

Sécurité des données

Les premières formes d'écriture ont été inventées il y a plus de 5000 ans. Pour la première fois, les hommes représentent l'information par une suite de symboles. C'est ainsi qu'apparut la première écriture connue. Les systèmes d'écriture ont été développés afin de sauvegarder des informations en dehors du cerveau humain. Cela permettait de **stocker** et de **communiquer** de l'information sur de longues distances.

En informatique, on appelle **données** la représentation d'informations par une suite de symboles (0 ou 1). Depuis que l'on peut traiter des données se pose le problème de leur sécurité. Ces données sont envoyées à travers les réseaux informatiques où l'on essaie de garantir les principes d'**intégrité**, de **confidentialité** et de **disponibilité**.

Par le principe, il faut que les données puissent être lues
seulement par les personnes autorisées. Pour cela, on a développé le **chiffrement** pour protéger
l'information.

Par le principe, il faut éviter que les données soient détruites ou modifiées lors de la transmission ou du stockage. Pour cela, on a développé des **codes vérificateurs d'erreur**. Ceux-ci détectent les erreurs dans les données et peuvent même parfois les corriger automatiquement.

Exercise 1

- a. Décrivez une situation où les données stockées peuvent être perdues (problème de disponibilité)

- b. Décrivez une situation où les données transmises peuvent être altérées (problème d'intégrité)

Chiffrement

Activité “chiffrement basique”

Alice et Bob utilisent deux codes secrets pour s'échanger des messages. Même si une tierce personne intercepte les messages, elle ne devrait pas pouvoir les comprendre. Alice utilise un premier code secret pour écrire des lettres à Bob. Bob utilise un deuxième code secret pour écrire à Alice. Eve est curieuse et veut savoir ce qu'Alice et Bob s'écrivent. Elle parvient à intercepter deux de leurs lettres.

De plus, Eve observe Alice en train de transformer son texte en code et sait que son message commence par PEUTONSE.

Cher Bob,
EPTUNOESOVITA
ERZIHUEEERS
Alice

Chère Alice,
KSOIKUASUOVZEDNERIU
O
Bob

a. À la place d'Eve, seriez-vous en mesure de déchiffrer le texte écrit par Alice ? Si oui, quel est son message ?

b. Utilisez les définitions dans l'encadré ci-dessous pour compléter le texte suivant :

Dans cette activité, Eve a intercepté deux
Elle veut pour connaître les
La méthode de utilisée par Alice consiste à ...

Définitions :

- L'étude des codes secrets s'appelle la **cryptologie**.
- La **cryptographie** est la branche qui vise à chiffrer les messages pour les rendre incompréhensibles par des personnes non autorisées. Elle applique un **algorithme de chiffrement** qui utilise souvent une fonction et un paramètre bien spécifique : une **clé**.
- La **cryptanalyse** est la branche qui vise à décrypter, à "**casser le code** secret" et déchiffrer les messages rendus incompréhensibles par la cryptographie.
- On appelle **texte en clair** (plaintext) un texte qui n'est pas secret.
- On appelle **texte chiffré** (ciphertext) la représentation d'un texte en un langage secret.
- La transformation d'un texte en clair à un texte chiffré s'appelle **chiffrement**.
- L'opération inverse, qui consiste à restituer le texte en clair à partir de texte chiffré, s'appelle **déchiffrement**.

Quelques algorithmes de chiffrement basique

Les premiers codes secrets datent de plus de 3500 ans. À cette époque, on chiffrait le texte en modifiant l'ordre des lettres après avoir supprimé les espaces.

Exemple 1

clé : permutation par deux

texte en clair :

I	N	F	O	R	M	A	T	I	Q	U	E
---	---	---	---	---	---	---	---	---	---	---	---

texte chiffré :

--	--	--	--	--	--	--	--	--	--	--	--

Exemple 2 : le chiffre de César

clé : nombre de décalages des lettres d'alphabets. Par exemple : 19

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

texte en clair : INFORMATIQUE

texte chiffré :



Exercice “chiffrement basique”

- a. Utilisez la permutation par deux pour déchiffrer le code secret suivant :

NUOCRUIRLESECTMOEMNULETERTOEVUREET

- b. Utilisez le code de César pour chiffrer le message suivant. La clé est le décalage de 3.

LESPIONSAPPELLEBOB

- g. Bernard a utilisé le chiffrement de César et a obtenu le texte secret suivant :

OVMOBQQSFOETBOTGBJSEFTFSSFVST

Sachant que le dernier mot du texte en clair est ERREURS, déchiffrez le reste du texte secret.

- h. Le texte secret suivant a été chiffré avec le code de César, mais le décalage est inconnu.

AVBASLTVUKLKLCLYHPAZHCVPYSPYLLALJYPYL

Comment déchiffrer ce texte sachant que dans le texte en clair original la lettre E est celle qui apparaît le plus souvent.

- i. Réfléchissez à un nouveau code secret. Décrivez le chiffrement à l'aide d'un schéma, puis utilisez votre méthode pour chiffrer une petite phrase.

Activité “Sécurité 1” ([Playlist L’informateur](#))

Visionnez le vidéo « [Sécurité 1](#) » à partir de 2:00 minutes et répondez aux questions suivantes.

Q1 : Quand on parle de sécuriser une communication, en quoi consiste les propriétés suivantes :

- la confidentialité :
- l'authenticité :
- l'intégrité :

Q2 : Que signifient les notations $E(m) = c$ et $D(c) = m$?

- m est ...
- c est ...
- $E()$ est la fonction
- $D()$ est la fonction ...

Q3 : Donnez au moins 3 points négatifs du chiffrement de César :

1. ...
2. ...
3. ...

Q4 : Utilisez le chiffrement de Vigenère pour crypter le mot « Hello » avec $k = \text{« bac »}$:

Q5 : Quel est le point positif de Vigenère par rapport au César ?

Q6 : Que dit le principe de Kerckhoffs ?

Q7 : Que signifie la cryptographie symétrique et asymétrique ?

- symétrique signifie
- asymétrique signifie ...

Activité “Sécurité 2” ([Playlist l’informateur](#))

Visionnez les différentes séquences du vidéo « [Sécurité 2](#) » et répondez aux questions suivantes.

Q1 : Comment s’appelle l’opération logique utilisée dans le chiffrement de Vernam ? Quelle est sa notation ?
Donnez sa table de valeurs.

- nom de l’opération : ...

- notation : ...

- table des valeurs :

Q2 : Pourquoi le chiffrement de Vernam est parfait mais non praticable ?

Q3 : Quelles sont les deux catégories de chiffrements symétriques ?

Q4 : Nommez deux méthodes principales de chiffrement par bloc utilisées actuellement. Lequel des deux méthodes est plus sûr ?

Q5 : Combien de temps faudrait-il pour craquer une clé AES ?

Q6 : Pourquoi est-ce que la cryptographie symétrique ne suffit plus à répondre aux besoins d’aujourd’hui ?

Activité “Sécurité 3” ([Playlist l’informateur](#))

Visionnez les 3 premières minutes du vidéo « Sécurité 3 » et répondez aux questions suivantes.

Q1. Comment s’appellent les deux types de clé utilisé dans la cryptographie Asymétrique et à quoi sert chacune ?

- la première s’appelle et elle sert à

- la deuxième s’appelle et elle sert à

Q2. Si Alice veut envoyer un message crypté à Bob, elle va utiliser quelle clé pour chiffrer son message ?

Q3. Quel est l’avantage de la cryptographie asymétrique par rapport à symétrique ?

Q4. Quelles sont les deux principales propriétés mathématiques de ces clés asymétriques ?

Q5. Avancez la vidéo jusqu’à 10:10. Est-ce que le système d’échange est sécurisé avec la cryptographie asymétrique ? Justifiez.

Activité 4 : Somme de contrôle (checksum) et la fonction de hachage

La transmission des données sur les réseaux se fait par bloc d'information. Les systèmes informatiques, dès lors qu'ils communiquent continuellement et abondamment, sont particulièrement sensibles au problème d'erreurs de transmission, des pertes d'information et des mutations. Pour garantir l'intégrité des données, on utilise la somme de contrôle (ou checksum) et la fonction de hachage.

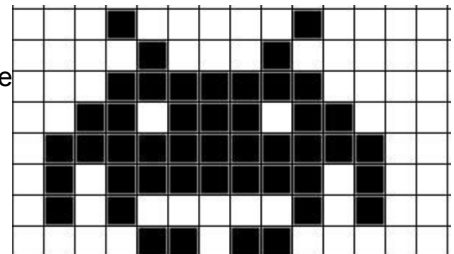
Checksum

Sur un paquet de données de 7 bits par exemple, les checksums utilisent un bit de parité pour contrôler par redondance une erreur sur la transmission. Dans l'exemple ci-contre, on donne la valeur 0 au bit de parité lorsque la somme des bits de la valeur à transmettre est paire, et la valeur 1 lorsque cette somme est impaire. On notera que, de cette façon, la somme des 8 bits est toujours paire.

Le bit de parité est habituellement placé à la position de poids le plus faible, ce qui permet de contrôler directement la valeur transmise.

Valeur à transmettre	Somme des bits	Bit de parité	Valeur transmise
0000000	0	0	00000000
0000001	1	1	00000011
0000010	1	1	00000101
0000011	2	0	00000110
0000100	1	1	00001001
0000101	2	0	00001010
0000110	2	0	00001100
0000111	3	1	00001111
...		...	...
1111101	6	0	11111010
1111110	6	0	11111100
1111111	7	1	11111111

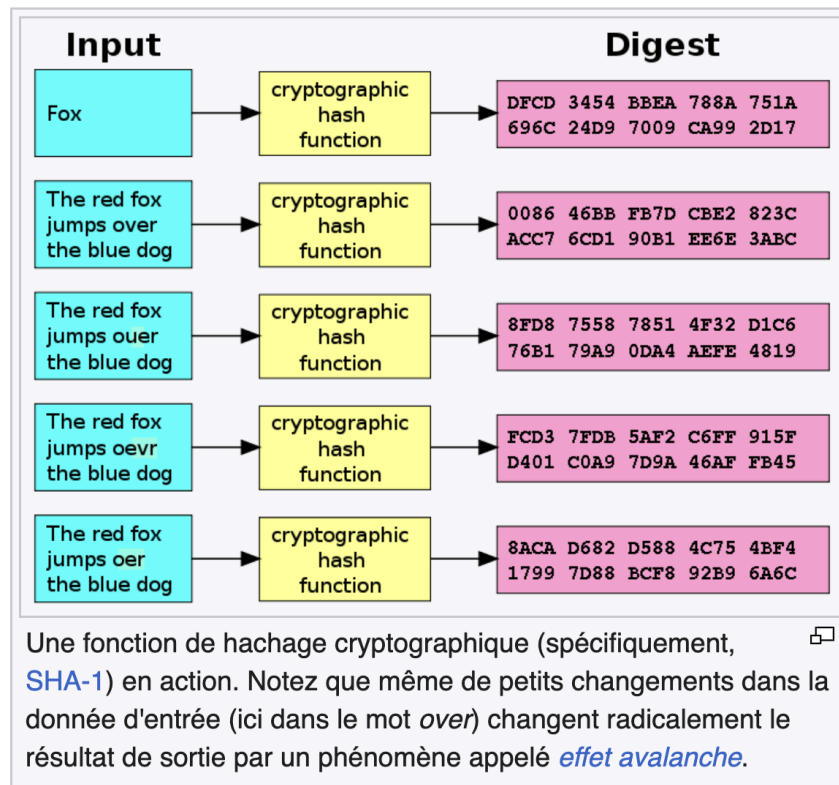
Exercice : En suivant l'exemple, complétez le tableau ci-dessous pour montrer quelles données seront envoyées pour transmettre l'image ci-contre avec les checksums.



Valeurs à transmettre pour chaque ligne	Somme des bits	Bit de parité	Valeur transmise en binaire	Valeur transmise en décimale
0001000 0010000	1 - 1	1 - 1	00010001 00100001	9 - 17

Fonction hachage

Une fonction de hachage est une fonction mathématique à sens unique (non réversible) qui prend en entrée des données de taille arbitraire appelées message (ou input) et génère un résultat numérique de taille fixe, appelé valeur de hachage, haché, empreinte numérique, hash ou digest.



Voici quelques caractéristiques importantes des fonctions de hachage :

1. Déterminisme : un même message aura toujours la même valeur de hachage ;
2. Non prévisible : il doit être difficile de prédire les résultats de la fonction à partir d'un ensemble d'entrées.
3. Résistance aux collisions : il est très difficile de trouver deux messages différents qui produisent le même haché.
4. Résistance à la préimage : il est difficile de retrouver le message original à partir de son haché.
5. Effet avalanche : de légères modifications des données d'entrée doivent entraîner une grande différence dans la valeur de hachage obtenue.

Du fait de ces propriétés, les fonctions de hachage (SHA-1, SHA-3, SHA-256, MD5, Blake2, etc.) sont utilisées pour vérifier l'intégrité des données, la sécurisation des mots de passe, etc.

Exercice : Voici un exemple d'utilisation de fonction de hachage intégrée à Python.

- Expliquez ce que fait chaque ligne de code.
- Vérifiez, si possible, les caractéristiques décrites ci-dessus.

```
Message = " Hello world "  
Digest = hash(Message)  
print("le message : ", Message)  
print("la valeur hache :", Digest )
```

Activité 5 : Signature digitale et certificat numérique

Pour **garantir l'authenticité** d'un message, on peut utiliser un **mot de passe**, mais cela présente plusieurs problèmes potentiels. Reliez l'intitulé de chaque problème avec sa description :

1. Faible complexité des mots de passe

•

•

Des programmes malveillants enregistrent les frappes au clavier de l'utilisateur, ce qui permet aux attaquants de récupérer les mots de passe saisis par l'utilisateur.

2. Réutilisation des mots de passe

•

•

Les attaquants incitent les utilisateurs à divulguer leur informations d'identification, par exemple en se faisant passer pour un service légitime par e-mail ou avec des faux sites Web.

3. Ingénierie sociale ou phishing

•

•

Les utilisateurs ont souvent tendance à choisir des mots de passe faciles à deviner ou à craquer.

4. Keylogging

•

•

Les utilisateurs ont souvent tendance à réutiliser les mêmes mots de passe sur plusieurs comptes en ligne.

5. Force brute et attaques par dictionnaire ..

•

•

Les attaquants utilisent des techniques automatisées pour essayer de deviner les mots de passe en utilisant des listes de mots courants ou en essayant toutes les combinaisons possibles.

Une **signature digitale** (ou signature numérique) est une autre technique pour authentifier une information. Elle permet à une entité de prouver qu'elle a créé ou approuvé un message, ou un document. Une signature digitale utilise une paire de clés asymétriques. À l'aide d'une clé privée, l'expéditeur génère un nombre pour «signer» un élément à certifier. La clé publique est utilisée par le destinataire pour vérifier l'authenticité de la signature.

Exercice : Quel(s) principe(s) peut garantir la signature digitale ? Biffez ce qui ne convient pas.

- La disponibilité
- L'intégrité
- La non-répudiation
- L'authenticité
- La confidentialité

Un **certificat numérique** est émis par une autorité de certification (CA) de confiance, après avoir vérifié l'identité de l'entité (un site Web, une personne ou une organisation). Ce certificat est un fichier numérique qui lie une clé publique à l'identité d'une entité. Il est signé numériquement par CA pour garantir son authenticité afin de protéger des données et des communications. En général, le processus de certification est simple et rapide. La plupart des systèmes d'exploitation et des navigateurs disposent des listes prédéfinies de certificats numériques de confiance pour authentifier un site web et pour s'y connecter et distribuer des informations en toute sécurité.

Exercice : Dans Chrome, ouvrez une page web et cliquez à gauche de l'adresse Web pour voir la sécurité. Que pouvez-vous dire des informations affichées ?

Activité 6 : Sécurité de transfert d'information chiffrée

Sur un réseau informatique, la sécurité d'envois des données est assurée principalement par le protocole TLS (Transport Layer Security). Voici une description simplifiée de son fonctionnement :

1. Handshake (Négociation des paramètres de sécurité)

Le client envoie un message '**Client-Hello**' au serveur indiquant ses capacités de chiffrement et d'autres paramètres.

Le serveur répond avec un message '**Serveur-Hello**' sélectionnant un ensemble commun de paramètres de sécurité.

Le serveur envoie son **certificat numérique** au client, qui contient sa clé publique.

Le client vérifie le certificat (éventuellement auprès d'une autorité de certification) pour s'assurer qu'il est valide et correspond au nom de domaine auquel il se connecte.

2. Échange de clés :

Le client génère une **clé de session** (symétrique), qu'il chiffre avec la clé publique du serveur et l'envoie au serveur.

Le serveur utilise sa clé privée pour déchiffrer la clé de session.

3. Protections des données :

Sur toute la durée de la session, cette **clé symétrique** est utilisée pour chiffrer les données avant d'être envoyées sur le réseau, puis on l'utilise pour déchiffrer le contenu après la réception des données.

De plus, sur chaque message est appliqué un processus combinant une fonction de hachage et une clé secrète. Ce processus est connu sous le nom de **MAC** (Message Authentication Code) ou **codes d'authentification de message**. Il permet de vérifier que les données reçues sont identiques aux données envoyées.

Exercice : Quel(s) principe(s) peut garantir chaque étape de TLS ? Justifiez.

Étapes	Principes de sécurité	Justifications
1. Handshake		
2. Échange de clés		
3. Protections des données		

À retenir :

La sécurité informatique consiste généralement à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. Elle vise généralement cinq principaux objectifs :

Principes	Rôle	Techniques utilisés et exemples
Confidentialité	Assurer que seules les personnes autorisées aient accès aux ressources échangées ;	Rendre l'information inintelligible à toute personne en dehors des acteurs de la transaction. Exemples : - Mots de passe. - Chiffrement symétrique : César, Vigenère, DES(Data Encryption Standard) , AES(Advanced Encryption Standard), etc, - Chiffrement asymétrique : RSA, El-Gamal - Chiffrement hybride : TLS
Intégrité	Garantir que les données sont bien celles que l'on croit être ;	Déterminer si les données n'ont pas été altérées durant la communication. Exemples : - Checksums - Fonctions hachage : SHA-1, SHA-256, MD5, - MAC. - Signature numérique.
Disponibilité	Permettant de maintenir le bon fonctionnement du système d'information ;	Garantir l'accès à un service ou à des ressources. Exemples : - Protection (Anti-virus, limitation de Droit d'accès), - Sauvegarde des données (backup),
Non-répudiation	Garantir qu'une transaction ne peut être niée ;	Garantie qu'aucun des correspondants ne pourra nier la transaction. Exemples : - Signature numérique. - Certificat numérique.
Authenticité	Assurer que seules les personnes autorisées aient accès aux ressources.	Garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Exemples : - identifiant et mots de passe - Signature numérique. - Certificat numériquement - TLS

Nécessité d'une approche globale.

La sécurité d'un système informatique fait souvent l'objet de métaphores. En effet, on la compare régulièrement à une chaîne en expliquant que le niveau de sécurité d'un système est caractérisé par le niveau de sécurité du maillon le plus faible. Ainsi, une porte blindée est inutile dans un bâtiment si les fenêtres sont ouvertes sur la rue.

Dans un contexte global, il faudrait donc prendre en compte du comportement des utilisateurs, du fonctionnement des programmes informatiques, de la sécurité des télécommunications et du matériel utilisé.

Remarque: Le maillon faible est pratiquement tout le temps le comportement de l'utilisateur.

Exercices de révision

Ex. 1 Chiffrer le message suivant avec le chiffrement de Vigenère.

Texte en clair = S E C R E T

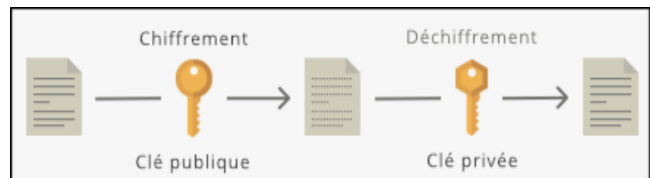
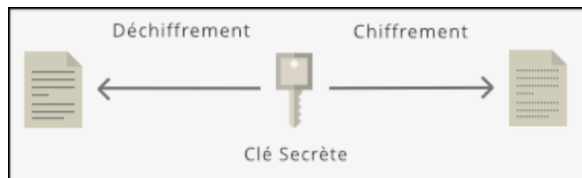
clé = B E C

Ex.2 Déchiffrer le message suivant et indiquer la méthode utilisée.

Texte chiffré = X K B K R K X

Ex. 4

a. Indiquer la famille de cryptographie (symétrique / asymétrique) correspondant :



b. Biffer ce qui ne convient pas :

- Si Bob veut écrire un message secret à Alice, il utilisera la clé **publique / privée** de **Bob/Alice**.
- Si Alice reçoit un message de Bob, pour le déchiffrer, elle utilisera la clé **publique / privée** de **Bob / Alice**.
- Si Alice veut écrire un message secret à Bob, elle utilisera la clé **publique / privée** de **Bob / Alice**.
- Si Bob reçoit un message d'Alice, pour le lire en clair, il utilisera la clé **publique / privée** de **Bob / Alice**.

c. Eve sait que Bob utilise le code de César pour écrire à Alice, mais elle ne connaît pas la clé. Pourra-t-elle lire en clair les messages chiffrés interceptés ? Justifier.

d. Eve a réussi à obtenir la clé publique de Bob. Quelle malversation pourrait-elle commettre ?

Ex.5 Indiquer le ou les principes de sécurité correspondant à chaque technique de protection.

SHA-1 :

TLS :

AES :

El-Gamal :

Signature numérique :

Ex.6 À partir du flux binaire ci-dessous, indiquer en base 10 les données envoyées avec les Checksums calculés sur 15 bits.

0 0 1 0 1 0 0 0 1 1 1 1 1 0 1 0 1 1 0 0 0 0 0 0 0 0 0 1 0 0 0 0 1 1 1 1 1 0 0 0 0 1

Ex.7 Placer les avantages et les inconvénients de chacun des chiffrements dans la bonne case.

Algorithme	Avantages	Inconvénients
	A. Ne nécessite pas d'échange de clé B. Facilité d'intégration C. Plus performant et plus sécurisé D. Plus performant	1. Moins performant (Coûteux en ressource, temps de calcul plus élevé) 2. Échange de deux informations (clé et message chiffré) 3. Moins sécurisé
Symétrique		
Asymétrique		
Hybride		

Ex.8 Numéroté l'ordre chronologique de chaque phase du protocole TLS d'après les descriptions.

Le serveur déchiffre avec sa clé privée la clé de session proposée par le client et applique la méthode de chiffrement convenu précédemment pour échanger les données.

Dans cette phase, le client et le serveur se mettent d'accord sur les paramètres de sécurité qui seront utilisés, en particulier les méthodes de chiffrement, dans le but de pouvoir mettre en œuvre les mêmes algorithmes.

Le serveur transmet au client un **certificat numérique** contenant sa clé publique. Le client peut vérifier la validité du certificat numérique auprès d'un tiers de confiance pour authentifier le serveur.

Le client génère une clé de session, qu'il chiffre avec la clé publique du serveur avant de la lui transmettre. Dans le cas optionnel où le serveur exige une authentification du client, celui-ci envoie aussi un certificat.

Ex.9 Indiquer le mot qui correspond à chacune des descriptions ci-dessous.

a. Cette procédure consiste à établir l'identité de l'utilisateur afin de répondre à la question : « Qui êtes-vous ? ».

b. Cette procédure permet à l'utilisateur d'apporter la preuve de son identité. Elle permet de répondre à la question : « Êtes-vous réellement cette personne ? ».

c. Cette procédure permet de signer un message avec clé privée. La vérification de la signature se fait avec la clé publique de l'expéditeur et prouve qu'un message a été créé par la personne possédant la clé privée, donc le contenu du message est validé.

Ex.10 Quel principe de sécurité est applicable à chacune des descriptions de l'exercice précédent ?

a.

b.

c.