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

RIJNCRYPT2 v1.0.

Auteur : Florent Lejaxhe

I. Installation.

1) Dézipper le package dans le dossier de votre choix. Je vous conseille néanmoins de créer un dossier spécial, par exemple : c:\Program Files\RijnCrypt2 qui se crée à partir de l' « Explorateur » Windows. Dans cet Explorateur, sélectionnez Program Files, puis « Fichier-Nouveau…-Dossier ». Une fenêtre intitulée « Nouveau dossier » apparaît dans le dossier Program Files et vous donne la possibilité de changer le nom. C'est là que vous pouvez taper « RijnCrypt2 » ou un nom de votre choix.
2) Le fichier de cryptage "RIJNDAEL2CLES.exe" se trouve donc dans le dossier "c:\ Program Files\CryptRijndael\ et peut être lancé de là mais il est préférable de créer un raccourci sur le bureau.
3) Le programme ne crée aucun fichier système : il se suffit à lui-même et ne perturbe en rien le système d'exploitation.

II. Utilisation.

Le programme a été conçu pour crypter les fichiers selon deux utilisations :

a) personnelle : il s'agit du cryptage des fichiers locaux ; dans ce cas, le programme remplace le fichier original par le fichier crypté, empêchant ainsi toute lecture (la phase d'essai du programme ne réalise pas cette opération).
b) Pour envois par E-mail (ou tout autre support) : dans ce cas, le programme effectue une copie cryptée du fichier, laissant l'original intact.

Exécutez "Rijndael2Clés.exe" grâce un double-clic sur le programme ou son raccourci.
Une fenêtre très simple apparaît avec les choix suivants :

1) Gestion des clés :

a) Générer votre clé publique : si vous avez bien compris le fonctionnement du cryptage à deux clés expliqué plus haut, vous savez que vous devez générer une clé publique lors du premier emploi du programme. C'est automatique : il suffit de demander. Cette option permet de changer de clé publique mais cette opération ne devrait normalement jamais avoir lieu car vos correspondants cryptent les fichiers qu'ils vous envoient grâce à cette clé (qu'ils ne connaissent pas mais le programme bien). Le programme vous demande une confirmation ainsi que votre mot de passe, ceci pour qu'une personne malintentionnée ne modifie votre Clé Publique.
b) Exporter votre clé publique. Quand votre clé a été générée, il faut l'exporter vers vos correspondant. Cette clé est un fichier binaire de 1 Ko que le programme copie dans un

endroit accessible et connu : « Mes documents ». Ce fichier sera mis en pièce-jointe des E-mail que vous enverrez à vos correspondants. Il vous appartient de détruire cette copie lorsque les envois seront effectués. Puisque nous sommes dans le domaine de la sécurité, sachez que la destruction sous Windows met votre fichier dans la « corbeille » et n'est donc pas détruit. A vous de vider votre corbeille contenant la clé.

c) Importer une clé publique. Si vos correspondants acceptent de crypter à l'aide du même programme que vous, ils vont donc vous envoyer leur clé publique (c'est avec elle que vous allez crypter les messages à leur intention ; la clé est donc différente pour chaque contact E-mail, mais c'est le programme qui gère le tout). Celle-ci sera une pièce-jointe de 1 Ko (voir ci-dessus) que vous allez sauver dans « Mes documents » … obligatoirement. C'est à ce moment que vous allez « importer » la clé publique de votre correspondant. Le terme « importer » signifie que le programme va chercher la clé dans « Mes Documents » et la sauver dans un endroit connu de lui. Il vous demande préalablement l'adresse E-mail du correspondant (le programme accepte toute chaîne de caractère : le nom et le prénom par exemple).

d) Modifier le mot de passe.(la Clé Privée) Cette option n'est possible que si le mot de passe actuel est donné. Cette opération peut être réalisée de temps en temps car la connaissance de cette Clé Privée donne accès à toutes les possibilités du programme. Il ne faut donc l'écrire nulle part mais la retenir. L'existence d'un autre mot de passe pour l'accès à l'ordinateur réduit considérablement cette faille potentielle du système. (deux possibilités qui peuvent être cumulées : au démarrage du DOS et au moment de l'ouverture du Windows ; les deux en même temps sont à déconseiller car l'oubli de l'une des clés est catastrophique). Il existe aussi une clé dans le traitement de texte Word qui empêche l'ouverture et/ou la modification du document).

e) Modifier une adresse E-mail. Cette option modifie l'adresse (ou le nom si c'est ça que vous avez entré la première fois) du correspondant sans modifier sa clé publique. Vous ne pouvez pas modifier votre appellation « Ma clé publique » car c'est une constante système.

f) Modifier une clé publique. Cette option n'existe pas ! Et pour cause : il vous suffit de supprimer la personne de l'agenda (Voir ci-après « Supprimer une adresse E-mail », sa Clé Publique se supprime également) et d'importer la nouvelle clé publique.

2) Adresse E-mail :

a) Supprimer une adresse E-mail. Lorsque vous ne correspondez plus avec quelqu'un, vous avez la possibilité de le supprimer de votre agenda. Attention, cette option supprime la clé publique de cette personne et vous ne saurez donc plus crypter de message à son intention. En cas de suppression par mégarde, rien de grave, demandez-lui sa clé publique et importez-la à nouveau.

b) Modifier une adresse E-mail. Le programme remplace l'ancienne adresse par la nouvelle sans toucher à la clé publique de la personne concernée.

c) Modifier une clé publique. Cette option n'a pas été programmée car il suffit de supprimer l'adresse (ce qui supprime sa clé publique) et d'importer la nouvelle clé (le programme demande la nouvelle adresse).

3) Les boutons.

a) Choix. C'est là que vous sélectionnez le fichier à crypter.

b) Crypt / Décryp. Le programme reconnaît automatiquement l'opération à réaliser mais demande de sélectionner l'adresse ou le nom du correspondant dans l'agenda visible dès l'ouverture du programme. Dans le cas d'un cryptage local, sélectionnez « Ma clé publique ». Vous aurez compris qu'un fichier crypté pour usage local ne peut pas être lu par vos correspondants (personne d'autre que vous ne pouvez le lire).

c) Aide. - Ce document.
- Mes coordonnées : E-mail : florent.lejaxhe@skynet.be
URL : http://www.groopy.be/florentlejaxhe et
http://users.skynet.be/florent.lejaxhe

d) Niveau de cryptage. Le niveau 2 provoque un deuxième tour de cryptage de la clé publique. A l'heure actuelle, le code Rijndael est réputé inviolable car l'algorithme inverse n'existe pas (il n'a pas été découvert). Seule la force brute des ordinateurs liée à leur vitesse de traitement permettrait de casser le code. Au niveau 1, il est possible que le « crakage » intervienne dans 15 ou 20 ans suite aux progrès techniques. Au niveau 2, cela est rigoureusement impossible, sauf si l'algorithme inverse venait à être trouvé. Par défaut, le niveau de cryptage est 1.

e) Quitter. Quit !

4) Les Flash-Infos. Des informations vous sont données sur :

a) La taille du fichier.
b) Les temps de cryptage / décryptage.
c) La vitesse réalisée.
d) Ce que fait le programme en cours et le bon aboutissement des demandes.

5) Suppression de fichiers.

L'onglet « Suppress Fich » permet de supprimer des fichiers de manière sécurisée, c'est-à-dire sans possibilité de les lire. Habituellement, lorque l'on supprime un fichier, celui va dans la « Poubelle », donnant ainsi l'occasion d'aller le récupérer en cas d'erreur. Celle-ci est vidée périodiquement de son contenu qui n'est théoriquement plus accessible mais il existe des programmes qui sont capables d'aller les récupérer. Ce fait peut être inadmissible pour des fichiers dits « sensibles » où on désirerait une suppression définitive et sans appel. C'est ce que réalise cet onglet selon le procédé suivant : le fichier est crypté à l'aide d'une clé aléatoire perdue puis vient remplacer (donc sans destruction) le fichier origine qui est écrasé. Le fichier crypté est enfin détruit et seule cette version est récupérable par des spécialistes mais définitivement illisible. A utiliser avec prudence !

III. Facilités. Les manipulations ont été réduites au maximum pour permettre un confort de cryptage / décryptage optimal.

IV. Performances. Le programme crypte et décrypte à une vitesse approximative de 700 Ko/s avec un Pentium 450 MHz au niveau 1 (la moitié au niveau 2). Les applications «on line » peuvent ralentir fortement cette vitesse ; ainsi, un FireWall la fait chuter à 100 Ko/s et l'ajout d'un gestionnaire de mémoire la fait descendre à 20 Ko/s. L'application vous indique cette performance.

V. Système d'exploitation : Windows 9X, Millénium, XP.

VI. Sécurité.

1) Le programme est garantit sans virus.
2) L'algorithme de cryptage est professionnel et sûr.
3) Pour augmenter la sécurité, il est possible d'installer les fichiers sur un autre support (Disquette, CD-R-RW, Zip, etc ...). Pour ce faire, copier le dossier entier "\CryptRijndael\" de "C:\Program Files\CryptRijndael\" sur l'autre support. Celui-ci contiendra donc : "*\ CryptRijndael*.*" (les étoiles remplacent la lettre du support – A, C, D, E, F, …- ainsi que les noms des fichiers et leur extension). Il est alors possible de supprimer le dossier "CryptRijndael" du disque dur, rendant ainsi impossible le décryptage local sans le support de sauvegarde. Attention, il est obligatoire de copier le dossier et pas seulement les fichiers.

VII. Remarques.

1) Le cœur du programme étant la version officielle du code Rijndael, il est définitif. Cela signifie donc que les versions ultérieures seront toujours compatibles entre elles et que les fichiers cryptés par l'une des versions pourront toujours être décryptés par une autre. Seuls le « look » et la convivialité du programme sont susceptibles de changer suite aux remarques des utilisateurs.
Les améliorations des versions ultérieures se situent au niveau des fonctionalités liées à Internet et à l'envois des E-mails, en particulier une intégration plus poussée du programme dans l'environnement Windows.
2) Ce programme est disponible gratuitement.

J'espère que vous aurez beaucoup de plaisir à utiliser ce programme et que votre intimité épistolaire sera efficacement préservée.

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