web et sécurité

TP1 L'outil OpenSSL

Exercices 01

1. Quelle version de TLS est utilisée ?
   Sur openSSL on trouve **TLSv1.**
2.

Google chrome

- **https://www.facebook.com/**

  - ✓ La version de TLS utilisée est : **TLS 1.2.**
  - ✓ La suite chiffrante est **ECDHE_ECDSA** with P-256 (a strong key exchange), and **AES_128_GCM** (a strong cipher).

ECDHE :
Algorithme d'échange de clés diffie-helman **asymétrique.**

ECDSA :
Algorithme de signature et de hachage : **asymétrique.**

AES_128_GCM :
Algorithme de chiffrement : **symétrique.**

- ✓ **Les objectifs :**
  L'Intégrité des données, la non répudiation, Garantir la confidentialité et l'authentification.

- **https://dpt-info-sciences.univ-rouen.fr**

  - ✓ La version de TLS utilisée est : **TLS 1.2.**
  - ✓ La suite chiffrante est **ECDHE_RSA** with P-256 (a strong key exchange), and **AES_256_GCM** (a strong cipher).

ECDHE :
Algorithme d'échange de clés diffie-helman **asymétrique.**

RSA :
Algorithme de signature et de hachage : **asymétrique.**

AES_256_GCM :
Algorithme de chiffrement : **symétrique.**

- ✓ **Les objectifs :**
  L'Intégrité des données, la non répudiation, Garantir la confidentialité et l'authentification.

https://www.globetrotter.ch/

- ✓ La version de TLS utilisée est : **TLS 1.0.**
- ✓ The connection to this site uses TLS 1.0 (an obsolete protocol), **RSA** (an obsolete key exchange), and **AES_128_CBC** with **HMAC-SHA1** (an obsolete cipher)

RSA :
Algorithme de signature et de hachage : **asymétrique.**

AES_128_CBC :
Algorithme de chiffrement : **symétrique.**

HMAC :
C'est pour l'authentification et l'intégrité des données.

SHA1 :
Fonctions de hachage.

- ✓ **Les objectifs :**
  L'Intégrité des données.

Firefox

- **https://www.facebook.com/**

  - ✓ La version de TLS utilisée est : **TLS 1.2.**
  - ✓ La suite chiffrante est **ECDHE_ECDSA** with P-256 (a strong key exchange), and **AES_128_GCM** (a strong cipher).

ECDHE :
Algorithme d'échange de clés diffie-helman **asymétrique.**

ECDSA :
Algorithme de signature et de hachage : **asymétrique.**

AES_128_GCM :
Algorithme de chiffrement : **symétrique.**

SHA256 :
Fonctions de hachage.

- ✓ **Les objectifs :**
  L'Intégrité des données, la non répudiation, Garantir la confidentialité et l'authentification.

- **https://dpt-info-sciences.univ-rouen.fr**

  - ✓ La version de TLS utilisée est : **TLS 1.2.**
  - ✓ La suite chiffrante est **ECDHE_ECDSA** with P-256 (a strong key exchange), and **AES_128_GCM** (a strong cipher).

ECDHE :
Algorithme d'échange de clés diffie-helman **asymétrique.**

RSA :
Algorithme de signature et de hachage : **asymétrique.**

AES_128_GCM :
Algorithme de chiffrement : **symétrique.**

SHA256 :
Fonctions de hachage.

✓ **Les objectifs :**

L'Intégrité des données, la non répudiation, Garantir la confidentialité et l'authentification.

https://www.globetrotter.ch/

✓ La version de TLS utilisée est : **TLS 1.0.**

DHE :

Protocole diffie helman pour échange de clé : **asymétrique.**

RSA :

Algorithme de signature et de hachage : **asymétrique.**

AES_128_CBC :

Algorithme de chiffrement : **symétrique.**

SHA128 :

Fonctions de hachage.

✓ **Les objectifs :**

L'Intégrité des données.

OpenSSL

- **https://www.facebook.com/**

  - ✓ La version de TLS utilisée est : **TLSv1**
  - ✓ L'algorithme de chiffrement est **AES128.**
  - ✓ La fonction de hachage est **sha 2.**

- **https://dpt-info-sciences.univ-rouen.fr**

  - ✓ La version de TLS utilisée est : **TLSv1**.
  - ✓ L'algorithme de chiffrement est **AES256.**
  - ✓ La fonction de hachage est **sha 2**.
  - ✓ L'algorithme de signature est **RSA**.
  - ✓ L'algorithme d'échange de clé est diffie helman **DHE.**

- **https://www.globetrotter.ch/**

  - ✓ La version de TLS utilisée est : **TLSv1**.
  - ✓ L'algorithme de chiffrement est **AES256.**
  - ✓ La fonction de hachage est **sha 2**.
  - ✓ L'algorithme de signature est **RSA**.
  - ✓ L'algorithme d'échange de clé est diffie helman **DHE.**

Remarque :

- Pour les algorithmes de chiffrement **symétriques** ils sont par bloc.
- Pour les algorithmes de chiffrement **asymétrique** les problèmes mathématiques sur lesquels sont fondés leur sécurité est le logarithme discret ainsi que la factorisation des nombres premiers.
  « difie helman résiste au problème de logarithme discret, RSA résiste au problème de factorisation de deux nombre premiers ».

- Les déférents objectifs sont :

  - ➢ L'intégrité des données, la non répudiation, l'authentification et la confidentialité.
  - ➢ L'intégrité des données est assurée par la fonction de hachage.
  - ➢ La confidentialité est assurée par le chiffrement.
  - ➢ L'authentification c'est grâce au HMAC.
  - ➢ Le non répudiation est assuré par l'algorithme de signature.

3. Ce n’est pas les mêmes suites chiffrantes entre les différents navigateurs et OpenSSL.

// Utilisation de whireshark

Les suites chiffrantes utilisées peuvent différer d'un client a l'autre parce que l'ors de l'envoie de paquet client_hello une liste de suites chiffrantes est envoyées au serveur par ordre de priorité, et le serveur réponds en choisissant la plus prioritaires des suites supporter par le serveur et le client, donc deux client différents peuvent envoyés des suites chiifrantes différentes selon leurs système.

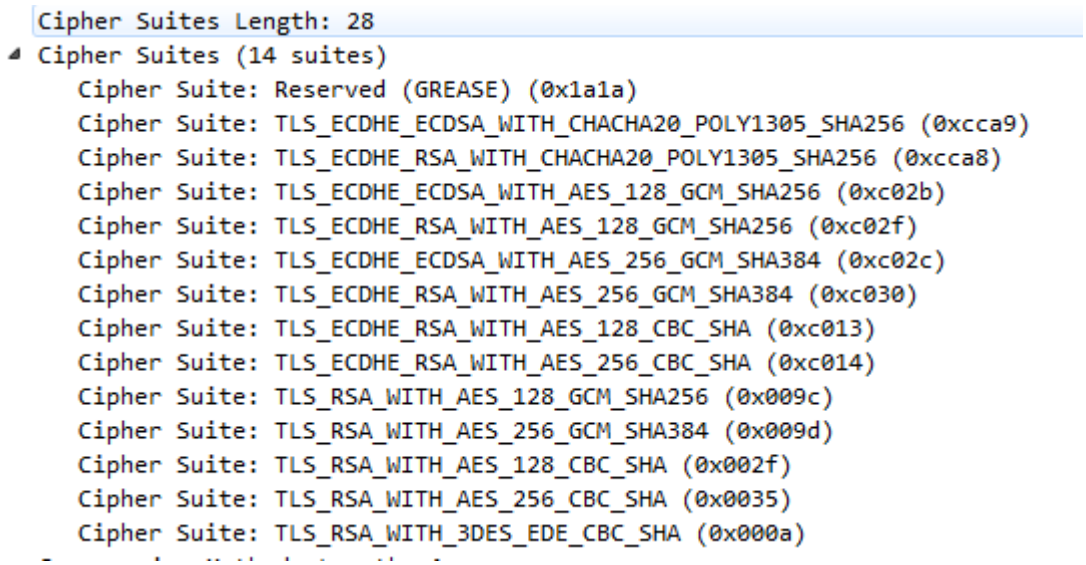

Figure 1 : Liste de suites chiffrantes supportées par le client.

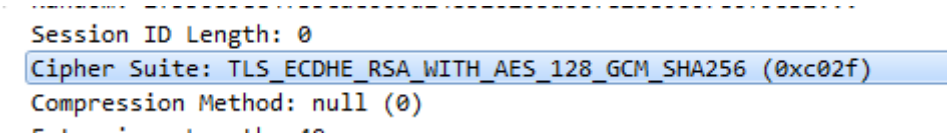

Figure 2 : La suite chiffrante choisis par le serveur.

4. Un **master-key** sert à l'échange des clés, cette dernières est générée aléatoirement.

5. L'erreur code 20 signifie qu’on ne peut pas déterminer le certificat de l'émetteur local, parce que on possède aucune certificat.

Exercices 02

1. Q