Programme Freeware de cryptage « Rijndael » à 2 clés publique et privée : le

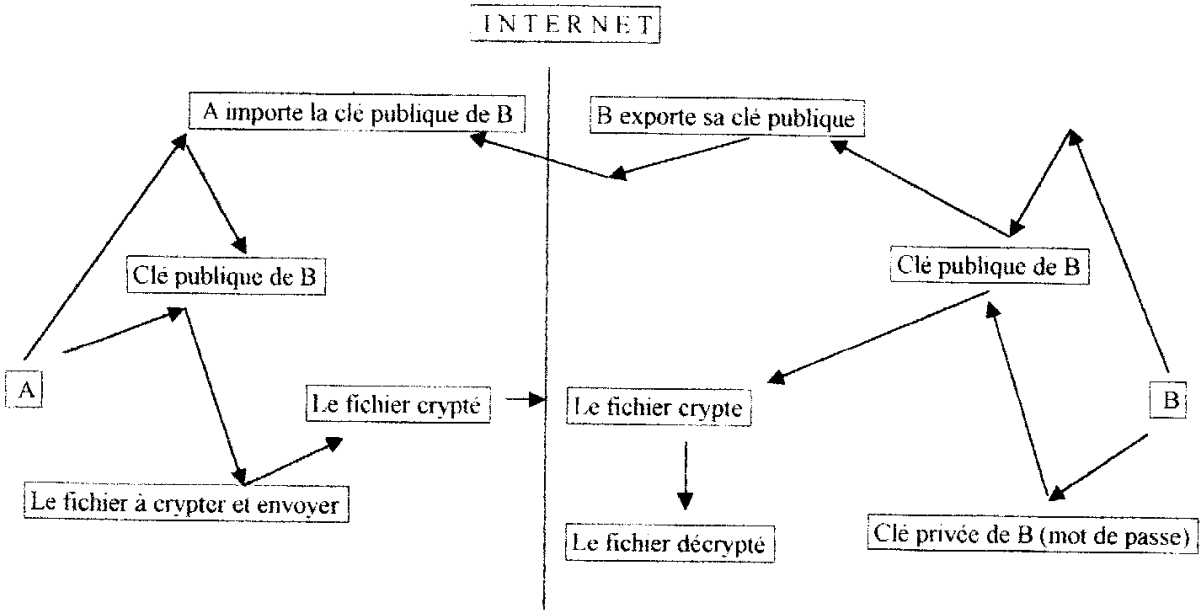
RIJNCRYPT2 v1.0.

Auteur : Florent Lejaxhe

Fonctionnement du programme.

Ce programme permet de crypter un fichier source grâce à une clé publique et n'autorise le décryptage que grâce à une clé privée (mot de passe). L'explication qui suit vous explique le fonctionnement shématique du programme et la sécurité du cryptage.

Principe général.

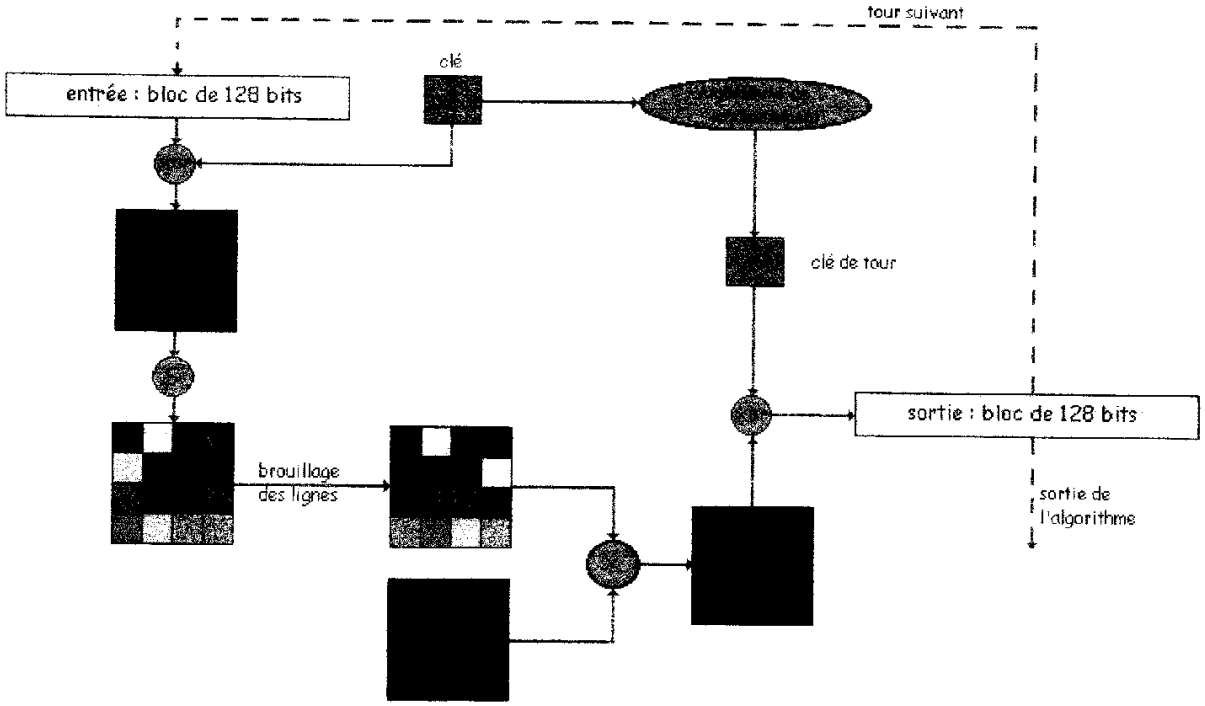


Ce principe général vous montre que le cryptage d'un fichier se fait, non pas à l'aide d'une clé personnelle, mais bien à l'aide de la clé publique du destinataire. C'est la raison pour laquelle le programme contient une « Génération de clé publique » (c'est le système qui la crée à la demande) et aussi une possibilité d' « Exportation de la clé publique » vers vos correspondants ou l'inverse.
C'est donc aussi pourquoi cette clé s'appelle « publique » : vos correspondants (en principe de confiance) la connaissent.
Lors de la réception du fichier crypté, le destinataire donne l'autorisation avec sa clé privée de décrypter le fichier (c'est sa clé publique qui réalise l'opération).
Si une personne intercepte (vole, détourne ou copie) le fichier, il lui est impossible de le décrypter, même si vous lui avez envoyé par erreur. Pourquoi ?
Mais, tout simplement (voir le shéma) pour deux bonnes raisons : le fichier qu'il reçoit à été crypté avec une autre clé publique que la sienne et le décryptage se fait avec une autre clé privée. Génial, non ? Ici non plus, pas d'inquiétude, c'est le programme qui gère tout : il vous suffit de lui dire à qui vous envoyez le fichier et il fait le reste. Ce double verrou ne laisse au voleur qu'une seule possibilité : essayer de découvrir la clé publique de

cryptage par « crackage » informatique. Cette opération n'est envisageable que par des Gouvernements ou des entreprises équipées d'ordinateurs ultra-performants pour réaliser l'opération en un temps acceptable. Même la connaissance et la détention du programme de cryptage (encore faut-il savoir quelle méthode a été employée) ne permet pas d'en connaître la clé. La raison est expliquée ci-dessous.

Un peu plus de détails.

En fait, le programme effectue beaucoup d'opérations et se base sur le fait que les voleurs de fichiers ne sont pas des enfants de cœur : ce sont des programmeurs chevronnés (parfois des professionnels payés par l'Etat), mathématiciens (avec une grosse bosse) qui mettent en œuvre des programmes de « cracking » sophistiqués. Pour eux, et uniquement pour eux (ils ont bien le droit de s'amuser eux aussi), le programme effectue les tâches suivantes :



Vous observez que le fichier à crypter est morcelé en blocs de 128 bits qui sont « travaillés » par la clé publique du correspondant (cette clé a été importée, vous vous rappelez ?). Ensuite les lignes sont mélangées, le résultat est multiplié par une matrice carrée, une clé de tour aléatoire est générée, celle-ci « travaille » le résultat et le bloc obtenu est réinjecté dans le circuit pour un nouveau tour : il y en a dix ! ... par bloc de 128 bits. Le bloc suivant subit le même sort, et ainsi de suite jusqu'à la fin du fichier. Les blocs sont ensuite réassemblés et cela constitue le fichier crypté. Le programme de décryptage doit réaliser l'inverse. Et les voleurs de fichier doivent découvrir ce qu'a fait le programme ! Cet algorithme « Rijndael », inventé par deux belges, a été choisi comme standard de cryptage par le Gouvernement américain en 2000 et c'est cet algorithme qu'utilise le programme « RijnCrypt2 » que j'ai mis au point. Il est donc sûr au niveau de la sécurité des données.

Fait à Bois de Lessines, le 5 décembre 2002
Florent Lejaxhe