**La Cryptographie.**

**Intro Cryptographie.**

La cryptographie est l'art de sécuriser la communication en convertissant des informations en un format illisible, de manière à ce qu'elles ne puissent être comprises que par des destinataires autorisés. C'est une discipline essentielle pour protéger la confidentialité, l'intégrité et l'authenticité des données dans le monde numérique. La cryptographie repose sur des techniques mathématiques et informatiques pour garantir la confidentialité des informations.

**Les Premières Inventions en Cryptographie.**

La cryptographie a des origines anciennes, remontant à l'Antiquité. Les premières méthodes de chiffrement consistaient en des substitutions de lettres, où chaque lettre du message original était remplacée par une autre lettre ou un symbole. L'une des méthodes les plus célèbres était le chiffre de César, où chaque lettre était décalée de trois positions dans l'alphabet.

Cependant, l'un des premiers systèmes de chiffrement complexe fut le chiffre de Vigenère, inventé par Blaise de Vigenère au XVIe siècle, qui utilisait un mot-clé pour déterminer les décalages de lettres. Cela a constitué une avancée significative dans le domaine de la cryptographie.

**Cryptographie et la Guerre.**

La cryptographie a souvent joué un rôle crucial pendant les guerres. Un exemple notoire est l'utilisation du code Navajo par les Marines américains pendant la Seconde Guerre mondiale. Les locuteurs de la langue Navajo ont été recrutés pour transmettre des messages codés qui étaient extrêmement difficiles à décoder pour les forces ennemies.

Cependant, le moment le plus célèbre de la cryptographie militaire est sans doute l'effort britannique pour décoder les communications allemandes pendant la Deuxième Guerre mondiale. Cela nous amène à Alan Turing.

**Cryptographie vs. Stéganographie.**

**Alan Turing et son Influence.**

Alan Turing était un mathématicien et informaticien britannique de renom. Il a eu un impact majeur sur le domaine de la cryptographie. Pendant la Seconde Guerre mondiale, Turing a travaillé au sein de l'équipe de déchiffrement britannique à Bletchley Park. Il a contribué au décryptage du code allemand Enigma en concevant la machine de Turing, une machine universelle capable de résoudre des problèmes mathématiques complexes, et qui a été utilisée pour casser le code Enigma.

L'œuvre d'Alan Turing en cryptographie a contribué de manière significative à la victoire des Alliés en aidant à décrypter les communications allemandes, ce qui a eu un impact direct sur le déroulement de la guerre.

**À quoi ça sert ?**

**Confidentialité des données**: La cryptographie est utilisée pour protéger la confidentialité des informations. Par exemple, lors de la transmission de données sensibles sur Internet (comme les informations de carte de crédit lors d'une transaction en ligne), la cryptographie est utilisée pour chiffrer les données de manière à ce qu'elles ne puissent pas être interceptées ou comprises par des tiers non autorisés.

**Intégrité des données**: Elle permet de s'assurer que les données n'ont pas été altérées pendant la transmission ou le stockage. Les codes de hachage sont couramment utilisés pour vérifier que les données n'ont pas été modifiées de manière non autorisée.

**Authentification**: La cryptographie est utilisée pour vérifier l'identité des parties impliquées dans une communication ou une transaction. Les certificats numériques et les signatures électroniques en sont des exemples.

**Non-répudiation**: Elle permet d'éviter que l'une des parties ne puisse nier son implication dans une transaction ou une communication. Les signatures numériques garantissent que le signataire ne peut pas nier avoir signé un document.

**Maintenant ?**

Aujourd'hui, la cryptographie joue un rôle fondamental dans notre vie quotidienne, en particulier à l'ère de la technologie de l'information. Voici comment elle est utilisée dans le monde contemporain

**Sécurité en ligne**: La cryptographie est utilisée pour sécuriser les communications en ligne, telles que les transactions bancaires, les échanges de courriels, les connexions aux réseaux sociaux, etc. Les protocoles HTTPS et SSL/TLS garantissent la sécurité des sites Web que nous visitons.

**Téléphonie mobile**: La cryptographie est intégrée aux réseaux de téléphonie mobile pour protéger les appels, les messages texte et les données mobiles.

**Cryptomonnaies**: Les cryptomonnaies telles que le Bitcoin s'appuient sur des algorithmes cryptographiques pour garantir la sécurité des transactions et la création de nouvelles unités de monnaie.

**Sécurité des données**: Dans le monde des entreprises, la cryptographie est essentielle pour protéger les données sensibles, telles que les informations clients, les secrets commerciaux et les données médicales.

**Sécurité des gouvernements**: Les gouvernements utilisent la cryptographie pour sécuriser les communications militaires, diplomatiques et gouvernementales.

**Internet des objets (IoT)**: La cryptographie est de plus en plus utilisée pour sécuriser les dispositifs connectés, tels que les caméras de sécurité et les thermostats intelligents.