Cryptography Module-20

Introduction to Cryptography

Cryptography is a vital aspect of information security, involving the transformation of readable plain text into an unreadable format (cipher text). This process helps secure data and maintain privacy. Users employ encryption algorithms and keys for both encryption and decryption.

Terminologies:

Plain Text:

Original, readable text created by individuals (e.g., ABCD1234!@#$%).

Cipher Text:

Encrypted text resulting from applying an algorithm to plain text.

Encryption:

The process of converting plain text to cipher text.

Decryption:

The process of converting cipher text to plain text.

Ciphers:

In cryptography, ciphers are encrypted texts produced through the encryption process. For example:

Caesar Cipher: Shifts each letter by a fixed number (e.g., a shift of 3: A becomes X).

Example Of Ceaser Cipher:-

KEY: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Encryption Algorithm: Subtraction of 3 characters

1. **Plain Text: DURGESH**
    - Apply the encryption algorithm (subtract 3 characters):
        - D minus 3 = A
        - U minus 3 = R
        - R minus 3 = O
        - G minus 3 = D
        - E minus 3 = B
        - S minus 3 = P
        - H minus 3 = E
2. **Cipher Text: ARODBPE**

Now, to decrypt:

Decryption Algorithm: Addition of 3 characters

1. **Cipher Text: ARODBPE**
    - Apply the decryption algorithm (add 3 characters):
        - A plus 3 = D
        - R plus 3 = U
        - O plus 3 = R
        - D plus 3 = G
        - B plus 3 = E
        - P plus 3 = S
        - E plus 3 = H
2. **Plain Text: DURGESH**

Encryption Algorithms:

Hill Climb

Playfair Cipher

Common standards include:

AES (Advanced Encryption Standard)

DES (Data Encryption Standard)

RSA (Rivest Shamir Adleman)

Key System in Cryptography:

Cryptographic keys are crucial bits used by algorithms for encryption and decryption. There are two main types:

Asymmetric Key (Public Key Cryptography):

Uses two related but different keys. Publicly provided by the web server. Examples: Public Key Cryptography: RSA Encryption Algorithm

Symmetric Key (Private Key Cryptography):

Uses a single key for both encryption and decryption. Privately kept.

Steganography:

Steganography involves hiding data within other data, like images or audio files. The least significant bit (LSB) technique is a common method.

Steganography Using Steghide

Steghide is a popular command-line tool used for embedding and extracting secret messages or files inside other files, also known as steganography. It provides a simple and effective way to hide information within images or audio files. Here's a basic guide on using Steghide:

Installation

Ensure that Steghide is installed on your system. You can install it using the package manager of your operating system. For example, on Linux, you can use

```
sudo apt-get install steghide
```

Embedding Data:

Command Syntax:

```
steghide embed -cf <cover file> -ef <embedded file> -sf <output file> -p <passphrase>
```

Example:

```
steghide embed -cf cover.jpg -ef secret.txt -sf stego.jpg -p mypass
```

This command hides the content of `secret.txt` inside the `cover.jpg` image and creates a new image file named `stego.jpg`.

Extracting Data:

Command Syntax:

```
steghide extract -sf <stego file> -xf <output file> -p <passphrase>
```

Example:

```
steghide extract -sf stego.jpg -xf extracted.txt -p mypass
```

Hashes

Hash functions convert data into fixed-size alphanumeric strings. Unlike encryption, hashes are irreversible. Examples include MD5 Hash and Base64 Encoding.

- **Cracking Methods for Hashes:**
  - Create a dictionary, hash each word, and compare with the target hash.

Hash Formats:

1. **Base64 Encoding:**
   - Converts plain text into alphanumeric form.
2. **MD5 (Message Digest 512 bit):**
   - Converts plain text into a fixed-length hexadecimal text.

Suggested Video -. **Watch here**.

MD algorithms create fixed-size hash values, ensuring data integrity. Examples include:

- **MD5 (Message Digest 5):** Produces a 128-bit hash value.
- **SHA-1 (Secure Hash Algorithm 1):** Generates a 160-bit hash value.
- **SHA-256, SHA-384, SHA-512:** Part of the SHA-2 family with varying hash lengths.

Automated Tool - Hashcat:

Hashcat is a powerful password recovery tool using GPU cores.

Usage:

```
hashcat -m 0 -a 3 <hashfile in txt> <dictionary|wordlist>
```

Example:

```
hashcat -m 0 -a 3 /root/Desktop/hash.txt /usr/share/wordlists/rockyou.txt
```