Master Eii

Fiche Algorithme de El Gamal

L'algorithme *El Gamal* est un algorithme de cryptographie asymétrique basé sur les logarithmes discrets. Il a été créé par Taher Elgamal en 1984.

Cet algorithme est utilisé par le logiciel libre GNU Privacy Guard, de récentes versions de PGP, et d'autres systèmes de chiffrement, et n'a jamais été sous la protection d'un brevet contrairement à RSA.

Il est facile de transformer la technique d'échange de clé selon Diffie et Hellman, en un système de cryptographie à clé publique : c'est la méthode d'El Gamal.

L'algorithme est décrit pour un groupe multiplicatif $\mathbb{Z}_p^*$, p premier, mais n'importe quel groupe cyclique fini pour lequel le problème du logarithme discret est difficile convient. On suppose que Bob veut envoyer un message à Alice (le chiffrement est asymétrique).

- Alice calcule deux clés, une clé publique et une clé privée : elle choisit d'abord p suffisamment grand pour que le calcul du logarithme discret soit infaisable pratiquement dans le groupe multiplicatif $\mathbb{Z}_p^*$, g un générateur de ce groupe et un entier naturel s, $s < p$, puis calcule $\boldsymbol{h = g^s \bmod p}$. L'entier s est la *clé secrète*, le triplet (p, g, h) la *clé publique*. Cette dernière seule est connue de Bob.
- Le message clair de Bob est supposé être un m dans $\mathbb{Z}_p^*$. Bob choisit aléatoirement un nombre entier k puis calcule (dans $\mathbb{Z}_p^*$) $\boldsymbol{c_1 = g^k}$ et $\boldsymbol{c_2 = m\, h^k}$. Le message chiffré est le couple (c_1,c_2) que Bob envoie à Alice.
- Alice peut déchiffrer le message reçu en calculant $m = c_2 / c_1^{\,s}$.

  En effet :

$$\frac{c_2}{{c_1}^s} = \frac{m \cdot h^k}{g^{ks}} = \frac{m \cdot h^k}{h^k} = m$$

Master Eii

Fiche Exercices

Diffie-Hellman & El Gamal

Enoncés :

Exercice 4 (Échange de clef de Diffie Hellman). Soit $p = 251$ et le générateur $g = 11$ modulo p. Soit maintenant $a = 15$ et $b = 21$. Déterminer la clef commune à Alice et Bob, s'ils effectuent un échange de clef de Diffie-Hellman.

Exercice 5 (ElGamal). Soit $p = 53, g = 2, B = 30$ la clef publique ElGamal de Bob.

- Chiffrer le message $m = 42$ avec la clef publique de Bob.
- On suppose que la clef secrète de Bob est $b = 13$ vérifier le et déchiffer le message $(R = 15, c = 17)$.

Solutions :

Diffie Hellman :

1. Alice et Bob choisissent un nombre premier p = 251 et une base g = *11.*
2. Alice choisit un nombre secret a = 15
3. Elle envoie à Bob la valeur g^a [mod p] = 11^{15} [251] = 182
4. Bob choisit à son tour un nombre secret b = 21
5. Bob envoie à Alice la valeur g^b [mod p] = 11^{21} [251] = 44
6. Alice peut maintenant calculer la clé secrète : $(g^b \text{ [mod } p])^a$ [mod p] = 44^{15} [251] = 200
7. Bob fait de même et obtient la même clé qu'Alice : $(g^a \text{ [mod } p])^b$ [mod p] = 182^{21} [251] = 200

El Gamal :

1. On a le système (p=53 ; g=2 ; h = B = 30). Pour chiffrer le message, on choisit au hasard k = 3.
2. On calcule le système ($c_1 = g^k = 2^3$ mod 53 = **8** ; c_2 = m h^k = 42 . 30^3 mod 53 = **12**) à transmettre
3. Vérifions que b = 13 est la clé secrète : calculons B = g^s mod p = 2^{13} mod 53 = 30. Donc OK !!
4. Déchiffrons le message (15;17) : m = 17 / (15^{13} mod 53) = 17 / (1 mod 53). Or l'inverse de 1 est 1 donc on arrive à m = 17 . 1^{-1} mod 53 = 17 . 1 mod 53 = 17 mod 53

Vérifions que le message codé (8;12) est bien le message m = 42 :

m = 12 / (8^{13} mod 53) = 12 / (23 mod 53) = 12 . 23^{-1} mod 53 = 12 . 30 mod 53 = 360 mod 53 = 42 !!