Synthèse 1/2

Comment sont cryptées les données avant d'être communiquées ?

Cycle 4
Technologie
SYNTHÈSE
COLLÈGE

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 **CONFIDENTIALITÉ** 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 **INTÉGRITÉ** 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.**

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*** (cifertext) 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***.

Synthèse 2/2

Comment sont cryptées les données avant d'être communiquées ?

Cycle 4
Technologie
SYNTHÈSE
COLLÈGE

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.