ENCRYPTION

PRESENTED TO:
Dr. Rajeshwari Trivedi
Assistant Professor

PRESENTED BY:
Aniket Kumar
BCA (5th Semester)

Department of Computer Science,
DSVV, Haridwar

IN THIS PRESENTATION

- What is Encryption?
- How does Encryption work?
- Encryption Techniques
- Types of Encryption
- Digital Signatures
- How does a digital signature work?
- Virtual Private Network

What is Encryption?

- Encryption is the process that scrambles readable text so it can only be read by the person who has the secret code, or decryption key.
- It helps provide data security for sensitive information.
- Encryption can help protect data you send, receive, and store, using a device.
- That can include text messages stored on your smartphone, running logs saved on your fitness watch, and banking information sent through your online account.

How does Encryption work?

- Encryption is the process of taking plain text, like a text message or email, and scrambling it into an unreadable format — called “cipher text.” This helps protect the confidentiality of digital data either stored on computer systems or transmitted through a network like the internet.
- When the intended recipient accesses the message, the information is translated back to its original form. This is called decryption.
- To unlock the message, both the sender and the recipient have to use a “secret” encryption key — a collection of algorithms that scramble and unscramble data back to a readable format.

Encryption Techniques

- An encryption key is a series of numbers used to encrypt and decrypt data. Encryption keys are created with algorithms. Each key is random and unique.
- There are two types of encryption systems: symmetric encryption and asymmetric encryption. Here's how they're different.
  - Symmetric encryption uses a single password to encrypt and decrypt data.
  - Asymmetric encryption uses two keys for encryption and decryption.
    - A public key, which is shared among users, encrypts the data.
    - A private key, which is not shared, decrypts the data.

Types of Encryption

- Data Encryption Standard (DES)
  - Data Encryption Standard is considered a low-level encryption standard. The U.S. government established the standard in 1977. Due to advances in technology and decreases in the cost of hardware, DES is essentially obsolete for protecting sensitive data.
- Triple DES
  - Triple DES runs DES encryption three times. Here's how it works: It encrypts, decrypts, and encrypts data — thus, "triple." It strengthens the original DES standard, which became regarded as too weak a type of encryption for sensitive data.
- RSA
  - RSA takes its name from the familial initials of three computer scientists. It uses a strong and popular algorithm for encryption. RSA is popular due to its key length and therefore widely used for secure data transmission.
- Advanced Encryption Standard (AES)
  - Advanced Encryption Standard is the U.S. government standard as of 2002. AES is used worldwide.
- TwoFish
  - Twofish is considered one of the fastest encryption algorithms and is free for anyone to use. It's used in hardware and software.

Digital Signatures

- A digital signature is a way to "seal" a document sent digitally and proves to the recipient that it hasn't been altered and is officially approved by you.
- These virtual fingerprints are unique to the sender and are not merely your handwriting like a typical signature.
- It is an encrypted stamp that can only be decrypted by the recipient, ensuring it is not intercepted and modified in transit.
- If the recipient gets the transmission and the digital signature does not match up with the digital certificate, then the document has been compromised.

How does a digital signature work?

- Digital signatures create a "hash" of the message. A hash is a string of numbers and letters that are pulled from the message, file, or document based on a mathematical algorithm.
- The hash is unique to the file, and any changes after the hash is created would change the hash.
- The sender signs the message or file digitally and then sends it to the recipient, who also generates a hash and then decrypts the sender's hash using the public key provided by the sender.
- The hashes are compared, and if they match, the message is considered authentic.

Virtual Private Network

- A virtual private network (VPN) gives the online privacy and anonymity by creating a private network from a public internet connection.
- VPNs mask our internet protocol (IP) address so our online actions are virtually untraceable.
- Most important, VPN services establish secure and encrypted connections to provide greater privacy than even a secured Wi-Fi hotspot.
- VPNs use one of three protocols based on PPP(Point to Point Protocol):
  - L2F (Layer 2 Forwarding) — Developed by Cisco; uses any authentication scheme supported by PPP
  - PPTP (Point-to-point Tunneling Protocol) — Supports 40-bit and 128-bit encryption and any authentication scheme supported by PPP
  - L2TP (Layer 2 Tunneling Protocol) — Combines features of PPTP and L2F and fully supports IPSec; also applicable in site-to-site VPNs

References

- What is encryption and how does it protect your data? - Norton
- 6 Types Of Encryption That You Must Know About - GoodCore
- What Is a Digital Signature and How Does It Work? - msn money
- What is a VPN? - Norton
- How a VPN (Virtual Private Network) Works – How Stuff Works