Course Name: "CRYPTOGRAPHY"

Course Code: B031009T

C.L. Jain College, Firozabad

(Affili. to Dr. B.R. Ambedkar University, Agra)

Cryptosystem

A cryptosystem is a set of algorithms, protocols, and procedures used to enable secure communication or data transmission by encrypting and decrypting information. It typically consists of cryptographic algorithms for encryption and decryption, key generation and management mechanisms, and protocols for secure communication between parties. Cryptosystems are essential for ensuring confidentiality, integrity, and authenticity of data in various applications such as secure messaging, online banking, e-commerce, and more. Examples of cryptosystems include RSA, AES, and Elliptic Curve Cryptography (ECC).

Symmetric cipher model

The symmetric cipher model, also known as symmetric-key cryptography, is a cryptographic approach where the same key is used for both encryption and decryption of data. In this model, both the sender and the receiver share a secret key, which they use to encrypt and decrypt messages.
Symmetric ciphers are efficient for encrypting and decrypting large amounts of data because they typically involve simpler mathematical operations compared to asymmetric encryption. However, one of the main challenges with symmetric ciphers is securely sharing the secret key between the communicating parties. This is often achieved through secure key exchange protocols or by physically exchanging the key in a secure manner.
Examples of symmetric cipher algorithms include Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple DES (3DES), and Blowfish. These algorithms are widely used in various applications where efficient encryption and decryption are required, such as data storage, network communication, and securing sensitive information.

Classical encryption techniques

Classical encryption techniques refer to historical methods of encrypting plaintext into ciphertext without the use of modern computers or complex mathematical algorithms. These techniques were primarily used before the advent of computers and modern cryptographic methods. Classical encryption techniques typically rely on simple substitution or transposition methods.

Substitution Ciphers:

In substitution ciphers, each letter in the plaintext is replaced with another letter or symbol according to a predetermined rule. One of the most famous substitution ciphers is the Caesar cipher, where each letter is shifted a certain number of places down or up the alphabet.

Transposition Ciphers:

In transposition ciphers, the letters of the plaintext are rearranged according to a certain system or rule to produce the ciphertext. An example of a transposition cipher is the Rail Fence cipher, where the plaintext is written in a zigzag pattern across multiple lines, and then the letters are read off in a different order to create the ciphertext.

Polyalphabetic Substitution Ciphers:

These ciphers involve multiple substitution alphabets, where different letters in the plaintext are replaced with different letters according to different substitution rules. The Vigenère cipher is a well-known example of a polyalphabetic substitution cipher.

Playfair Cipher:

The Playfair cipher is a digraph substitution cipher that encrypts pairs of letters (digraphs) instead of single letters. It uses a 5x5 grid of letters (usually excluding 'J'), and a keyword to generate the grid.

One-Time Pad:

While not strictly classical, the one-time pad is a symmetric-key encryption technique that predates modern computing. It involves using a random key that is at least as long as the plaintext and used only once. The key is combined with the plaintext using modular addition to produce the ciphertext.

Classical encryption techniques are generally not considered secure by modern standards due to their susceptibility to cryptanalysis, especially with the advent of computers and sophisticated cryptographic methods. However, they played a significant role in the history of cryptography and laid the foundation for modern cryptographic techniques.

Caesar cipher

The Caesar cipher, also known as the shift cipher, is one of the simplest and earliest known substitution ciphers used in cryptography. It is named after Julius Caesar, who is historically reported to have used this cipher for secret communication. In the Caesar cipher, each letter in the plaintext is shifted a certain number of places down or up the alphabet. For example, with a left shift of 3, 'A' would be replaced by 'X', 'B' would become 'Y', and so on. The shift value is the key of the cipher.

The general formula for encryption using the Caesar cipher is:
$E(x) = (x + k) \bmod 26$ where:
$E(x)$ is the encrypted letter x is the numerical value of the plaintext letter ($A=0$, $B=1$, ..., $Z=25$) k is the shift value (the key) mod 26 ensures that the result remains within the range of the alphabet (0 to 25) Decryption using the Caesar cipher involves shifting the letters of the ciphertext in the opposite direction by the same number of places.
The formula for decryption is:
$D(x) = (x - k) \bmod 26$ where $D(x)$ is the decrypted letter.

Despite its simplicity, the Caesar cipher can be easily broken using brute force or frequency analysis, where the frequencies of letters in the ciphertext are analyzed to deduce the shift value. Nonetheless, it serves as a foundational example of substitution ciphers and illustrates basic principles of cryptography.

Block cipher Principles

Block ciphers are a type of symmetric encryption algorithm that operates on fixed-size blocks of plaintext, transforming each block into ciphertext under the control of a secret key. The basic principle of block ciphers involves breaking the plaintext into blocks of fixed size (e.g., 64 or 128 bits), and then applying a series of cryptographic transformations (rounds) to each block based on the encryption key. The same key is used for both encryption and decryption.

Key principles of block ciphers include:

Substitution: Block ciphers typically involve substitution, where plaintext blocks are replaced with ciphertext blocks based on a transformation determined by the key. This substitution process often involves a series of substitution boxes (S-boxes) that perform nonlinear transformations on the input data.
Permutation: In addition to substitution, block ciphers also involve permutation, where the order of the bits within the block is rearranged according to the encryption key. This permutation process is usually achieved through a series of permutation boxes (P-boxes) or permutation functions.
Key Expansion: Block ciphers often require key expansion mechanisms to generate a set of round keys from the original encryption key. These round keys are used in the cryptographic transformations applied to each block during encryption and decryption.
Rounds: Block ciphers typically operate in multiple rounds, where each round consists of a combination of substitution, permutation, and key mixing operations. The number of rounds can vary depending on the specific block cipher design, with more rounds generally providing increased security at the cost of performance.
Feistel Structure: Many block ciphers are based on the Feistel structure, which divides the input block into two halves and applies separate transformations to each half in each round. The output of one half is combined with the other half in a reversible manner, typically through XOR operations.

Example: The Advanced Encryption Standard (AES) is a widely used block cipher that follows the principles outlined above. AES operates on 128-bit blocks and supports key sizes of 128, 192, or 256 bits. It consists of a series of substitution and permutation operations, known as the SubBytes, ShiftRows, MixColumns, and AddRoundKey transformations, applied in multiple rounds based on the encryption key. AES has a fixed number of rounds depending on the key size: 10 rounds for a 128-bit key, 12 rounds for a 192-bit key, and 14 rounds for a 256-bit key.

Shannon theory of diffusion and confusion

The Shannon Theory of Diffusion and Confusion, formulated by Claude Shannon in the 1940s, is a fundamental concept in the field of cryptography that serves as a guiding principle for designing secure encryption algorithms.

Diffusion:

This concept refers to spreading the influence of the plaintext throughout the ciphertext in a manner that makes the relationship between the plaintext and the ciphertext as complex and unpredictable as possible. In other words, even a small change in the plaintext should result in significant changes throughout the ciphertext. Achieving diffusion ensures that local changes in the plaintext are not localized in the ciphertext, making it harder for an attacker to discern patterns or relationships between the two.

Confusion:

Confusion involves making the relationship between the plaintext and the encryption key as complex and obscure as possible. This means that even if an attacker knows the encryption algorithm being used, without knowledge of the encryption key, it should be computationally infeasible to decrypt the ciphertext and recover the plaintext. Confusion aims to hide any statistical or structural patterns in the plaintext by introducing randomness and non-linearity through the encryption process.

The Shannon Theory of Diffusion and Confusion provides a theoretical framework for evaluating the effectiveness of encryption algorithms in terms of their ability to thwart various cryptographic attacks, including brute-force attacks, statistical attacks, and differential cryptanalysis.
Encryption algorithms designed based on these principles are typically considered secure against such attacks if they provide sufficient levels of diffusion and confusion.
Encryption algorithms such as the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES) are designed with diffusion and confusion principles in mind, making them widely adopted and trusted in various applications requiring secure communication and data protection.

Data encryption standard (DES)

The Data Encryption Standard (DES) is a symmetric-key block cipher algorithm that was developed in the early 1970s by IBM and adopted by the United States government as a federal standard for encryption and decryption of sensitive, unclassified information. DES was later standardized by the National Institute of Standards and Technology (NIST) in 1977.

Key features of the Data Encryption Standard (DES) include:

Symmetric-Key Cryptography: DES is a symmetric-key encryption algorithm, meaning the same key is used for both encryption and decryption of data. This key is typically 56 bits long, although DES operates on 64-bit blocks of data.
Block Cipher: DES operates on fixed-size blocks of plaintext (64 bits) and produces corresponding blocks of ciphertext using a series of cryptographic transformations. Each block is processed independently.
Feistel Cipher Structure: DES is based on a Feistel cipher structure, which divides the input block into two halves and applies a series of alternating substitution (S-box) and permutation (P-box) operations to each half in multiple rounds.
Key Expansion: DES employs key expansion to generate a set of round keys from the original 56-bit encryption key. These round keys are used in the encryption and decryption process to modify the data block in each round.
Multiple Rounds: DES operates in 16 rounds, with each round consisting of a combination of substitution, permutation, and key mixing operations. The number of rounds provides security against various cryptographic attacks.

Thank You