**Aubrée Romain** **Beauvallet**
**20/11/2025**

**Groupe 1**

# Bloc 3 TH 2 TP 2

# Exercice 1.1.1

Ils ont visé la composante référentielle (le nom de domaine/adresse IP) et, par extension, l'image/réputation de l'organisation.

# Exercice 1.1.2

- Le poste du hackeur envoie une requête vers le serveur DNS.
- Le serveur DNS interroge un serveur externe et reçoit une fausse réponse du serveur DNS du pirate, qui contient une adresse IP/nom de domaine erronée pour “tradec.com”. C'est l'injection de la fausse information dans le cache du serveur DNS.
- Réponse au poste du hackeur
- Le poste d'un salarié de TRADEC envoie une requête au nom de domaine (pour “tradec.com”) au serveur DNS.
- Le serveur DNS de TRADEC (piraté) répond au salarié avec l'adresse IP du serveur web du hackeur.
- Le salarié se connecte ensuite au serveur web du hackeur, où ces informations personnelles (mot de passe, nom utilisateur) pourraient être volées.

# Exercice 1.2.1-5

Impossibilité de faire les 5 exercices, je n’ai pas réussi a trouvé une version fiable de **Packet Tracer** sur internet (certain site non officiel le propose mais peuvent contenir des virus ou autres).

# Exercice 1.3.1

La signature doit avoir :

- L'auteur identifié.
- Lien prouvé (le système doit garantir que c'est bien la personne identifiée qui est à l'origine du contrat).
- Aucune modification après signature.
- L'accord client est donné.

# Exercice 1.3.2

La vérification est faite avec un système de “chiffrement asymétrique”. Un logiciel crée une empreinte numérique du contrat, qui est codée grâce à la clé privée de l'auteur qui est dans son certificat. La vérification est faite en utilisant la clé publique correspondante pour décrypter cette empreinte et s'assurer que le contrat n'a pas été modifié et qu'il vient bien de l'auteur déclaré.

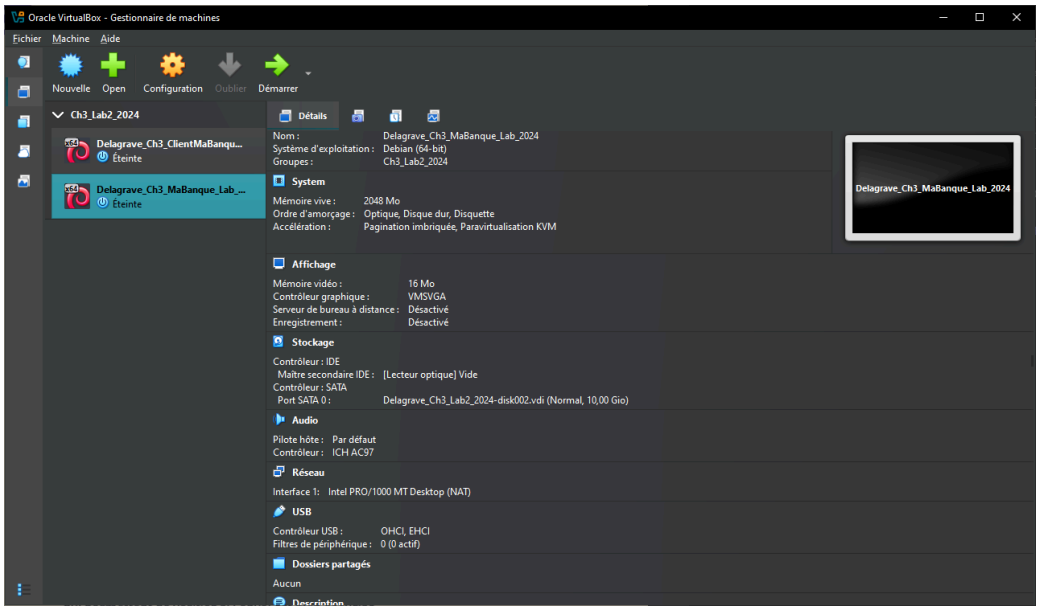
# Exercice 1.3.3

La signature électronique permet de faciliter la gestion du dossier et de signer à distance.

# Exercice 1.3.4

- Le contrat pourrait ne pas être considéré comme valable légalement.
- Le client pourrait dire que le contrat a été modifié après signature.
- Si les concurrents utilisent tous le format numérique, ça sera un désavantage car signer un contrat serait plus lent (papier) contrairement au concurrent.

# Exercice 2.1




# Exercice 2.2

M@Banque : Création du compte **“MaBanque”** avec l'adresse fictive *mabanque1987@gmail.com*.

ClientM@Banque : Création du compte **“Client-MaBanque”** avec l'adresse fictive *clientmabanque1987@gmail.com*.

# Exercice 2.3

Le contenu du message n'est pas crypté, il serait lisible par un attaquant interceptant le trafic.

# Exercice 2.4

Génération d’une paires de clés, une nouvelle paire de clés OpenPGP a été générée pour chaque utilisateur (MaBanque et Client-MaBanque) via les paramètres de compte Thunderbird.

La clé publique de MaBanque a été envoyée par courriel à Client-MaBanque.

La clé publique de Client-MaBanque a été envoyée par courriel à MaBanque.

Chaque utilisateur a importé la clé publique reçue de son correspondant dans son gestionnaire de clés OpenPGP.

# Exercice 2.5

L'envoi d'un mail de MaBanque vers Client-MaBanque avec l'option **"Chiffrer le message"** activée a confirmé le succès du cryptage.

Sur la machine de l'expéditeur, l’icône d’un cadenas est affichée et verrouillée avant l'envoi, confirmant l'application du cryptage.

Sur la machine du destinataire, le message reçu est d’abord affiché comme des caractères illisibles, la lecture nécessite la saisie de la clé privée de l'utilisateur.

# Exercice 2.6

La signature utilise la clé privée de l'expéditeur. Cette clé est protégée par une ***“phrase secrète”*** qui doit être donnée par l'utilisateur à chaque utilisation, garantissant que seul le propriétaire peut l'utiliser.

Il y a aussi la non-répudiation, cette démarche volontaire et authentifiée lie l'expéditeur au contenu du message, elle garantit la non-répudiation, un principe légal fort, l'expéditeur ne pourra pas nier avoir signé et envoyé le document, car il a donné son autorisation explicite via sa ***“phrase secrète”***.

# Exercice 2.7

Ce rapport conclut que l'utilisation du chiffrement PGP répond aux exigences de renforcement des preuves sécurisées :

**Confidentialité** : Assurée par le chiffrement du contenu, seul le destinataire qui possède la clé privée peut lire le message.

**Intégrité** : Assurée par le chiffrement et la fonction de hachage de la signature, garantissant que le message n'a pas été altéré.

**Authenticité** : Assurée par la signature numérique, qui prouve l'identité de l'expéditeur.

L'intégration de PGP permet de convertir un mail, preuve électronique de faible valeur, en un document à forte valeur légale.

# Conclusion

Ce TP nous a introduit aux chiffrement PGP et de la signature électronique. Nous avons abordé l'utilisation des clés cryptographiques pour assurer la confidentialité des messages et leur authenticité. L'objectif final était de comprendre comment ces outils garantissent l'intégrité et la valeur probante des communications numériques.