PGP - PRETTY GOOFY PRIVACY
PROJET D'IMPLEMENTATION DU CHIFFREMENT RSA

Boris Ho - Pauline de Bouet du Portal

EISTI - Mars 2015

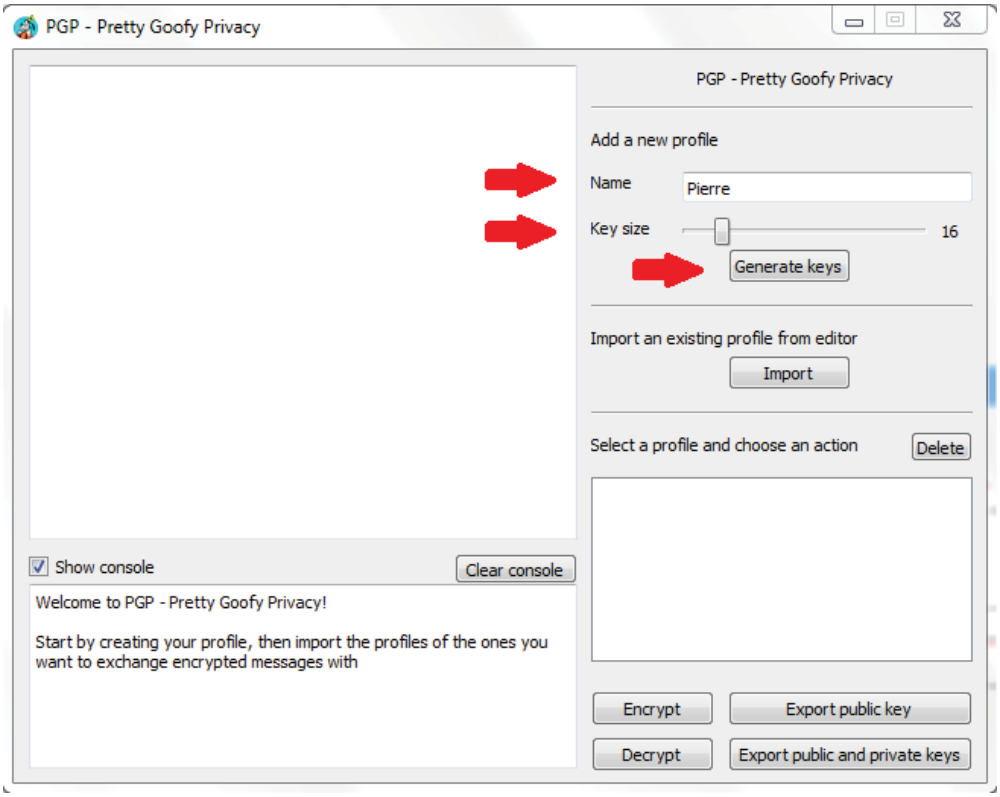
GUIDE D'UTILISATION

Le logiciel s'appelle PGP - Pretty Goofy Privacy, nom librement inspiré du logiciel de chiffrement PGP (Pretty Good Privacy) créé par Phil Zimmermann en 1991.

CREATION D'UN PROFIL

Pour créer un profil et générer les clés publique et privée associées, renseignez un nom, choisissez une longueur pour la clé en bits et cliquer sur Generate keys.

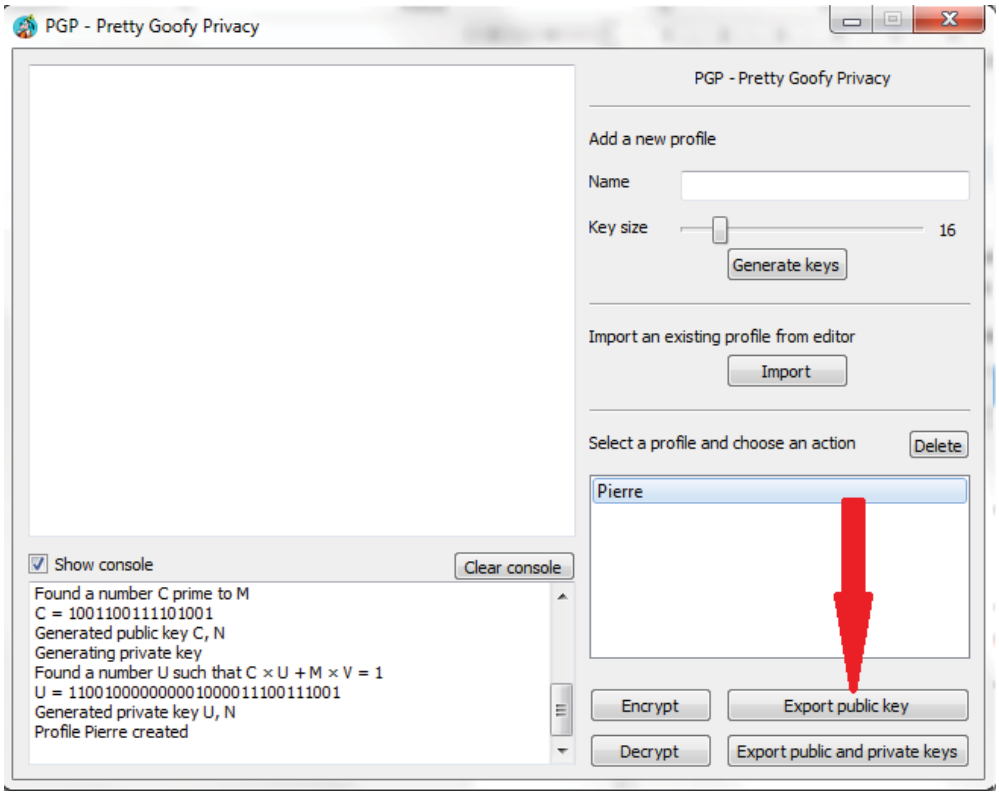
La Key size correspond en fait à la longueur maximale en bits des nombres P et Q utilisés pour générer les clés.



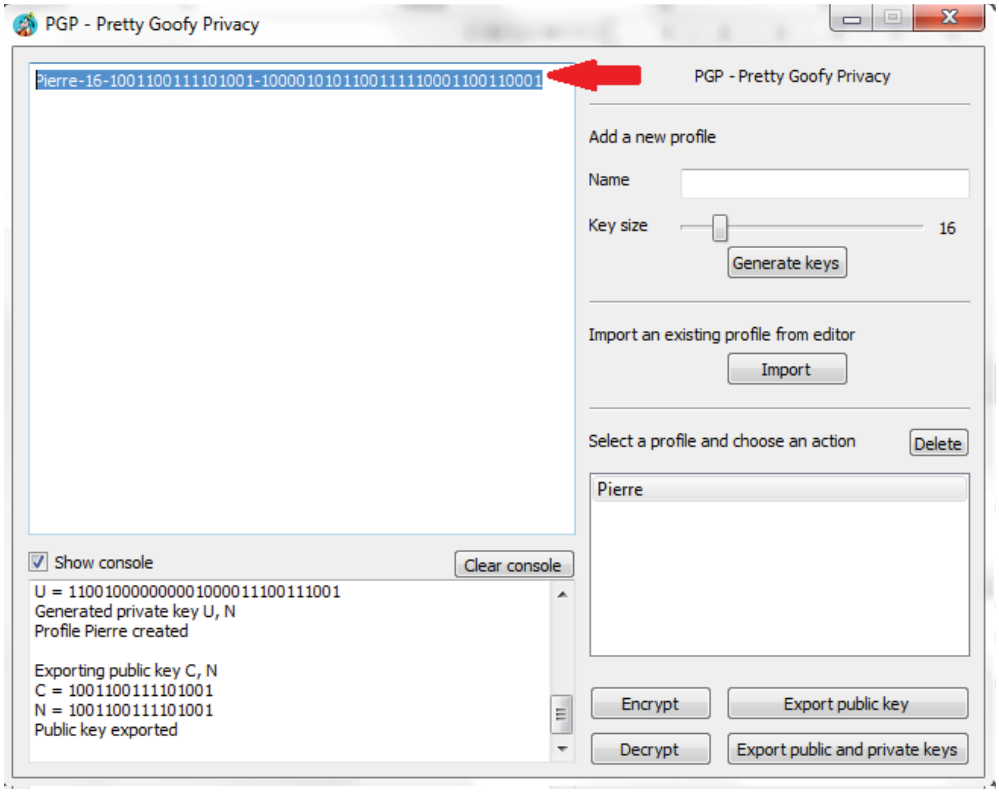
EXPORT DE LA CLE PUBLIQUE

Après avoir créé votre profil, celui-ci apparaîtra dans la liste de profils. Cliquez dessus puis sur le bouton Export public key pour exporter votre clé publique dans l'éditeur de texte.

(N'exportez pas votre clé privée, elle ne doit être connue que par vous)

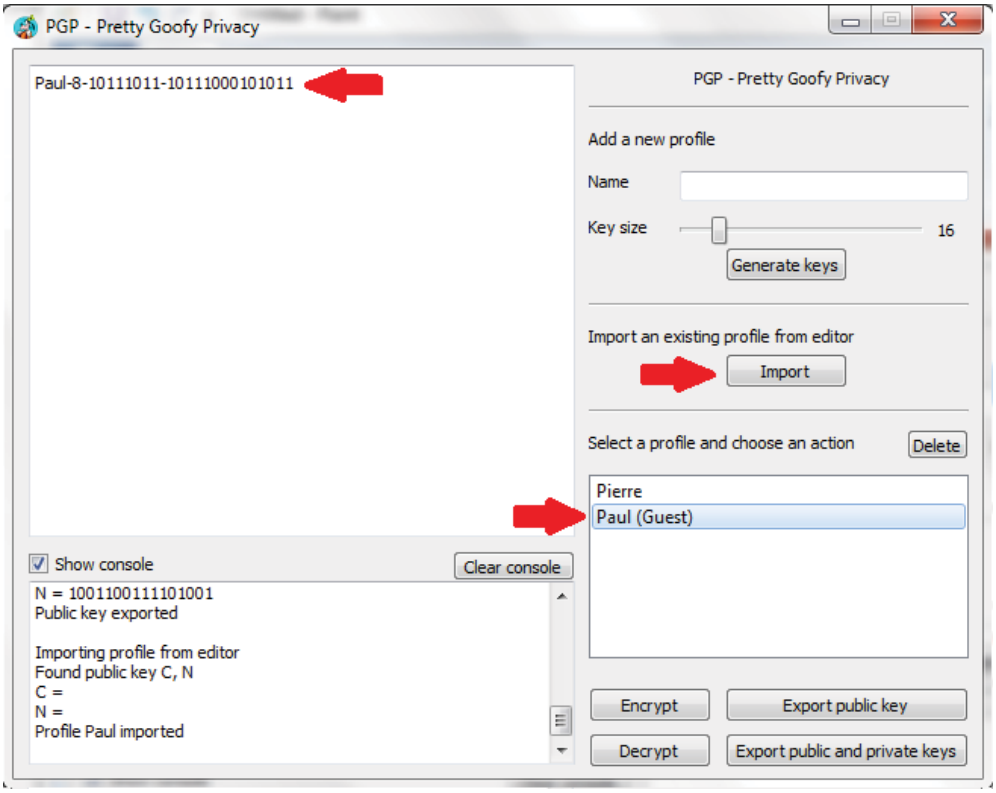


Copiez le texte affiché dans l'éditeur et transmettez-le à la personne avec qui vous voulez communiquer.



IMPORT D'UN PROFIL

Dites à votre interlocuteur d'effectuer les mêmes étapes de son côté avec le programme. Une fois qu'il vous aura transmis son profil qu'il aura exporté, importez-le dans votre programme en le collant dans l'éditeur de texte, puis en cliquant sur Import.

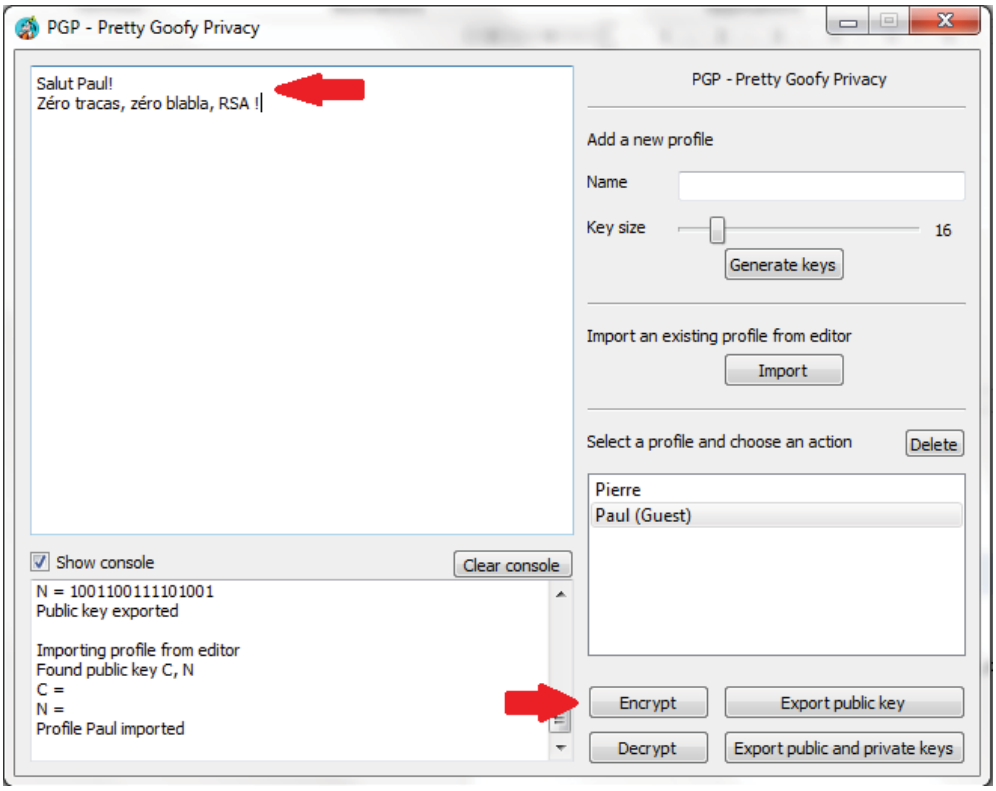


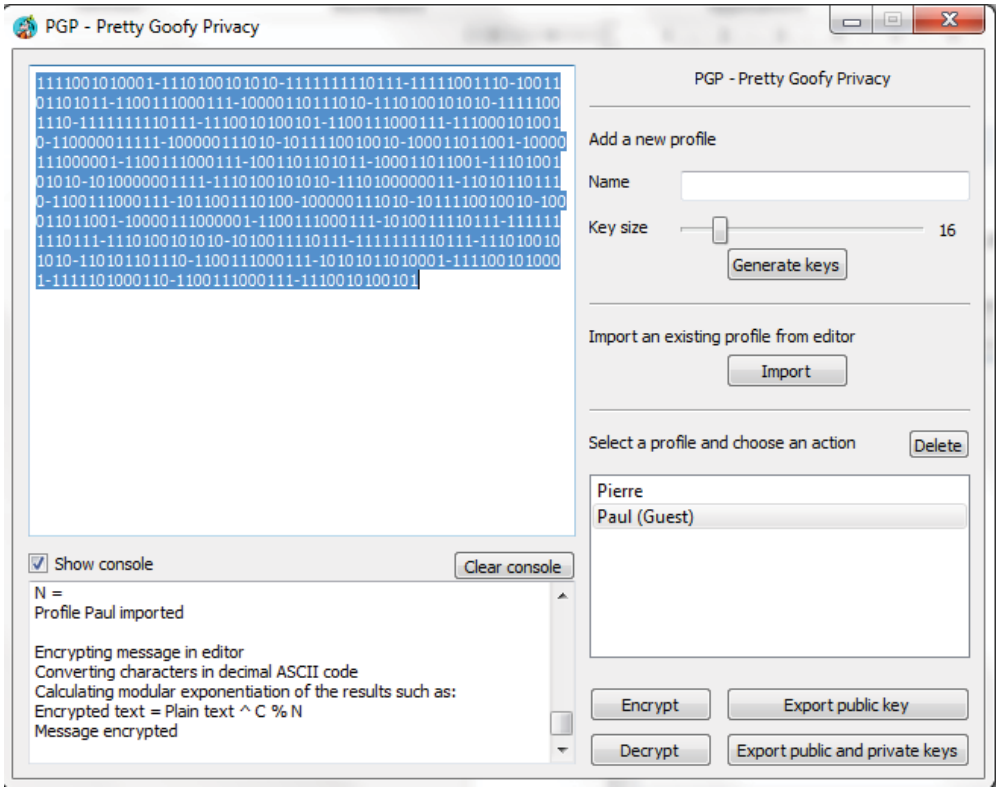
Les profils marqués comme Guest signifie que vous n'avez que la clé publique de ce profil et pas la clé privée. Vous pouvez chiffrer des messages avec mais pas en déchiffrer.

CHIFFREMENT D'UN MESSAGE

Ecrivez votre message dans l'éditeur de texte, puis sélectionner le profil à qui vous souhaitez transmettre le message, puis cliquez sur Encrypt.

(Le programme gère mal le chiffrement des caractères à accents)





Copiez le message chiffré et transmettez-le à votre interlocuteur.

DECHIFFREMENT D'UN MESSAGE

Pour déchiffrer un message que votre interlocuteur vous a envoyé, copiez ce message dans l'éditeur de texte, sélectionnez votre profil dans la liste de profils et cliquez sur Decrypt.