Ugo BEMBEN 2023

TP chiffrement

1. Le Code César est une méthode de cryptographie qui implique de décaler chaque lettre d'un message par un certain nombre de positions dans l'alphabet. Ce décalage est connu sous le nom de clé de chiffrement.

2. Le Carré de Vigenère est un système de chiffrement qui utilise une grille de substitution pour remplacer chaque lettre du message par une autre lettre. La grille est basée sur une clé de chiffrement qui détermine quelle ligne ou colonne de la grille utiliser pour chaque lettre.

3. La machine « Enigma » était une machine de chiffrement utilisée par l'armée allemande

4. pendant la Seconde Guerre mondiale. Elle utilisait un système complexe de substitution et de permutation pour crypter les messages.

5. Le téléphone rouge était une ligne de communication directe entre les États-Unis et l'Union soviétique pendant la guerre froide. Il a été utilisé pour réduire les erreurs de communication et faciliter les discussions entre les dirigeants des deux pays.

6. Le hachage est une technique de cryptographie qui convertit une chaîne de caractères en une valeur numérique unique et fixe. Les fonctions de hachage sont souvent utilisées pour stocker des mots de passe de manière sécurisée.

7. Le chiffrement à clé symétrique est un système de cryptographie où la même clé est utilisée pour chiffrer et déchiffrer un message. Les algorithmes de chiffrement à clé symétrique incluent DES, AES et Blowfish.

8. Le chiffrement à clé asymétrique est un système de cryptographie qui utilise deux clés distinctes, une publique et une privée. La clé publique est utilisée pour crypter le message, tandis que la clé privée est utilisée pour le décrypter. L'algorithme de chiffrement à clé asymétrique le plus connu est RSA.

9. Le chiffrement AES est un algorithme de chiffrement à clé symétrique largement utilisé pour protéger les données sensibles. Il utilise des blocs de 128 bits et des clés de 128, 192 ou 256 bits.

10. La différence entre le chiffrement bijectif et le hachage réside dans le fait que le chiffrement bijectif est réversible, tandis que le hachage ne l'est pas. Le chiffrement bijectif est utilisé pour crypter des messages, tandis que le hachage est utilisé pour stocker des mots de passe de manière sécurisée.

11. Les limites du hachage des mots de passe sont qu'il est possible pour les attaquants d'utiliser des techniques d'attaque telles que la force brute ou les attaques par dictionnaire pour deviner le mot de passe original à partir de la valeur de hachage. Pour éviter cela, les mots de passe doivent être salés avant d'être hachés.

12. Le salage des mots de passe est une technique de sécurité qui consiste à ajouter un préfixe ou un suffixe aléatoire à un mot de passe avant de le hacher. Cela rend plus difficile pour les attaquants de deviner le mot de passe original à partir de la valeur de hachage, même

TRUESCRIPT :

13. TrueCrypt est un logiciel de chiffrement de disque dur complet qui permet de créer un disque virtuel chiffré sur votre ordinateur. Il est utilisé pour protéger les données sensibles et confidentielles en les cryptant pour empêcher tout accès non autorisé.

14. TrueCrypt utilise une méthode de chiffrement basée sur la création d'un disque virtuel chiffré qui agit comme un conteneur pour stocker des fichiers et des dossiers sensibles. Ce conteneur peut être monté comme un disque dur normal, avec une lettre de lecteur assignée, et est accessible avec un mot de passe. Le contenu du disque virtuel est automatiquement crypté et décrypté en temps réel. Le chiffrement utilisé par TrueCrypt est différent des autres outils de chiffrement classiques en raison de sa méthode de création de conteneurs chiffrés plutôt que de crypter l'ensemble du disque dur.

15. L'utilisation de TrueCrypt au sein d'une société présente de nombreux avantages en matière de sécurité des données. Les données sensibles peuvent être stockées de manière sécurisée, même sur des ordinateurs portables ou des disques durs externes qui pourraient être perdus ou volés. TrueCrypt offre également une sécurité supplémentaire contre les attaques informatiques, les virus et les logiciels malveillants.

16. Depuis que TrueCrypt a été abandonné en 2014, plusieurs alternatives ont été proposées, notamment VeraCrypt, qui est une version améliorée et mise à jour de TrueCrypt, ou encore BitLocker de Microsoft, qui est intégré à certaines versions de Windows. D'autres alternatives incluent CipherShed et DiskCryptor, qui offrent également des fonctionnalités de chiffrement similaires.

Voicie la partie Bitlocker :

Watch my Powtoon: Project Kickoff

Voicie la partie Veracrypt :

Watch my Powtoon: 5 Whiteboard Tips