Steganography and Encryption (Chapter 5)

by Sean Sanders

Steganography: The Art of Hidden Communication

Steganography is the practice of concealing a message within another message or a physical object, to avoid detection. Unlike encryption, which scrambles data to make it unreadable, steganography hides the very existence of the communication. The goal is to ensure no one suspects a secret message even exists.

A Hidden History: Steganography Through the Ages

From ancient battlefields to modern digital files, steganography has a long and ingenious past, evolving alongside communication methods to keep secrets safe.

Ancient Greece

Histiaeus tattooed messages onto a slave's shaved scalp, waiting for hair regrowth to conceal the secret.

Roman Empire

Secret writings were etched onto wood tablets, then covered with wax to appear as blank surfaces.

WWII Microdots

German spies reduced documents to tiny photographs, often hidden as a period on a letter or postcard.

Digital Era

Messages are embedded invisibly within digital media like images, audio, or video files, exploiting data redundancy.

Example

stylesuxx.github.io

Steganography Online

To encode a message into an image, choose the image you want to use, enter your text and hit the Encode button. Save the last image, it will contain your hidden message. Remember, the more text you want to hide, the larger the image has to be. In case you chose an image that is too...

sandilands.info

Steganography Example

Here is a simple example of steganography. In this case a message will be include in a image. For simplicity, the message is not encrypted although it could be. outguess is the application being used. It is freely available for Linux operating systems.

Encryption: Securing Communication

Encryption transforms information into a secret code to protect it from unauthorized access. Unlike steganography, which conceals the mere presence of a message, encryption openly acknowledges that data exists but renders it unreadable without the correct decryption key. Its primary goal is confidentiality, ensuring that even if intercepted, the message's content remains private.

Encryption History: A Journey Through Secrecy

From ancient codes to modern algorithms, the art of securing messages has evolved significantly over centuries, adapting to new threats and technological advancements.

1

Ancient Ciphers

Early methods like the Caesar Cipher and Scytale offered basic protection, often relying on simple substitution or transposition of letters.

2

Renaissance to 19th Century

More sophisticated ciphers, such as Vigenère, emerged. However, cryptanalysis also advanced, creating a continuous arms race between secrecy and decipherment.

3

World War Eras

Mechanical devices like the Enigma Machine dramatically increased complexity. Their eventual decryption significantly impacted the course of global conflicts.

4

Digital Age

The advent of computers enabled powerful algorithms like DES and AES, forming the backbone of secure digital communication for individuals and nations alike.

Symmetric vs. Asymmetric Encryption

Understanding the distinction between symmetric and asymmetric encryption is fundamental to modern cybersecurity, as each serves different purposes and addresses unique challenges in secure communication.

Symmetric Encryption

Uses a single, identical key for both encrypting and decrypting data. It's highly efficient and fast for large volumes of data, but securely sharing the key between parties can be a challenge.

Asymmetric Encryption

Employs a pair of mathematically linked keys: a public key for encryption and a private key for decryption. Slower than symmetric encryption, it excels in secure key exchange and digital signatures.

Examples of Encryption Algorithms

Both symmetric and asymmetric encryption employ various algorithms, each with distinct strengths and applications in securing digital communications.

Symmetric Algorithms

- **AES (Advanced Encryption Standard):** The current standard for government and industry, known for its speed and security.
- **DES (Data Encryption Standard):** An older algorithm, now considered insecure for most applications but historically significant.
- **3DES (Triple DES):** An enhancement of DES, offering improved security but is slower than AES.

Asymmetric Algorithms

- **RSA (Rivest–Shamir–Adleman):** Widely used for secure data transmission, digital signatures, and key exchange due to its strong security based on prime numbers.
- **ECC (Elliptic Curve Cryptography):** Offers similar security to RSA with smaller key sizes, making it ideal for mobile and low-bandwidth applications.
- **Diffie-Hellman Key Exchange:** Primarily used for securely exchanging cryptographic keys over a public channel, laying the foundation for further encrypted communication.

Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) is a powerful form of public-key cryptography that relies on the algebraic structure of elliptic curves over finite fields. It provides a level of security comparable to older methods like RSA, but with significantly smaller key sizes.

Smaller Keys

ECC achieves high security with much shorter key lengths, leading to faster computations and reduced storage requirements.

Strong Security

Its security is based on the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP), making it robust against attacks.

Modern Adoption

Widely used in modern applications such as TLS/SSL, digital signatures, and cryptocurrencies for efficient security.

Examples

Wierk

Caesar cipher: Encode and decode online

Method in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. The method is named after Julius Caesar, who used it in hi...

Wierk

Vigenère cipher: Encrypt and decrypt online

Method of encrypting alphabetic text by using a series of interwoven Caesar ciphers based on the letters of a keyword. Though the 'chiffre indéchiffrable' is easy to...

devglan

AES Encryption and Decryption Online

A free online tool for AES encryption and decryption. This aes calculator supports aes encryption and decryption in ECB, CBC, CTR and GCM mode with key sizes 128, 192, an...