TP n°2

Chiffrement asymétrique - GPG

1. Exercice 1 : RSA 1024

1. Utilisez openssl pour générer une paire de clés RSA de 1024 bits dans un fichier testCle.pem en la protégeant avec 3DES.
2. Décodez le fichier testCle.pem et affichez l'exposant et le modulus.
3. Extraire la clé publique dans un fichier VOTRENOM_PUB.pem
4. 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.
5. Faites de même avec un fichier très volumineux (par exemple RFC8017.txt) long_text. L'échange doit demeurer confidentiel comme précédemment. Que constatez- vous ?
6. Mettez en œuvre une autre solution asymétrique avec *openssl* afin de transmettre ce fichier long_text de manière sécurisée
7. Maintenant que vous pouvez chiffrer vos échanges, faites-en sorte de garantir l'intégrité en utilisant une signature.
8. Votre solution garantit-elle également l'authentification des échanges ?

2. Exercice 2 : GnuPG

GnuPG est une implémentation opensource de PGP, disponible dans le RFC 4880. Cette suite GnuPG vous permet de générer vos clés PGP, avec lesquelles vous pouvez chiffrer et signer des documents. Vous pouvez également diffuser vos clés à l'aide de serveurs de clés et ainsi accéder facilement à celles des autres. Vous pourrez en profiter pour signer les clés 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 asymétriques correspondants à votre identité réelle
3. Maintenant que nous avons nos clés, nous voulons partager la clé publique au monde entier, et nous n'allons pas l'envoyer à chaque correspondant. Nous allons la déposer sur un serveur d'échange de clés. Envoyez votre clé sur le serveur d'échanges keyserver.ubuntu.com
4. Récupérez la clé publique d'une personne de votre groupe via ce serveur d'échange.

5. Peut-on être certain de l'identité du possesseur de la clé gpg ?
6. Chiffrez en asymétrique un fichier secret.gpg à destination d'une autre personne de votre groupe à l'aide de sa clé publique
7. À l'aide de votre clé privé, déchiffrez le fichier secret secret.gpg provenant d'une autre personne de votre groupe
8. Chiffrez et signez un nouveau fichier secretSi*gne.gpg* à destination d'une autre personne de votre groupe et transférez-lui ce fichier.
9. Vérifiez la signature du fichier réceptionné et déchiffrez celui-ci avec votre clé privée.
10. 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 noté

Pour cet exercice, nous vous demandons de répondre à ces quelques questions de manière synthétique.

Votre synthèse devra être déposée au format pdf sur Moodle avant le dimanche 27 novembre.

1. Quelle est la différence technique entre les certificats X509v3 et les couples de clés GNUPG ?
2. Quel mécanisme permet de vérifier l'authenticité d'un certificat X509v3 ?
3. Quelles sont les limites d'utilisation et les contextes d'usage de GnuPG ?
4. Quels sont les différentes contextes d'utilisation d'un certificat X509v3 ?
5. Quelle confiance peut-on accorder à l'usage des certificats X509v3?
6. Que penser de Let's Encrypt ? Avantages/inconvénients/limites.