CORRIGE EXAMENS SUR LA CRYPTOGRAPHIE

Réponses :

1- La cryptographie classique est l'art d'écrire ou de résoudre des codes, principalement utilisé pour la communication privée entre deux parties partageant des informations secrètes à l'avance.
2- La cryptographie classique se concentrait sur la confidentialité des messages, tandis que la cryptographie moderne couvre un champ plus large, incluant l'intégrité des données, l'authentification, et des protocoles complexes.
3- La stéganographie est l'art de cacher un message dans un autre support. Un exemple historique est celui de Damaratus, qui a caché un message sur des tablettes de bois recouvertes de cire.
4- Le principe de Kerckhoff stipule que la sécurité d'un système de cryptographie ne doit pas dépendre de l'algorithme, mais uniquement de la clé.
5- Le chiffrement de César est une méthode de chiffrement par substitution où chaque lettre du texte en clair est décalée de trois positions dans l'alphabet.
6- Le chiffrement de Vigenère utilise une clé pour décaler les lettres du texte en clair, ce qui rend le chiffrement plus complexe que celui de César, car chaque lettre peut être décalée d'un nombre différent de positions.
7- Un "one-time pad" est un chiffrement qui utilise une clé aléatoire de la même longueur que le message. Il est considéré comme parfait car il garantit un secret absolu, à condition que la clé ne soit utilisée qu'une seule fois.

8- La cryptographie symétrique utilise une seule clé pour chiffrer et déchiffrer, tandis que la cryptographie asymétrique utilise une paire de clés : une clé publique pour chiffrer et une clé privée pour déchiffrer.

9- Une fonction de hachage cryptographique convertit un message en une valeur de longueur fixe (hash) qui est unique. Ses propriétés principales incluent la résistance aux collisions et le fait qu'elle soit à sens unique.

10- Une signature numérique permet de vérifier l'intégrité et l'authenticité d'un message. Elle est créée en hachant le message et en chiffrant le hash avec la clé privée de l'expéditeur. Le destinataire utilise la clé publique pour vérifier la signature.