UFR de mathématique et d'informatique
Université de Strasbourg

MASTER INFORMATIQUE

UE Sécurité

TP n°2

Chiffrement asymétrique - GPG

1. Exercice 1 : RSA 1024

1. Utilisez openssl pour générer une paire de clés RSA dans un fichier testCle.pem et protégez la clé privée en utilisant 3DES.
2. Visualisez le contenu du fichier testCle.pem, que peut-on en conclure ?
3. Décodez le fichier testCle.pem et afficher l'exposant et le modulus.
4. Affichez la clé publique.
5. Envoyez à une autre personne de la salle un fichier court (20 caractères) *short_text* chiffré en RSA de façon à ce qu'elle seule puisse le déchiffrer.
6. Faites de même avec un fichier très volumineux (RFC8017.txt sur MOODLE) *long_text*. L'échange doit demeurer confidentiel comme précédemment.
7. Que constatez- vous ?
8. Mettez en œuvre une autre solution avec *openssl* afin de transmettre ce fichier *long_text* de manière sécurisée
9. Maintenant que vous pouvez chiffrer vos échanges, faites-en sorte de garantir l'intégrité en utilisant une signature.
10. Votre solution garantit-elle également l'authentification des échanges?

2. Exercice 2 : GnuPG

GnuPG est un implémentation opensource de PGP, disponible dans le RFC 4880. Cette suite GnuPG vous permet de générer vos clefs PGP, avec lesquelles vous pouvez chiffrer et signer des documents. Vous pouvez également diffuser vos clefs à l'aide de serveurs de clefs et ainsi accéder facilement à celles des autres. Vous pourrez en profiter pour signer les clefs de personnes de confiance.

1. En utilisant GPG, chiffrez un message à l'aide d'une clé symétrique et déchiffrez-le à nouveau.
2. Générez une paire de clés correspondants à votre identité réelle
3. Maintenant que nous avons nos clés, nous voulons les partager au monde entier, et on ne va pas s'amuser à envoyer notre clé publique à chaque correspondant, on va la mettre sur un serveur d'échange de clés. Envoyer votre clé sur un serveur d'échanges http://keys.gnupg.net.
4. Récupérez la clé publique d'une personne de votre groupe via le serveur d'échange.
5. Peut-on être certain de l'identité du possesseur de la clé gpg ?
6. Chiffrez en asymétrique un fichier *secret_Nom_destinataire.gpg* à destination d'une autre personne de votre
7. Déchiffrer un fichier secret à votre attention provenant d'une autre personne de votre groupe
8. Chiffrez et signez un nouveau fichier *secret_Nom_destinataire_signe.gpg* à destination d'une autre personne de votre groupe et transférez-lui ce fichier.
1. Vérifiez la signature du fichier réceptionné et déchiffrer celui-ci avec votre clé privée.
2. Établissez une "Toile de confiance" en signant les clés des membres du groupe. Le concept est la "keysigning party" où par votre signature vous confirmez (avec un certain niveau de confiance) le lien entre l'identité réelle (Carte d'identité…) et la clé gpg proposée. Attention cependant à ne pas signer n'importe-quelle clé. La clé ainsi signée peut-être renvoyée sur un serveur de clé

3. Exercice BONUS : Messagerie et GPG

1. Implémentez votre clés GPG dans un client de messagerie et envoyer un message signé et chiffré à une personne de votre groupe