TD 10 : Chiffrement Elgamal

christina.boura@uvsq.fr

10 avril 2018

Exercice 1 *Elgamal : À faire avec votre voisin*
Pour cet exercice formez des groupes de deux personnes. Générez indépendamment vos clés privées et publiques pour le chiffrement Elgamal. Gardez votre clé privée secrète (!) et transmettez votre clé publique à votre voisin. Chiffrez ensuite votre date d'anniversaire JJMM avec la clé publique de votre voisin et transmettez lui ce message chiffré. Si votre voisin vous souhaite "Joyeux anniversaire" la prochaine fois, alors tout s'est bien passé.

Pour cet exercice on travaillera dans le groupe multiplicatif $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. L'alphabet clair est alors constitué de 10 chiffres, $1, \ldots, 10$, où le chiffre 0 sera substitué par 10. Utilisez la table ci-dessous pour vos calculs.

n	1	2	3	4	5	6	7	8	9	10
$2^n \mod 11$	2	4	8	5	10	9	7	3	6	1
$3^n \mod 11$	3	9	5	4	1	3	9	5	4	1
$4^n \mod 11$	4	5	9	3	1	4	5	9	3	1
$5^n \mod 11$	5	3	4	9	1	5	3	4	9	1
$6^n \mod 11$	6	3	7	9	10	5	8	4	2	1
$7^n \mod 11$	7	5	2	3	10	4	6	9	8	1
$8^n \mod 11$	8	9	6	4	10	3	2	5	7	1
$9^n \mod 11$	9	4	3	5	1	9	4	3	5	1
$10^n \mod 11$	10	1	10	1	10	1	10	1	10	1

Exercice 2 *Elgamal : Clé publique de petit ordre*
On exploitera ici une faiblesse du système Elgamal quand une clé publique de petit ordre est utilisée. On suppose que Bob utilise le groupe multiplicatif $\mathbb{Z}_{29}^*$ avec $\alpha = 2$ comme élément primitif. Sa clé publique est $\beta = 28$.

1. Quel est l'ordre de la clé publique ?
2. Quels clés de masquage k_M sont possibles ?
3. Alice chiffre un message. Chaque caractère est codé selon la règle simple suivante : a $\rightarrow$ 0, b $\rightarrow 1, \ldots,$ z $\rightarrow$ 25. Il y a 3 symboles de plus é $\rightarrow$ 26, è $\rightarrow$ 27 et à $\rightarrow$ 28. Alice transmet les 8 blocs chiffrés (k_E, c) suivants :

$$(3, 8), (6, 8), (4, 21), (8, 25), (13, 11), (17, 3), (18, 10), (9, 26).$$

Déchiffrer le message sans calculer la clé privée de Bob. Exploiter le fait que très peu de clés de masquage sont possibles.

Exercice 3 *Elgamal : Bob est feignant*
Bob envoie des messages chiffrés à Alice en utilisant le système de chiffrement Elgamal avec paramètres $(p, \alpha, \beta) = (31, 3, 18)$. Cependant, Bob est un peu feignant et utilise le même paramètre secret k pour tous les messages. On connaît en plus que pour toutes ses communications, Bob envoie d'abord le message $m_1 = 21$ qui est son identifiant personnel. On obtient les messages chiffrés suivants :

$$\begin{aligned} (k_{E,1}, c_1) &= (6, 17) \\ (k_{E,2}, c_2) &= (6, 25) \end{aligned}$$

Quel est le deuxième message m_2 que Bob a envoyé ?

Exercice 4 *Elgamal : Problème du générateur pseudo-aléatoire*
Bob utilise le système Elgamal pour recevoir des messages chiffrés. Soit $k_{pubB} = (p, \alpha, \beta)$ sa clé publique et k_{prB} sa clé privée. Alice souhaite envoyer n messages $m_1, \ldots, m_n$ à Bob, mais à cause d'un problème d'implantation de son générateur pseudo-aléatoire, les puissances aléatoires k_i, $i = 1, \ldots, n$ qu'elle génère vérifient la relation suivante :

$$k_{i+1} = k_i + 1, \text{ pour } i = 1, \ldots, n-1.$$

Alice chiffre les n messages et envoie à Bob les chiffrés correspondants

$$(k_{E_1}, c_1), (k_{E_2}, c_2), \ldots, (k_{E_n}, c_n),$$

1. Quelle est la relation entre les clés éphémères k_{E_i} et les clés de masquage k_{M_i} générées ?
2. On suppose qu'un attaquant, Éve, connaît le message m_1. Expliquer comment Éve peut retrouver $m_2, \ldots, m_n$.

Exercice 5 *Force brute*
Soit $(p, \alpha, \beta) = (53, 2, 16)$ la clé publique d'un système Elgamal et $(k_E, c) = (15, 50)$ un message chiffré produit par ce système. Quel est le message clair correspondant ?