Sécurité - TD 2

21 septembre 2018

1 Exercice 1 : Chiffrement symétrique vs asymétrique

1. $\sum_{i=1}^{n-1} = \frac{(n-1)(n-2)}{2}$ avec $n = 7$, il faut donc 21 clés symétriques.
2. AES car il est un standard fiable.
3. 7, une clé privé et une publique par personne.
4. Sa clé privé et la clé publique d'Alice.
5. RSA
6. Chiffrement plus rapide, possibilité de signature par l'expéditeur

2 Exercice 2 : Clé privée

1. Non il ne peut plus envoyer de courriers électroniques. Il peut en recevoir car il à toujours sa clé publique.
2. Il ne peut pas signer ses courriers mais peut vérifier la signatures de ceux qu'il reçoit.
3. Il doit créer un nouveau couple de clés privée/publique.

3 Exercice 3 : Certificats

1. Fichier contenant des informations tel que l'identité du signataire, l'algorithme de chiffrement, la clé publique du titulaire, etc...
2. La différence majeure est que les certificats PGP n'ont pas d'autorités de certifications.
3. Vérification de la présence du certificat dans le magasins de certificats du navigateur.

4 Exercice 4 : Certificats

1. Le signataire des deux certificats est le même
2.
3.

5 Exercice 5 : Attention connexion non certifiée

6 Exercice 6 : Diffie-Hellman

7 Exercice 7 : RSA

$$
\begin{aligned}
(n, e) &= (33, 3) \\
n &= 33 = 3 * 11 \text{ (Nombre premiers)} \\
p &= 3 \\
q &= 11 \\
e * d &= 1 \ \% \ (p-1)(q-1) \\
e * d &= 1 \ \% \ 20 \\
3 * d - 1 &= 20 \\
\frac{d}{3} &= \frac{21}{3} \\
d &= 7 \\
\text{Clé privée (n,d)} &= (33, 7)
\end{aligned}
$$