résoudre DLP est la seule méthode générale connue pour résoudre DH.
  - MAIS : pas de preuve que résoudre DLP $\equiv$ résoudre DH.
- Choix du groupe G : $G = \mathbb{F}_p^*$, $G = E(\mathbb{F}_p)$, etc.
  - Attention au bon choix des paramètres.

Le cryptosystème de El Gamal

El Gamal



Le cryptosystème de El Gamal

Données publiques pré-requise :

- $(G, .) =< g >$ un groupe cyclique d'ordre n

Génération des clefs

- Bob choisit $a \in [1, n-1]$ et calcule $A = g^a$ dans G.
- Clef publique : (G, g, n, A).
- Clef secrète : a.

Le cryptosystème de El Gamal (2)

Chiffrement : Alice souhaite envoyer le message $M \in G$ à Bob

- Alice récupère la clef publique (G, g, n, A) de Bob.
- Alice choisit au hasard $k \in [1, n-1]$
- Le message chiffré qu'Alice envoit à Bob est $C = (y_1, y_2)$ avec

$$y_1 = g^k \text{ et } y_2 = M.A^k$$

Le cryptosystème de El Gamal (3)

Déchiffrement

- Bob recoit le message chiffré $C = (y_1, y_2)$
- Il lui suffit alors de calculer

$$M = y_2.(y_1^a)^{-1} = y_2.y_1^{n-a}$$

En effet :

$$\begin{aligned} y_2.y_1^{n-a} &= M.A^k.(g^k)^{n-a} \\ &= M.g^{a.k}.g^{k.n}.g^{-ka} \\ &= M.g^{a.k}.(g^n)^k.g^{-ka} \\ &= M.g^{a.k}.g^{-ka} = M \end{aligned}$$

Le protocole d'El Gamal

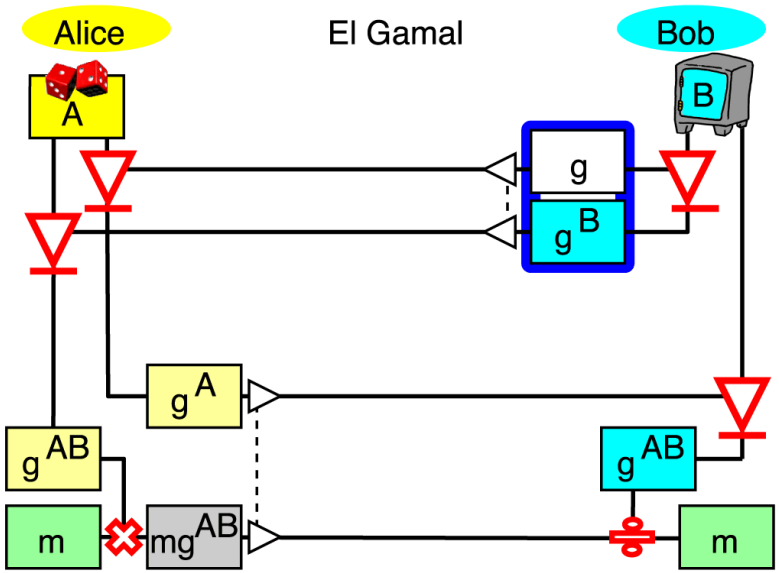


Fig.: `www.petworkshop.org/2004/talks/fairbrother/`

Sécurité du cryptosystème de El Gamal

- Résoudre DLP dans $G \Rightarrow$ Casser El Gamal dans G
  - l'attaquant peut alors calculer a à partir de A (public).
- La réciproque n'est pas encore prouvée !

Cas particulier de $G = \mathbb{F}_p^*$:

- utiliser un nombre premier p de 1024 bits choisis uniformément
- permet de résister aux méthodes actuelles de résolution de DLP sur $\mathbb{F}_p^*$