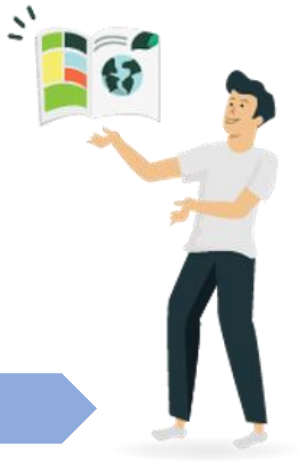
Cryptographie : Protocoles cryptographiques



Introduction

Salut à tous ! La cryptographie ne se limite pas uniquement au chiffrement des données. Elle englobe également des protocoles qui définissent comment ces techniques de chiffrement sont mises en œuvre pour garantir la sécurité. Aujourd'hui, nous allons plonger dans le monde fascinant des protocoles cryptographiques. Prêts ? Allons-y !

1. Protocole SSL/TLS

Qu'est-ce que c'est ?

SSL (Secure Socket Layer) et sa version améliorée, TLS (Transport Layer Security), sont des protocoles cryptographiques qui protègent la transmission de données sur Internet.

Comment ça fonctionne ?

Une « poignée de main » initiale est établie entre le client et le serveur.

Ils conviennent d'une clé de chiffrement pour la session.

Les données échangées sont ensuite chiffrées et déchiffrées à l'aide de cette clé.

Exemple concret :

Lorsque vous visitez un site web commençant par "https", cela signifie qu'il utilise SSL/TLS pour sécuriser la transmission de vos données.

2. Protocole SSH (Secure SHell)

Qu'est-ce que c'est ?

SSH est un protocole cryptographique utilisé pour administrer et accéder à distance à des machines de manière sécurisée.

Comment ça fonctionne ?

SSH utilise un chiffrement asymétrique pour établir une connexion sécurisée.

Une fois la connexion établie, il utilise un chiffrement symétrique pour la communication.

Exemple concret :

Un administrateur système peut utiliser SSH pour se connecter à un serveur distant et exécuter des commandes sans craindre que quelqu'un intercepte sa session.

3. Protocole IPsec (Internet Protocol Security)

Qu'est-ce que c'est ?

IPsec est un ensemble de protocoles utilisés pour sécuriser les communications Internet.

Comment ça fonctionne ?

IPsec opère au niveau du protocole IP, sécurisant tout le trafic IP entre deux points.

Il utilise des techniques comme le tunneling et l'encapsulation pour sécuriser les données.

Exemple concret :

IPsec est souvent utilisé dans les VPN (Virtual Private Networks) pour sécuriser la communication entre un client et un réseau d'entreprise.

Je retiens

- SSL/TLS : Sécurise la transmission de données sur Internet. Recherchez "https" dans la barre d'adresse pour savoir si un site utilise SSL/TLS.
- SSH : Permet une connexion à distance sécurisée à des machines. C'est l'outil de choix pour les administrateurs système.
- IPsec : Sécurise les communications Internet au niveau du protocole IP. Fréquemment utilisé dans les VPN.