Chapter 20

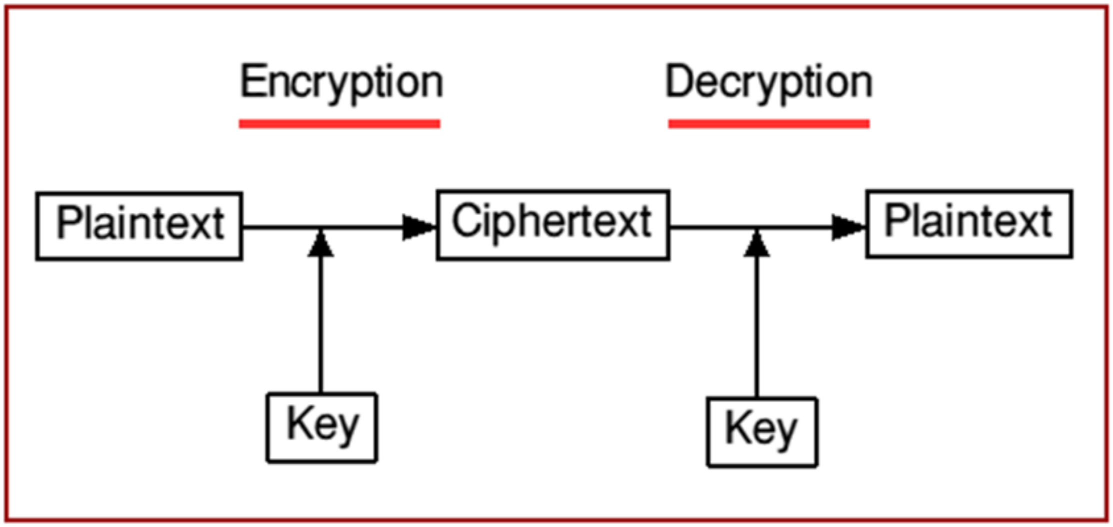
Cryptography

Theory

Ethical Hacking

Cryptography

Cryptography is a process of converting plain text data (readable) into ciphertext (unreadable) data to protect confidentiality so that unauthorized users cannot understand what is transmitted. Encryption algorithms are used to perform mathematical computation on data using the key and convert data to ciphertext. The algorithm that is chosen to perform encryption with some key can also be used for decryption. Decryption is the process of converting ciphertext to plaintext. Encryption is a reversible operation, i.e., converting plaintext to ciphertext and vice versa is possible using the algorithm and key. Cryptography is used to protect the confidentiality of information shared on the internet such as email messages, chat sessions, web transactions, personal data, corporate data, e-commerce applications, etc.



Objectives of Cryptography

Confidentiality: To ensure that private or confidential information is not made available or disclosed to unauthorized individuals.

Integrity: To ensure that an unauthorized individual does not tamper the information exchanged over the internet.

Availability: To ensure that services are not denied to authorized users.

Types of Cryptography

Based on the number of keys used for encryption they are classified into two types

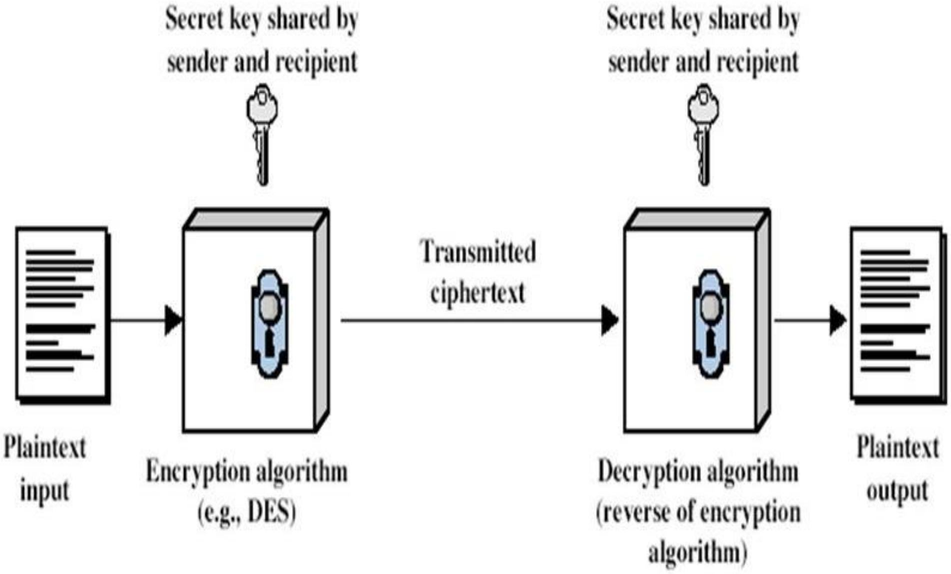
- Symmetric key cryptography
- Asymmetric key cryptography

Symmetric Encryption

The symmetric key algorithm is also known as the secret key algorithm. Symmetric key algorithms use the same cryptographic key for both encryption and decryption. Data Encryption Standard (DES) and Advanced Encryption Standard (AES) algorithms are the most commonly used symmetric key algorithm which uses a key at sender side for encryption, and the receiver uses the same key for decryption. To make two parties (sender and receiver) to communicate confidentially, they must first exchange the secret key so that each party can encrypt messages to send and decrypt messages to read. This process is known as key exchange. This key is shared between two parties over a secure channel. Based on input data these algorithms can be further divided into two categories

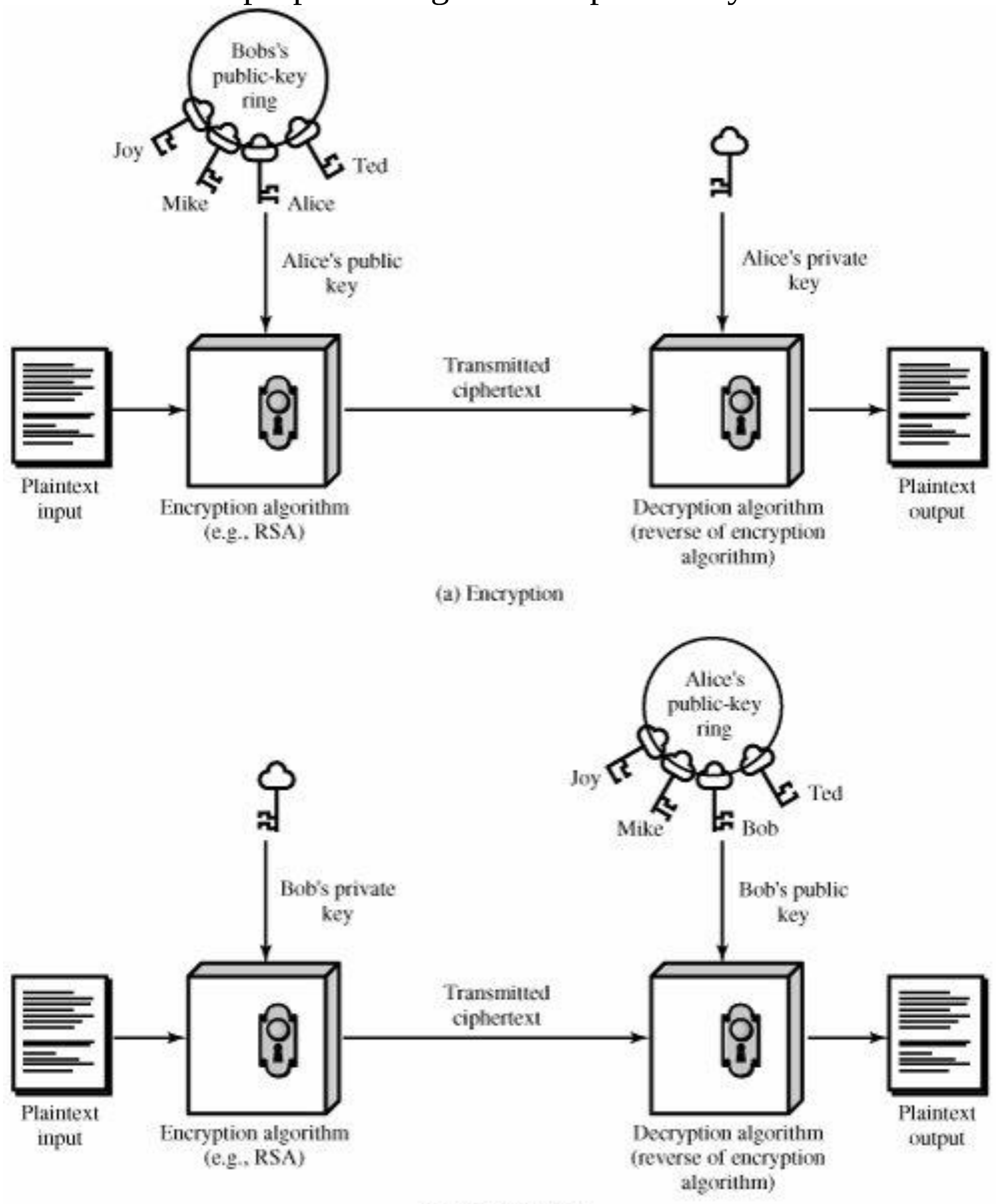
Block ciphers: Block ciphers encrypt data one block at a time.
Stream ciphers: Stream ciphers encrypt data byte by byte.

The strength of any cryptographic algorithm depends on the secrecy of the key. If keys are not securely shared, then unauthorized parties can gain access to a secret key used for encryption and they can un-encrypt data and read every packet shared between two parties.


Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Asymmetric Encryption

Asymmetric key algorithms use two different keys known as a public key and a private key for encryption and decryption. The sender and receiver generate a private key which is kept secret (not shared with anyone) and a public key which is shared with other parties. In case of asymmetric algorithms, senders encrypt messages using the receiver's public key. The receiver's private key can only decrypt this encrypted message. In this manner, it ensures that both the confidentiality and integrity of information are preserved. The best part of asymmetric encryption is its Key Management system; it takes advantage of Public Key Infrastructure for proper management of public keys.

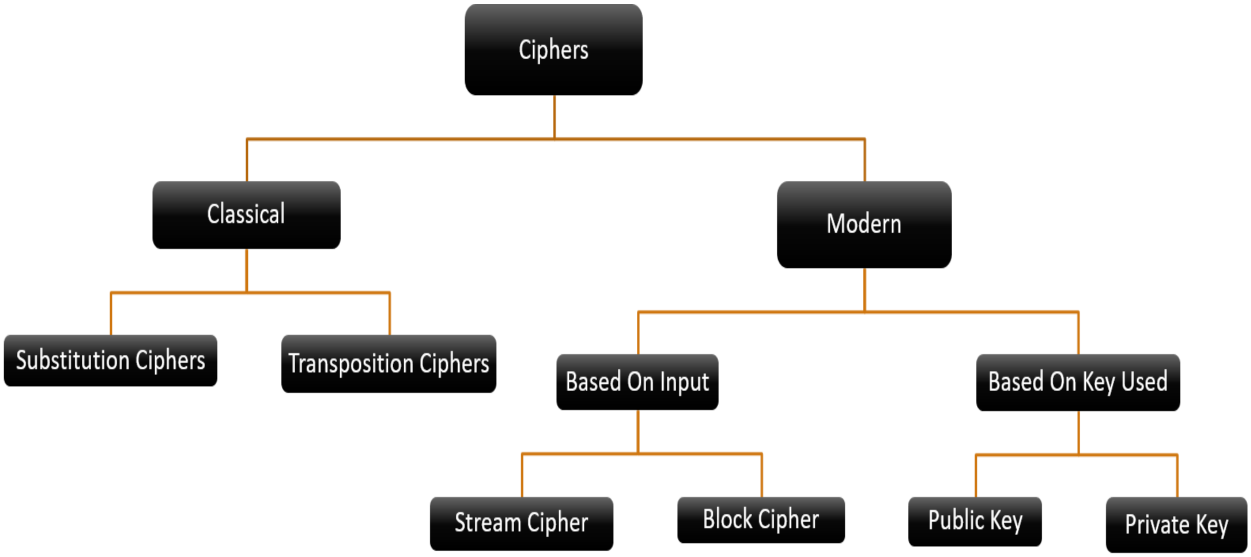


(a) Encryption

(b) Authentication

Cipher

In cryptography, a cipher is an algorithm that performs encryption or decryption in a series of well-defined steps that can be followed as a procedure. Ciphers are classified based on input data, a number of keys used for encryption.



Classical ciphers

Classical ciphers are cryptographic algorithms that have been used in the past (practically computed and solved manually). Classical ciphers are often divided into substitution ciphers and transposition ciphers.

Substitution cipher: In a substitution cipher, letters are systematically replaced throughout the message for other letters. In these cipher method monoalphabetic substitution ciphers, where just one cipher alphabet is used. Polyalphabetic substitution cipher, where multiple cipher alphabets are used.

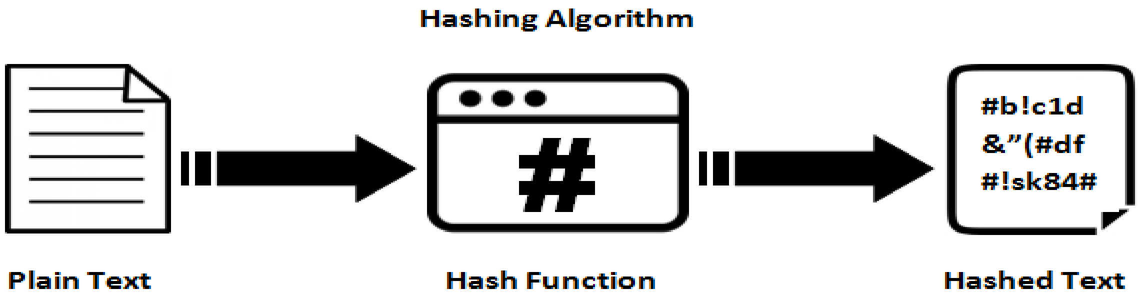
Transposition ciphers: In a transposition cipher, the letters themselves are kept unchanged, but their order within the message is scrambled. Many transposition ciphers are done according to geometric design.

Modern ciphers

Modern ciphers are designed based on various concepts of mathematics such as number theory, computational complexity theory, and probability theory. It needs the computational power to encrypt and decrypt the data. Modern encryption methods are divided into two type based on input data (Block and Stream ciphers), and a number of keys (secret key and public key) used.

Hash function

A hash function performs a series of mathematical operations to convert input data into a fixed length alphanumeric characters. The input to the hash function is an arbitrary length, but the output is always of fixed length.



Features of Hash Functions

- **Fixed Length Output**: Hash function converts data of arbitrary length to a fixed length.
- **The efficiency of Operation**: Computationally hash functions are much faster than asymmetric encryption.

Examples of the Hash functions

These are examples of well-known hash functions:

Hashed Message Authentication Code (HMAC): Combines authentication via a shared secret with hashing.

Message Digest 2 (MD2): Byte-oriented, produces a 128-bit hash value from an arbitrary-length message, designed for smart cards.

MD4: Similar to MD2, designed specifically for fast processing in software.

MD5: Similar to MD4 but slower because the data is manipulated more.

Secure Hash Algorithm (SHA): Modeled after MD4 and proposed by NIST for the Secure Hash Standard (SHS), produces a 160-bit hash value.

Steganography

Steganography is an art of hiding a secret message within an ordinary message and extracting it at the destination to maintain the confidentiality of data. The program named 'snow' is used to conceal messages in ASCII text by appending whitespace to the end of lines. There are different tools that can hide text in pictures so that to retrieve the hidden secret message the receiver must use the same tool as sender used to hide the text message. Steganalysis is the art of discovering and rendering secret messages using steganography.

Cryptography Attacks

Cryptography attacks are based on the assumption that the cryptanalyst has access to the encrypted information.

- Chosen plaintext
- Adaptive chosen plaintext attack
- Known plaintext
- Known ciphertext
- Chosen ciphertext
- Chosen key
- Rubber cosh cryptanalysis

Brute force attack is a process of defeating a cryptographic scheme by trying a large number of possible keys until the correct encryption key is discovered.

References:

1. Stallings, W. (2017). *Cryptography and network security: Principles and practice*. Boston: Pearson Prentice Hall.
2. Ninocrudele. (2018, April 03). Retrieved from http://ninocrudele.com/azureleap-aes-encryption-and-hash-algorithm-concepts-and-best-practices-in-cloud