Technologies de l'information

Cours:

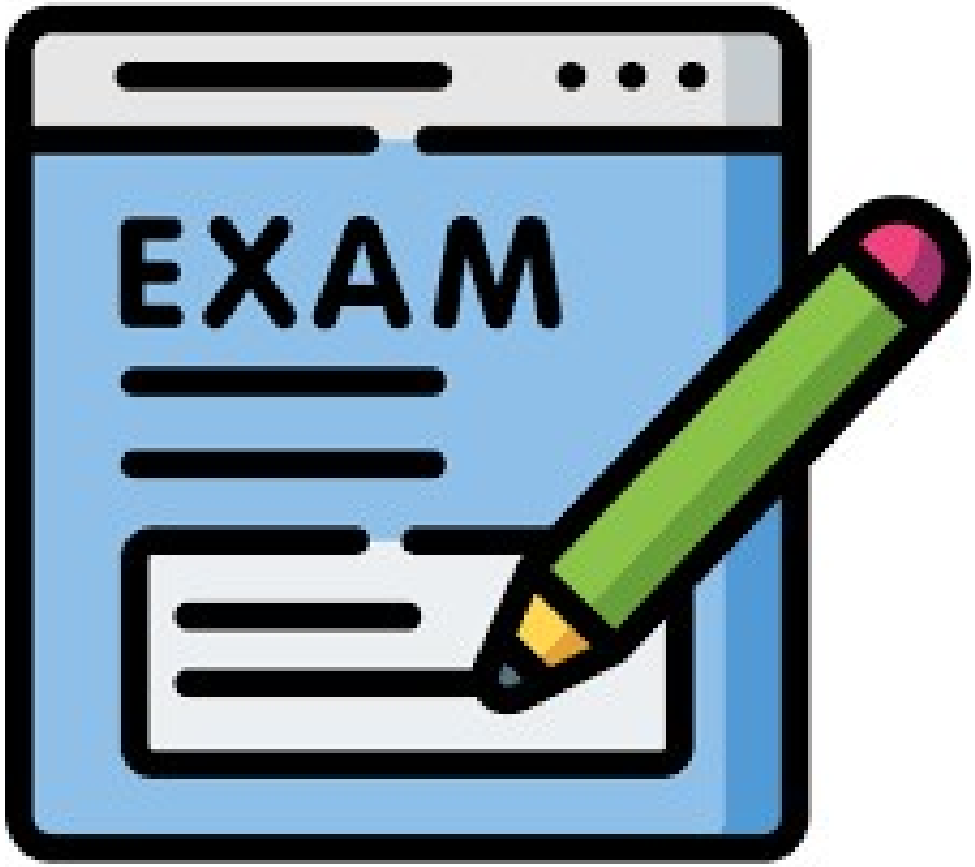
Sécurité des systèmes informatiques

DESS

Séance # 5

Préparé par: Blaise Arbouet

Retour sur l’examen



Concepts de base

Le mot « cryptographie » vient du grec et signifie « écriture secrète ».

La cryptographie est la science de la communication sur des canaux non fiables.

Historiquement, la cryptographie a été associée à l'espionnage, aux gouvernements et à l'armée, et est utilisée en temps de guerre depuis des millénaires.

Au cours des 50 dernières années, la cryptographie a acquis de solides bases mathématiques et est passée d'applications militaires à des applications commerciales.

Exemple dans la vraie vie

Imaginez un scénario de commerce électronique où Alice, une acheteuse, souhaite commander des produits auprès de Bob, son fournisseur.

Conditions requises pour la transaction :

- Alice veut s'assurer qu'elle traite bien avec Bob et non avec un imposteur (**authentification**).
- Bob veut s'assurer qu'Alice est bien Alice et non un imposteur (**authentification**), car elle bénéficie des tarifs préférentiels négociés.
- Alice souhaite que la commande reste secrète vis-à-vis de ses concurrents ; et Bob ne souhaite pas que d'autres clients voient ses tarifs préférentiels (**confidentialité**).
- Alice et Bob veulent tous deux s'assurer que les pirates ne puissent pas modifier le prix ou la quantité (**intégrité**).
- Bob veut s'assurer qu'Alice ne puisse pas prétendre ultérieurement ne pas avoir passé la commande (**non-répudiation**).

Requis

Authentification : L'expéditeur sait que le message est destiné au destinataire prévu ; et le destinataire sait que le message a été envoyé par le bon expéditeur.

Confidentialité : Le message est secret : seuls l'expéditeur et le destinataire prévu en connaissent le contenu.

Intégrité : Le message n'a pas été modifié (intentionnellement ou accidentellement) pendant son transit.

Non-répudiation : L'auteur du message ne peut nier ultérieurement l'avoir envoyé.

Des techniques cryptographiques peuvent être utilisées pour satisfaire aux exigences ci-dessus.

Comment cela fonctionne?

Un message ordinaire (**le texte en clair**) est traité par un algorithme de chiffrement pour produire un message brouillé (**le texte chiffré**).

Le récepteur utilise ensuite un algorithme de déchiffrement correspondant pour récupérer le texte en clair à partir du texte chiffré.

Il n'y aurait aucune sécurité si ces algorithmes étaient connus de tous.

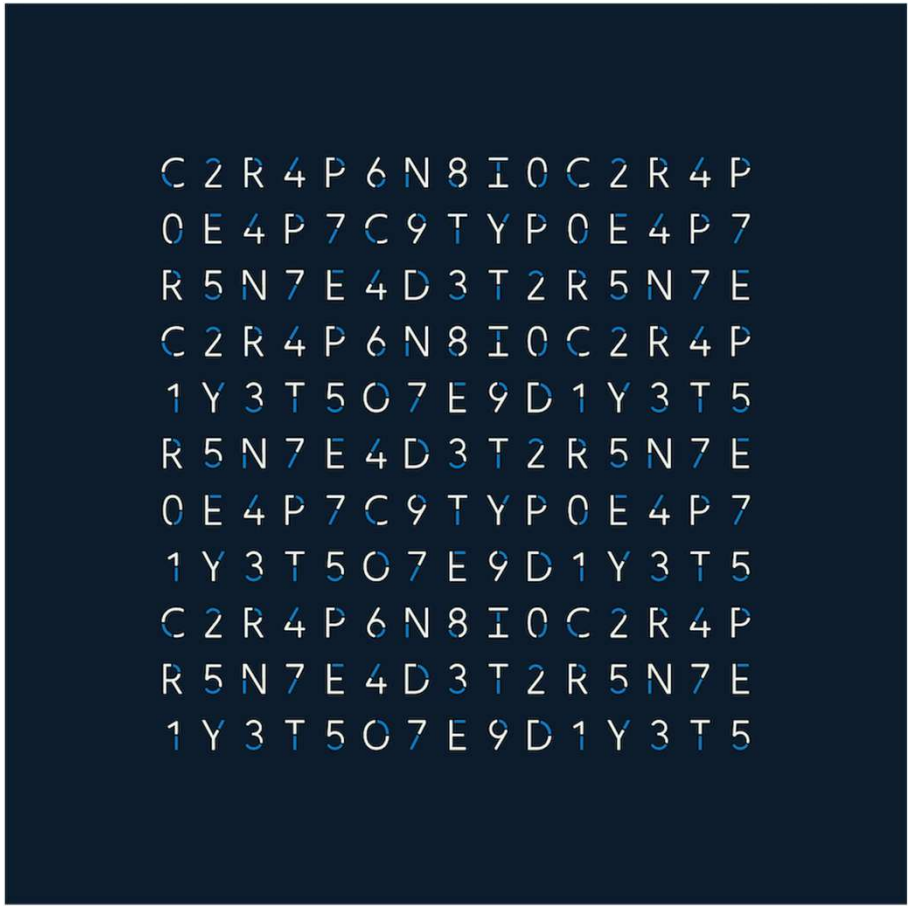
D'où l'existence d'une donnée d'entrée supplémentaire appelée **clé**.

Cette clé est secrète, même si de nombreuses personnes connaissent les algorithmes.

Le principe est le même que celui des serrures à combinaison : plusieurs personnes peuvent utiliser des serrures de même conception, mais chacune choisit une combinaison différente (c'est-à-dire une clé différente).

C’est quoi le chiffrement (cryptage)?

Le cryptage est le processus de **brouillage** ou de **chiffrement** des données afin qu'elles ne puissent être **lues** que par une personne disposant des moyens de les rétablir dans leur état d'origine. Il s'agit d'une caractéristique essentielle d'un **Internet sûr** et **fiable**. Il contribue à assurer la sécurité des données pour les informations sensibles.



Types de chiffrement (cryptage)

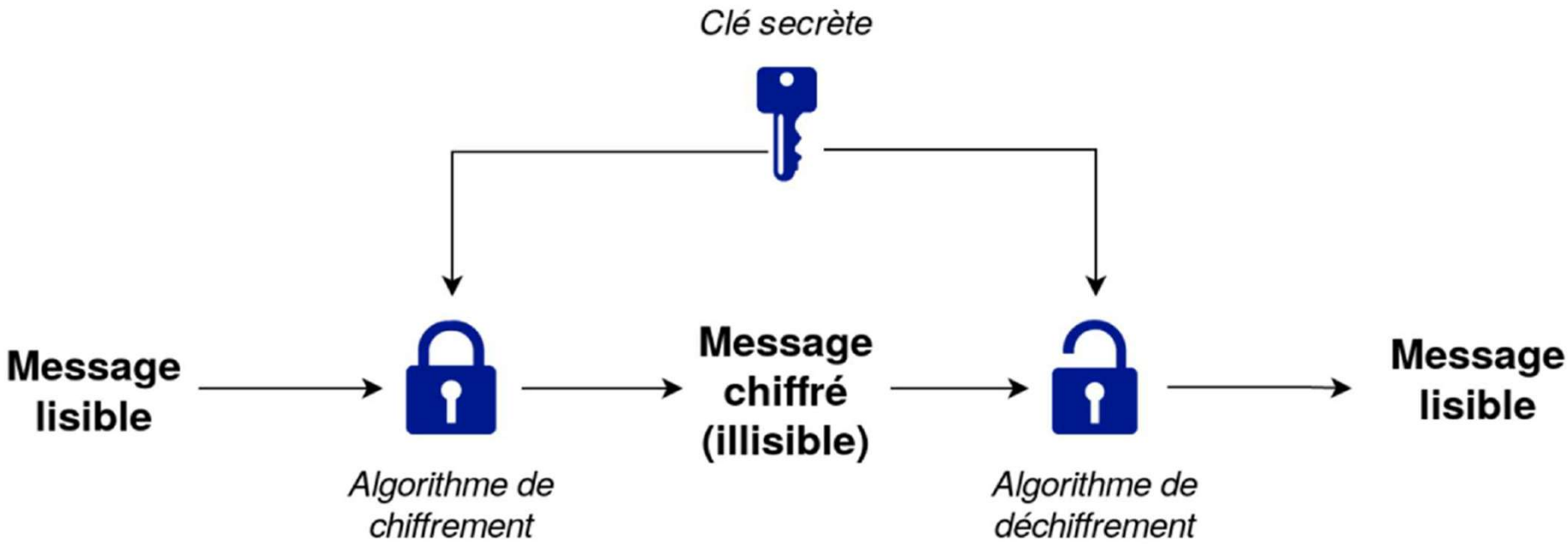
Cryptographie à clé secrète (ou symétrique) :

- Les opérations de chiffrement et de déchiffrement utilisent la même clé.
- Les systèmes à clé secrète existent depuis plusieurs siècles.

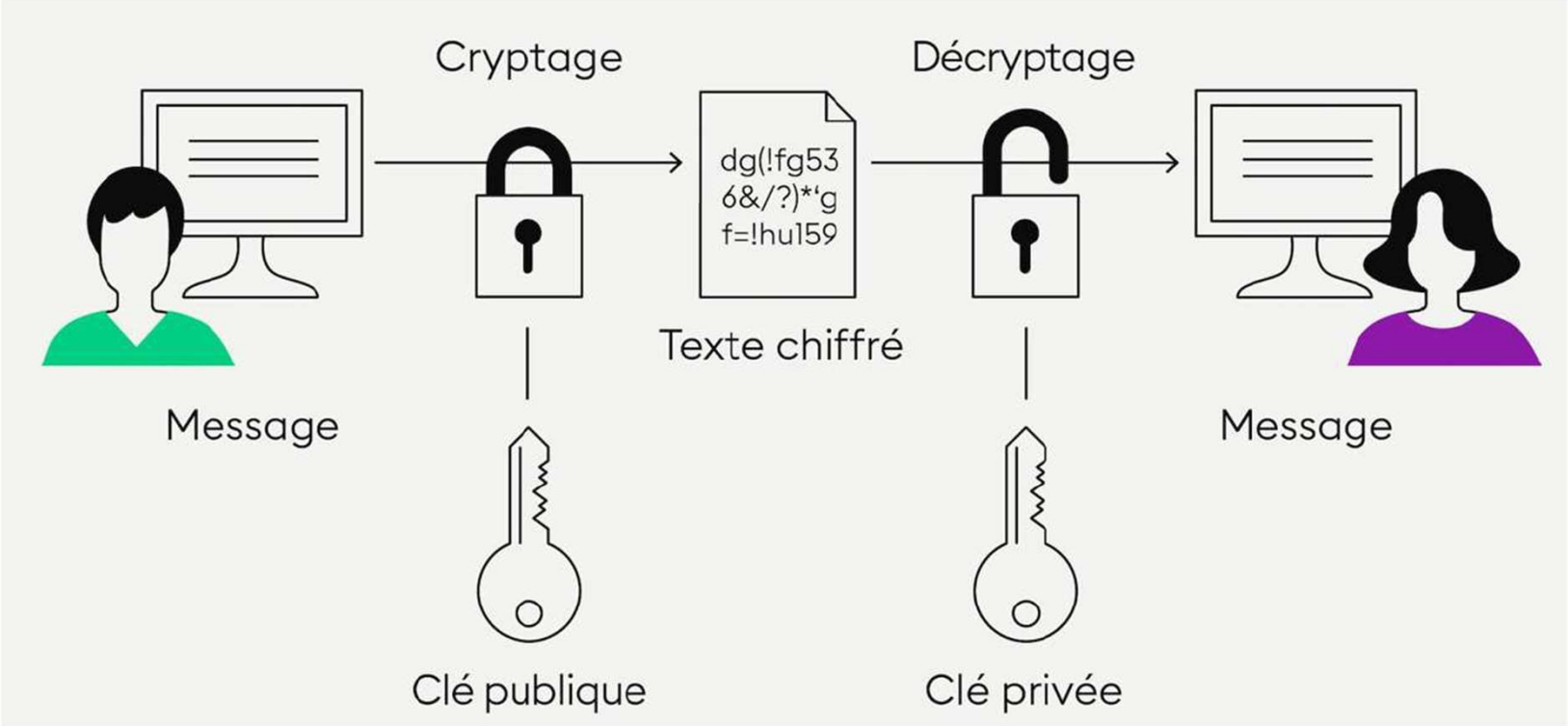
Cryptographie à clé publique (ou asymétrique) :

- Les systèmes à clé publique utilisent des clés différentes pour les opérations de chiffrement et de déchiffrement.
- Une clé peut être rendue publique tandis que l'autre est gardée secrète (on parle alors de clé privée) et date des années 1970.
- Peut être utilisé pour fournir des signatures numériques

Chiffrement symétrique



Chiffrement asymétrique



Algos de chiffrement

Différences clées	Chiffrement symétrique	Chiffrement asymétrique
Sécurité	Moins sécurisé en raison de l'utilisation d'une seule clé pour le cryptage.	Beaucoup plus sûr car deux clés sont impliquées dans le cryptage et le décryptage.
Confidentialité	Une clé unique pour le chiffrement et le déchiffrement peut entraîner une compromission de la clé.	Deux clés créées séparément pour le chiffrement et le déchiffrement, ce qui élimine le besoin de partager une clé.
Vitesse	Le chiffrement symétrique est plus rapide techniquement	Le cryptage asymétrique est plus lent en termes de vitesse.
Algorithme	RC4, AES, DES, 3DES et QUAD.	RSA, Diffie-Hellman, algorithms ECC

Exemples réels de chiffrement symétrique

Stockage de données : lorsque vous chiffrez des fichiers sur votre ordinateur ou une clé USB à l'aide d'un mot de passe, cela implique souvent un chiffrement symétrique. Le même mot de passe est utilisé pour chiffrer et déchiffrer les données.

Secure Sockets Layer (SSL) / Transport Layer Security (TLS) : ces protocoles utilisent un chiffrement de réseau symétrique pour protéger les données transmises sur Internet, par exemple lors de transactions bancaires en ligne ou lorsque vous vous connectez à un site Web sécurisé.

Réseaux privés virtuels (VPN) : de nombreux services VPN utilisent un chiffrement symétrique pour sécuriser les données transmises entre votre appareil et le serveur VPN, garantissant ainsi la confidentialité et la sécurité lors de la navigation sur Internet.

Chiffrement de disque : les outils de chiffrement de disque entier comme BitLocker (Windows) et FileVault (macOS) utilisent un chiffrement symétrique pour protéger l'intégralité du contenu d'un disque dur ou d'un disque SSD.

Applications de messagerie : certaines applications de messagerie comme WhatsApp utilisent un chiffrement symétrique pour protéger les messages envoyés entre les utilisateurs, de sorte que seul le destinataire disposant de la clé de déchiffrement correcte puisse lire les messages.

Exemples réels de chiffrement asymétrique

1

Courriel sécurisé : lorsque vous envoyez un courrier électronique chiffré à l'aide de plateformes telles que PGP (Pretty Good Privacy) ou S/MIME (Secure/Multipurpose Internet Mail Extensions), vous utilisez un chiffrement asymétrique. Vous utilisez la clé publique du destinataire pour le chiffrement, et seule sa clé privée peut déchiffrer le message.

2

Signatures numériques : les utilisateurs utilisent le chiffrement asymétrique pour générer des signatures numériques pour des documents ou des logiciels. Lorsque vous signez un document avec votre clé privée, d'autres peuvent vérifier son authenticité à l'aide de votre clé publique.

3

Navigation Web sécurisée (HTTPS) : lorsque vous visitez un site Web sécurisé avec une URL « https:// », le chiffrement asymétrique permet d'établir une connexion sécurisée entre votre navigateur et le serveur Web. Ce chiffrement sécurise activement le transfert de données entre vous et le site Web.

4

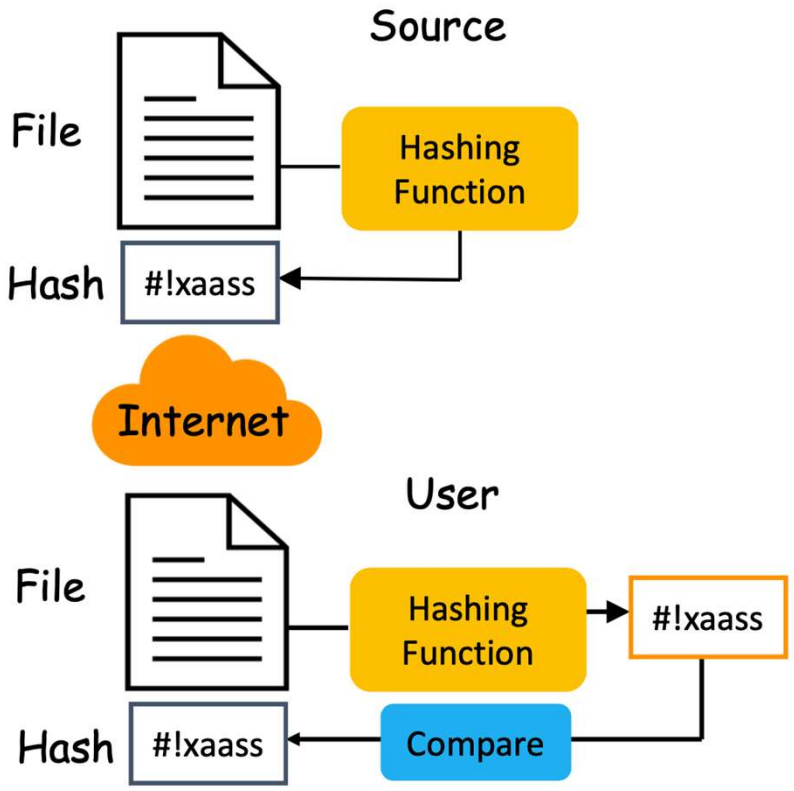
Secure Shell (SSH) : le protocole SSH utilise un chiffrement asymétrique pour authentifier et sécuriser les connexions à distance et les transferts de fichiers entre les ordinateurs. L'authentification repose sur la clé publique du serveur, tandis que le chiffrement des données implique la génération d'une clé de session.

5

Technologie Blockchain : les crypto-monnaies comme Bitcoin et Ethereum utilisent un chiffrement asymétrique pour sécuriser les transactions et la gestion des portefeuilles. Les clés publiques et privées sont au cœur de ces systèmes de blockchain.

Hachage

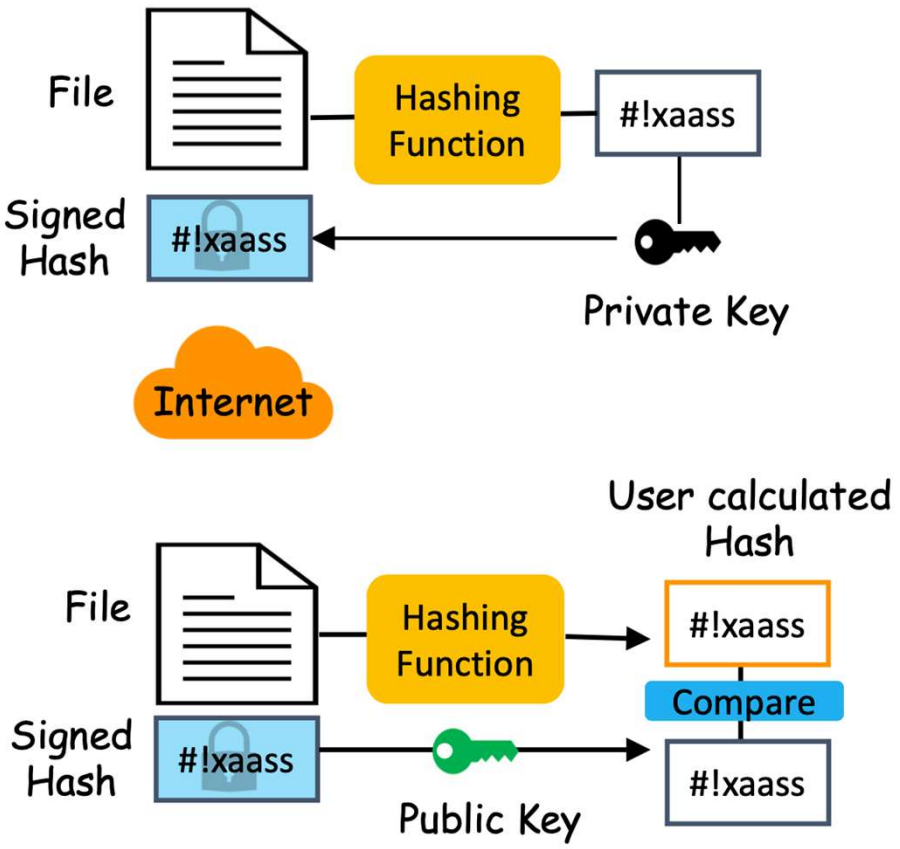
Un hachage est une fonction qui convertit une entrée (souvent appelée « message ») en une chaîne d'octets de longueur fixe, d'apparence aléatoire. Cette sortie est communément appelée valeur de hachage ou condensé.



Signature numérique vs Hachage

Fondamentalement, une signature numérique est un mécanisme permettant de vérifier l'authenticité et l'intégrité d'un message, d'un logiciel ou d'un document numérique. C'est comme un cachet électronique, prouvant que le contenu n'a pas été modifié depuis sa signature et authentifiant l'identité du signataire.

En revanche, une signature numérique implique bien plus que le simple codage et le hachage des données de sortie. Elle utilise un algorithme de signature, dont l'une des étapes est souvent une fonction de hachage.



Chiffrement au jour le jour:

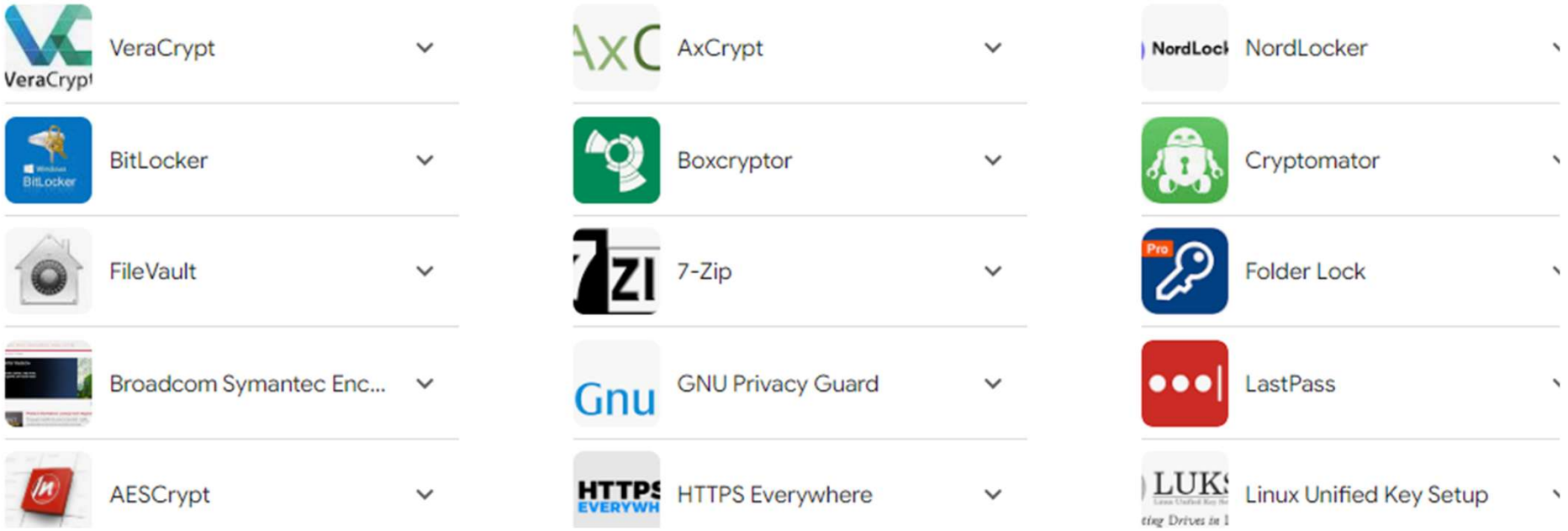
Navigation

Achat en ligne

Messagerie sécurisée

Chiffrement de bout en out

Outils de chiffrement “open source” populaires



Enjeux à la cryptographie

- Gestion de la clé
- Faiblesse des alogs
- Cryptographie quantique
- Protection de la vie privée (backdoor, surveillance)

Questions ?

En avez-vous?

Cégep Sherbrooke

Temps personnel

TRAVAIL DE GROUPE

LAB

Références

- https://www.idemia.com/fr/cryptographie
- https://www.mailinblack.com/ressources/glossaire/la-cryptographie-au-service-de-la-cybersecurite/
- https://medium.com/@sebastienwebdev/cryptography-cybersecurity-project-42b7eb7462d5
- https://learn.logixacademy.com/pages/digitalalchemist?p=hashing-and-digital-signatures
- https://www.osboxes.org/ubuntu-server/
- https://medium.com/@amittidke/understanding-tls-ssl-encryption-symmetric-vs-asymmetric-f4eef15270d4