DECISION ALPHA

Parc technologique du Zoopole
Espace d'entreprises Keraia
18C, rue du Sabot
F-22440 PLOUFRAGAN
Tel : 02 96 76 63 68
Mail : info@decision-alpha.com

Cryptage asymétrique

Théorie :

Soit deux nombres premiers A et B

Théorème d'Euler : **Quel que soit x, non multiple de A ou de B :**

$$x^{(A-1)*(B-1)} = 1 + y * (A * B) = 1 \text{ modulo } (A * B)$$

(Pour des grands nombres pour A et B, la probabilité que X en soit multiple est quasi-nulle)

En simplifiant : $M = A * B$

. $K = (A - 1)*(B-1)$

$$X^{k} = 1 + yM = 1 \text{ modulo } M$$

Choix des clés

La clé publique M est la multiplication de deux nombres premiers A et B

On choisit une clé S (secrète) qui, multipliée par un nombre P donne le résultat suivant :

$$S * P = (n * (A - 1)*(B-1)) - 1 = (n * K) - 1$$

Le nombre de clés secrètes correspondant à la clé publique est très grand dans la mesure où on travaille sur des nombres très grands (environ 300 chiffres pour les écrire). Connaissant une des clés, on ne peut pas calculer l'autre « dans des délais raisonnables ».

Fonctionnement :

Le texte est condensé en un chiffre qu'on élève à la puissance S :

$$T' = T^{S}$$

Le chiffre T^S est envoyé

A réception, T' est élevé à la puissance P

$$T'' = T'^{P} = T^{S*P} = T^{nK+1} = T * T^{nK}$$

Or $T^{nK} = 1 \text{ modulo } M$

Donc le texte reçu, si aucune modification n'a été faite, sera T'' = T modulo M