Petit Wesley

TP2 – Sécurité des réseaux et du Web

1. a) openssl rsa -in PETW04119907-publique.pem -pubin -text -noout

b) Le modulus (n) de mon fichier est 3 492 413 941, à l'aide du site suivant : http://www.factordb.com/index.php?query=3492413941 on retrouve p = 54563 et q = 64007 (n = pq).

On sait que φ(n) = (p - 1) * (q – 1), soit φ(n) = 54562 * 64006 = 3 492 295 372.

On a utilisé φ(n) = 3 492 295 372 pour générer ma clé.

2. a) openssl genrsa 1024

b) openssl genrsa -out CleEtudiant.pem 1024

c) openssl req -x509 -new -key CleEtudiant.pem -days 7 -nodes

d) openssl req -x509 -new -key CleEtudiant.pem -out CertificatEtudiant.pem -days 7 -nodes

3. a) Avec la commande ci-dessous, on obtient la date d'expiration : « Dec 25 22:42:52 2013 GMT ». Le certificat est donc expiré depuis près de 6 ans, il est donc inutilisable le jour de l'examen final de ce cours (le 16 décembre 2019).

Commande : openssl x509 -in Certificat.pem -noout - dates

b) openssl x509 -in Certificat.pem -pubkey -out PublicKey.pem, Commande pour extraire la clé public du certificat.

openssl rsautl -encrypt -in Equipe.txt -inkey PublicKey.pem -pubin -out Equipe-chiffre.txt, Chiffre le fichier avec la clé public.

4. Ce certificat peut protéger l'université contre ce genre d'attaque, car il permettra de garantir l'identité du site de l'UQAC grâce à la signature d'une autorité externe. L'autorité externe ayant vérifié l'identité de l'uqac.ca avant de l'enregistrer. Ce certificat permettra à l'utilisateur de distinguer les deux sites.

5. a) Le certificat n'est pas auto-signé, car il a été signé par GTS CA 101.

b) Le certificat expire le 02/01/2020.

c) SHA-256 est la fonction de hachage utilisé pour signer le certificat.

d) La clé publique de Google contient 256 bits.