ANNÉE PASSERELLE EN INGÉNIERIE

Chapitre 14 — Cryptographie, Telnet et SSH

Introduction à la Téléinformatique

Vincent Audergon · HEIA-FR

Année académique 2026-2027

Plan du chapitre

Objectifs du chapitre

HEIA-FR
HTA-FR

À l'issue de ce chapitre, vous saurez :

- **expliquer** les notions de chiffrement, déchiffrement, clés symétriques et asymétriques, fonction de hachage et signature numérique ;
- **distinguer** les trois critères de sécurité : confidentialité, intégrité, authenticité ;
- **décrire** l'utilité et le fonctionnement de Telnet et SSH ;
- **comparer** la sécurité de Telnet et de SSH pour l'administration à distance.

SECTION
01

Bases de la cryptographie

Pourquoi chiffrer ?

DÉFINITION · CRYPTOGRAPHIE

Ensemble des techniques de chiffrement qui assurent l'inviolabilité de textes et, en informatique, de données. (larousse.fr)

ATTENTION

Domaine complexe et sensible : il est vivement déconseillé de programmer soi-même des algorithmes de chiffrement.

EXEMPLE · VERSIONS SÉCURISÉES

De nombreux protocoles ont une variante chiffrée : **HTTPS** (HTTP), **FTPS** (FTP), **SSH** (Telnet)...

Trois critères de sécurité

- **Confidentialité** : seules les parties autorisées peuvent lire l'information.
- **Intégrité** : les données n'ont pas été modifiées en chemin.
- **Authenticité** : l'expéditeur est bien celui qu'il prétend être.

? QUESTION 1

Un message est intercepté et modifié en transit par un attaquant, qui le laisse ensuite poursuivre sa route. Quel critère de sécurité est violé ?

RÉPONSE
L'**intégrité** : le contenu du message a été altéré sans autorisation entre l'émetteur et le récepteur.

Vocabulaire de la cryptographie

Terme	Définition
Chiffrement	Transformer des données en un format illisible, avec un algorithme et une clé.
Déchiffrement	Retrouver les données originales, avec la clé appropriée.
Décryptage	Retrouver les données originales **sans** la clé.
Cryptanalyse	Étude des faiblesses des systèmes de chiffrement.
Clé	Élément permettant de chiffrer et déchiffrer.

ATTENTION
Chiffrement ≠ codage. Le **codage** (ex. Base64, encodage URL) rend les données compatibles avec un format, sans les rendre illisibles.

Fonction de hachage

DÉFINITION · FONCTION DE HACHAGE

Algorithme qui produit, à partir de données de taille variable, une empreinte de **taille fixe**. Un petit changement d'entrée change radicalement la sortie.

REMARQUE

Le hachage **n'est pas** du chiffrement : il est **irréversible**, il n'existe pas de clé pour retrouver les données d'origine.

- Collisions : deux entrées différentes produisent la même empreinte. Les fonctions de hachage modernes sont conçues pour minimiser ce risque.
- MD5 et SHA-1 sont obsolètes et vulnérables. Aujourd'hui : **SHA-256**, **SHA-3**.

Exemple de hachage

- Exemple SHA-256 sur « Bonjour! » :

```
083de31ac1fa14f95671a6e39cc6c72d8fed1590b2a51759bc3f54a76b4169c4
```

- « Bonjour? » :

```
25a4b98d96586efa767983c0df7fdee2be5ec5f850086d19ad07c20e386452c4
```

- « Ceci est un texte beaucoup plus long » :

```
f623b67eacff60461895ea31437de69d3afc6ecc40580deb233d7ce88a0b4980
```

? QUESTION 2

Que pouvez-vous constater sur l’exemple de hachage précédent ?

RÉPONSE

- La taille de l’empreinte est fixe (32 octets, 64 caractères hexadécimaux) quelle que soit la taille du texte d’entrée.
- Un petit changement dans le texte d’entrée (un point d’exclamation remplacé par un point d’interrogation) change complètement l’empreinte.

? QUESTION 3

64 caractères hexadécimaux… ça fait combien d’empreintes possibles ?

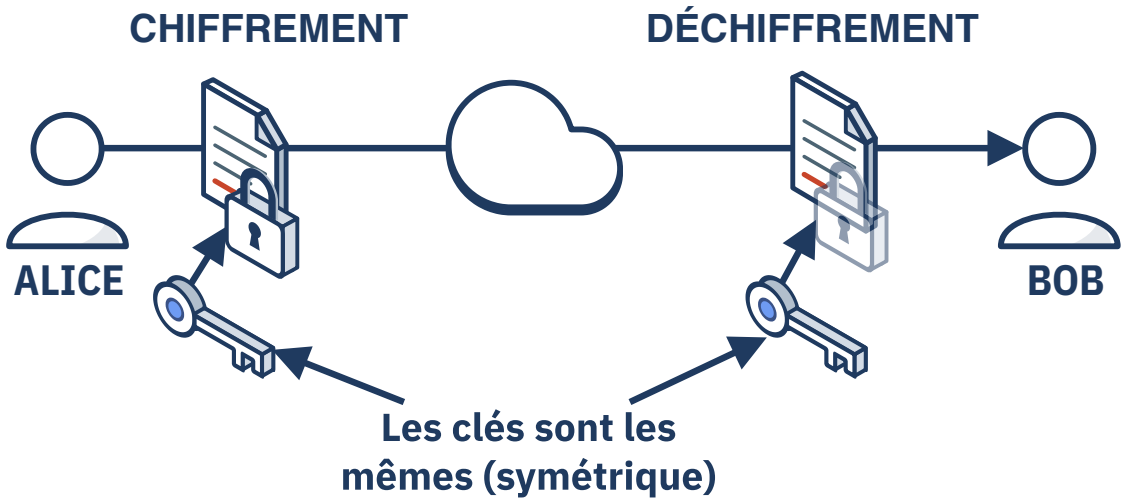
RÉPONSE

64 caractères hexadécimaux = 256 bits (4 bits par caractère). Donc 2^{256} possibilités, soit 1.15×2^{77} soit environ le nombre d’atomes dans l’univers observable (10^{80})

SECTION
02 —

Clés symétriques et asymétriques

Chiffrement symétrique



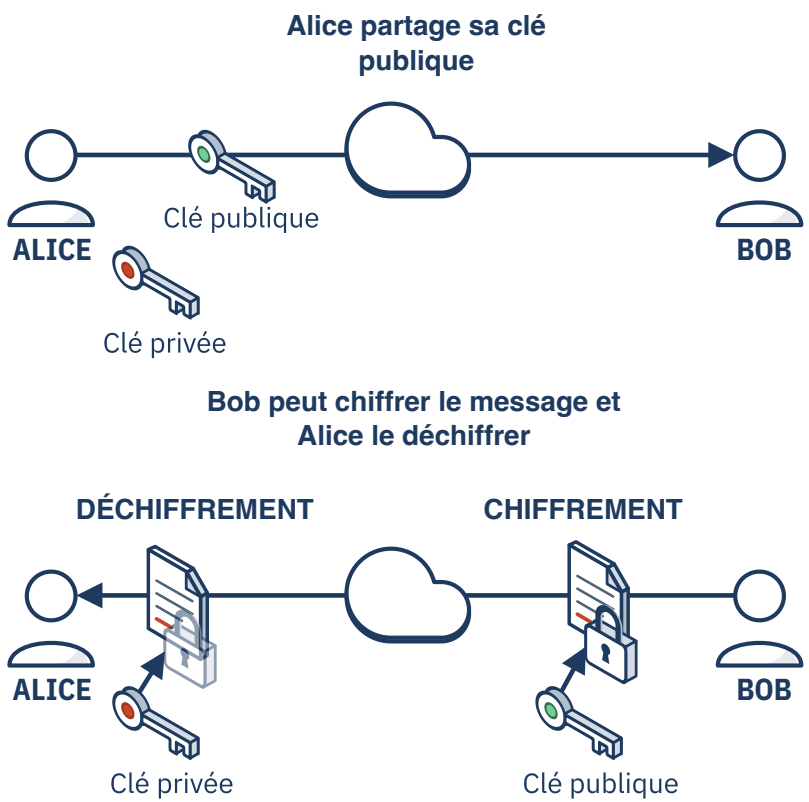
Une **seule clé**, partagée à l'avance, sert au chiffrement **et** au déchiffrement.

- **+** rapide
- **–** distribution et gestion de la clé délicates

EXEMPLE · ALGORITHME

AES (Advanced Encryption Standard)

Chiffrement asymétrique



Une **paire de clés** : la **publique** (partageable) chiffre, la **privée** (secrète) déchiffre. Impossible de retrouver l'une à partir de l'autre.

EXEMPLE · ALGORITHME

RSA (Rivest-Shamir-Adleman)

REMARQUE

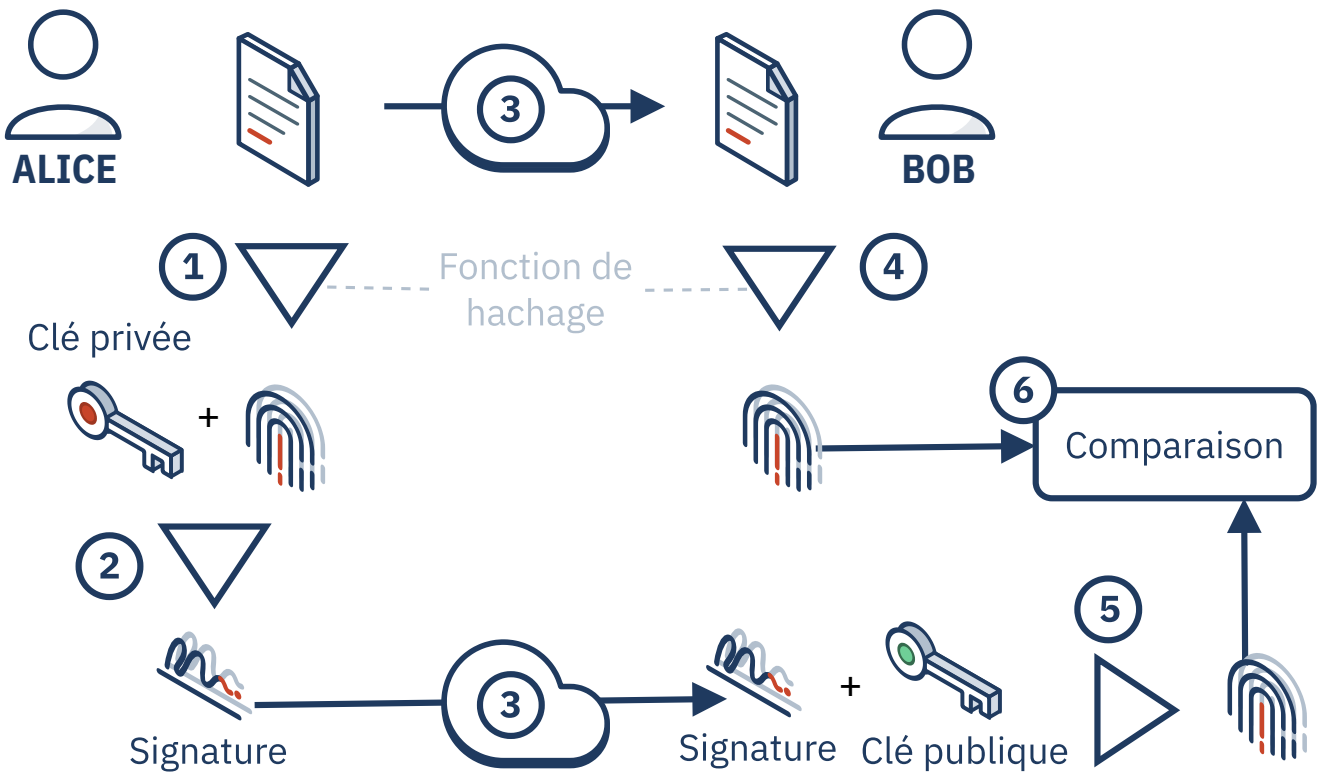
RSA est réversible dans les deux sens (chiffrer avec la clé publique **ou** la clé privée). Exception parmi les algorithmes asymétriques.

? QUESTION 4

Bob chiffre un message avec **sa clé privée** et l'envoie à Alice, qui le déchiffre avec la clé **publique** de Bob. Quel critère de sécurité est garanti ? Lequel ne l'est pas ?

RÉPONSE
Authenticité et **intégrité** garanties : seul Bob peut chiffrer avec sa clé privée. **Confidentialité** non garantie : n'importe qui ayant la clé publique de Bob peut déchiffrer le message.

Signature numérique



Signature numérique (suite)

1. Alice **hache** son message.
2. Alice **signe** l'empreinte avec sa clé **privée**.
3. Bob **hache** le message reçu, puis **vérifie** la signature avec la clé **publique** d'Alice.
4. Les empreintes correspondent → message authentique et intègre.

> **ATTENTION**
> La signature numérique ne chiffre pas la donnée : elle signe un **hachage** de la donnée.

La signature numérique a la propriété de fournir la **non-répudiation** : Alice ne peut pas nier avoir signé le message, car seule sa clé privée peut produire la signature.

SECTION
03

Telnet

Un terminal à distance… en clair

HEIA-FR
HTA-FR

DÉFINITION · TELNET

Protocole applicatif (L7, port **23**, sur TCP) qui émule un terminal virtuel sur un hôte distant, comme si on y était physiquement.

ATTENTION

Telnet transmet **tout en clair**, y compris identifiants et mots de passe : fortement déconseillé aujourd'hui, hors apprentissage.

EXEMPLE · USAGE PÉDAGOGIQUE

Telnet permet de tester « à la main » des protocoles textuels comme HTTP ou SMTP, en tapant directement les commandes du protocole.

Démo Telnet : regarder Star Wars dans le terminal ?!

telnet telehack.com

? QUESTION 5

Un administrateur utilise Telnet pour se connecter à un switch sur un réseau partagé. Un attaquant capture le trafic. Que peut-il récupérer ?

RÉPONSE
Tout : identifiants, mot de passe et l'intégralité de la session, car Telnet ne chiffre rien, les données circulent en clair sur le réseau.

SECTION
04 —

SSH

Le successeur sécurisé

DÉFINITION · SSH

Secure Shell : protocole applicatif (L7, port **22**, sur TCP), équivalent fonctionnel de Telnet mais dont les échanges sont **chiffrés**.

Garantit **confidentialité** et **intégrité** des données échangées. Base aussi de **SFTP** et **SCP** pour le transfert de fichiers.

Deux méthodes d'authentification

HEIA-FR
HTA-FR

Mot de passe

Nom d'utilisateur + mot de passe.

- + simple à mettre en place
- – moins sécurisée

Paire de clés asymétriques

Clé publique déposée sur le serveur, clé privée conservée par l'utilisateur.

- + plus sécurisée
- + pas si compliqué à mettre en place
- – nécessite de gérer les clés et de les stocker en sécurité

Démo : SSH

? QUESTION 6

Comment SSH vérifie-t-il que l'utilisateur possède bien la clé privée correspondant à la clé publique enregistrée, **sans** que la clé privée ne transite jamais sur le réseau ?

RÉPONSE

Mécanisme de **challenge-réponse** : le serveur envoie un message aléatoire (challenge). Le client le **signe** avec sa clé privée et renvoie la signature. Le serveur **vérifie** la signature avec la clé publique stockée. La clé privée reste toujours sur le client.

Vérifier l'identité du serveur

Lors de la première connexion, le client reçoit la clé publique du serveur et la stocke dans `known_hosts`.

ATTENTION
Si la clé du serveur change soudainement (« WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! »), c'est peut-être une attaque **man-in-the-middle**, ou simplement une réinstallation légitime du serveur.

REMARQUE
Ce mécanisme garantit l'**authenticité** du serveur : sans lui, un attaquant pourrait se faire passer pour le serveur légitime dès la première connexion.

Synthèse

CE QU'IL FAUT RETENIR

- Trois critères de sécurité : **confidentialité**, **intégrité**, **authenticité**.
- Clé **symétrique** (une seule clé, rapide) vs **asymétrique** (paire publique/privée, résout la distribution de clé).
- La **signature numérique** combine hachage et clé privée : authenticité, intégrité, non-répudiation, sans chiffrer la donnée elle-même.
- **Telnet** (port 23) transmet en clair, obsolète. **SSH** (port 22) chiffre les échanges et authentifie par mot de passe ou paire de clés.

Des questions ?

Sources

Les sources utilisées pour ce cours (normes, documentation officielle, articles, ouvrages de référence) sont citées et listées intégralement dans la **bibliographie du support de cours écrit**, disponible sur le site du cours :

https://api-teleinfo.isc.heia-fr.ch