Cryptography:

Cryptography is the science of securing data. It is designed to solve four important security issues — confidentiality, authentication, integrity and control over the participants.

Cryptography: is a process of converting any type of data(*data at rest and data in transit/motion*) in a form that only those people for whom it is actually intended for can understand/read/evaluate that data and no one else. Once the data is converted/modulated/changed(also known as ***ciphertext***) then no unauthorized users would be able to access this information as it will not be available in raw data form(also known as ***plaintext***)

substitution cipher

In cryptography, a **substitution cipher** is a method of encrypting in which units of plaintext are replaced with the ciphertext, in a defined manner, with the help of a key; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing the inverse substitution process to extract the original message.

Hiding some data is known as encryption. When plain text is encrypted it becomes unreadable and is known as ciphertext. In a Substitution cipher, any character of plain text from the given fixed set of characters is substituted by some other character from the same set depending on a key. For example with a shift of 1, A would be replaced by B, B would become C, and so on.

Algorithm for Substitution Cipher:
Input:

- A String of both lower and upper case letters, called PlainText.
- An Integer denoting the required key.

Procedure:

- Create a list of all the characters.
- Create a dictionary to store the substitution for all characters.
- For each character, transform the given character as per the rule, depending on whether we're encrypting or decrypting the text.
- Print the new string generated.

Transposition cipher

In cryptography, a **transposition cipher** is a method of encryption which scrambles the positions of characters (*transposition*) without changing the characters themselves.

Transposition Cipher is a cryptographic algorithm where the order of alphabets in the plaintext is rearranged to form a cipher text. In this process, the actual plain text alphabets are not included.

A simple example for a transposition cipher is **columnar transposition cipher** where each character in the plain text is written horizontally with specified alphabet width. The cipher is written vertically, which creates an entirely different cipher text.

Consider the plain text **hello world**, and let us apply the simple columnar transposition technique as shown below

h	e	l	l
o	w	o	r
l	d		

The plain text characters are placed horizontally and the cipher text is created with vertical format as **: holewdlo lr.** Now, the receiver has to use the same table to decrypt the cipher text to plain text.

Making “Good” Encryption Algorithms

Substitution algorithms “hide” the plaintext and dissipate high letter frequenciesTransposition algorithms scramble textMany “good” algorithms combine both techniques

Shannon’s Characteristics of “Good” Ciphers

- Amount of secrecy needed should determine the amount of labor appropriate for encryption/decryption.
- Set of keys and enciphering algorithm should be free from complexity.
- Implementation should be simple
- Errors in ciphering should not propogate.
- Size of ciphertext should be no larger than the size of the plaintext

Properties of “Trustworthy” Encryption Systems

- Based on sound mathematics
- Been analyzed by competent experts and found to be sound Stood the “test of time”
- Three Examples:
- DES (data encryption standard)
- RSA (Rivest-Shamir-Adelman)
- AES (Advanced Encryption Standard)

Symmetric and Asymmetric Encryption Systems

Symmetric requires one “secret” key that is used for encryption AND decryption (e.g. Caesar cipher might use a “key” of 3 to indicate shift by 3). As long as key remains secret, authentication is provided. Problem is key distribution; if there are n users, we need n * (n-1)/2 unique keys.

Asymmetric requires two keys one of which is a “public key”. The public key is used for encryption and the “private” key is used for decryption. If there are n users, there are n public keys that everyone knows and n private keys known only to the user.

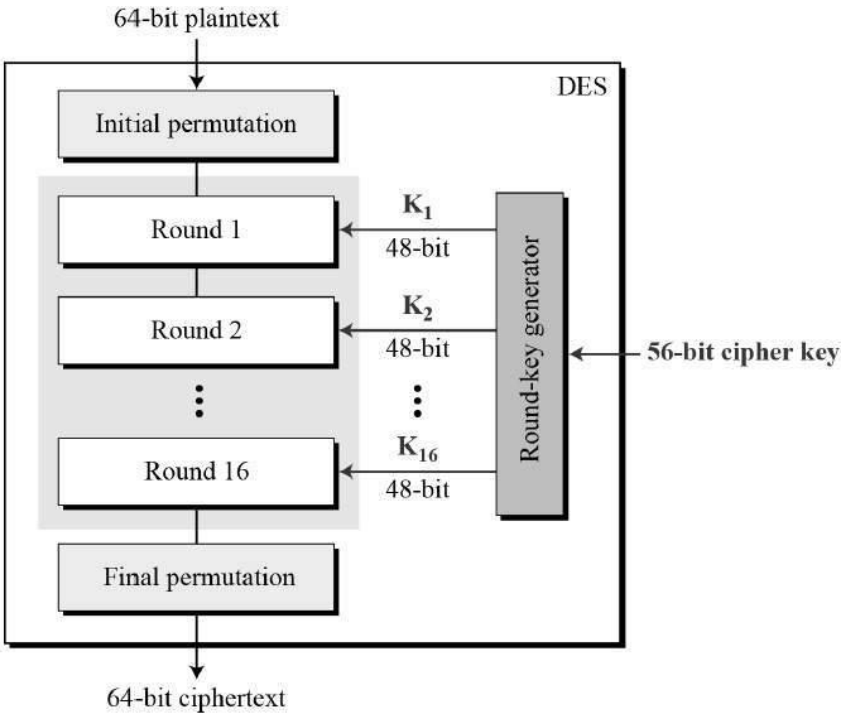
Data Encryption

Data encryption **converts data from a readable, plaintext format into an unreadable, encoded format: ciphertext**. Users and processes can only read and process encrypted data after it is decrypted. The decryption key is secret, so it must be protected against unauthorized access.

Data Encryption Standard(DES)

Data encryption standard (DES) has been found vulnerable to very powerful attacks and therefore, the popularity of DES has been found slightly on the decline. DES is a block cipher and encrypts data in blocks of size of 64 bits each, which means 64 bits of plain text go as the input to DES, which produces 64 bits of ciphertext. The same algorithm and key are used for encryption and decryption, with

minor differences. The key length is 56 bits. The basic idea is shown in the figure:



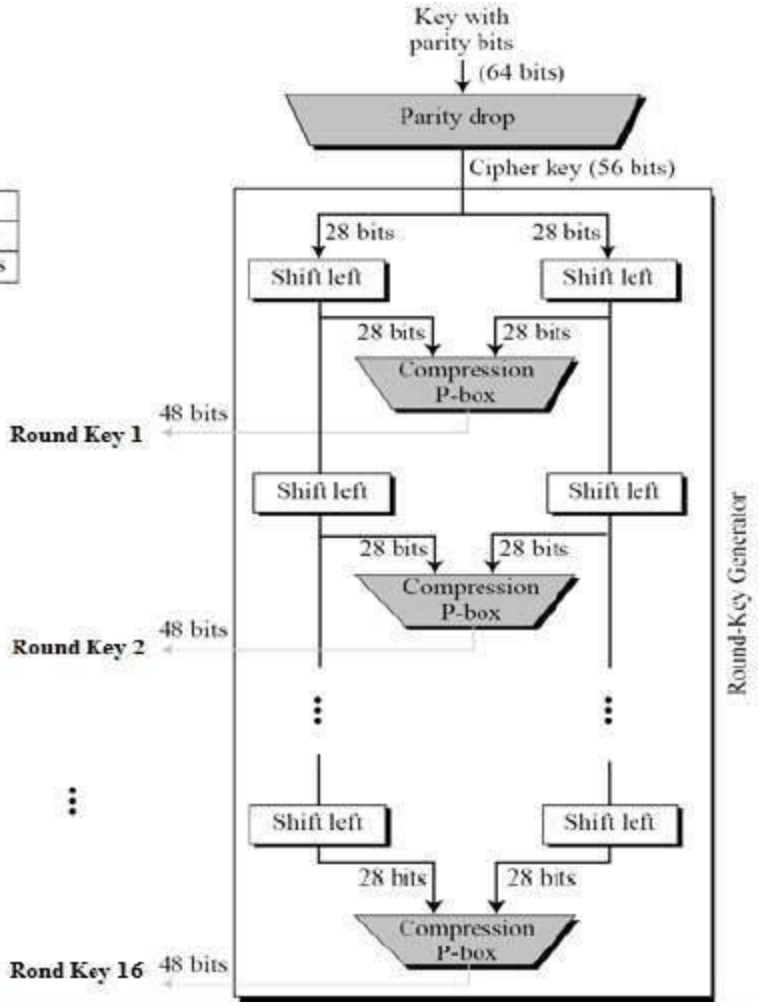
We have mentioned that DES uses a 56-bit key. Actually, the initial key consists of 64 bits. However, before the DES process even starts, every 8th bit of the key is discarded to produce a 56-bit key. That is bit positions 8, 16, 24, 32, 40, 48, 56, and 64 are discarded.

Key generation

The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key. The process of key generation is depicted in the following illustration −

Shifting

Rounds	Shift
1, 2, 9, 16	one bit
Others	two bits



- In the first step, the 64-bit plain text block is handed over to an initial Permutation (IP) function.
- The initial permutation is performed on plain text.
- Next, the initial permutation (IP) produces two halves of the permuted block; saying Left Plain Text (LPT) and Right Plain Text (RPT).
- Now each LPT and RPT go through 16 rounds of the encryption process.
- In the end, LPT and RPT are rejoined and a Final Permutation (FP) is performed on the combined block
- The result of this process produces 64-bit ciphertext.

Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.

Points to remember

- AES is a block cipher.
- The key size can be 128/192/256 bits.
- Encrypts data in blocks of 128 bits each.

That means it takes 128 bits as input and outputs 128 bits of encrypted cipher text as output. AES relies on substitution-permutation network principle which means it is performed using a series of linked operations which involves replacing and shuffling of the input data.

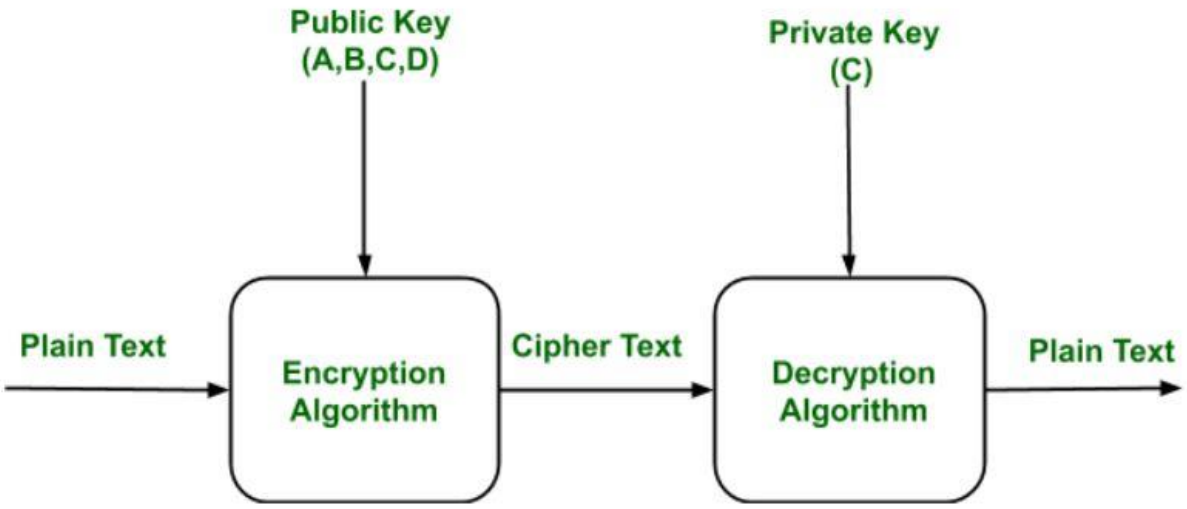
Working of the cipher :

AES performs operations on bytes of data rather than in bits. Since the block size is 128 bits, the cipher processes 128 bits (or 16 bytes) of the input data at a time.

The number of rounds depends on the key length as follows :

- 128 bit key – 10 rounds
- 192 bit key – 12 rounds
- 256 bit key – 14 rounds

Public Key Encryption : Asymmetric is a form of Cryptosystem in which encryption and decryption are performed using different keys-Public key (known to everyone) and Private key (Secret key). This is known as Public Key Encryption.



Components of Public Key Encryption:

Plain Text:

This is the message which is readable or understandable. This message is given to the Encryption algorithm as an input.

Cipher Text:

The cipher text is produced as an output of Encryption algorithm. We cannot simply understand this message.

Encryption Algorithm:

The encryption algorithm is used to convert plain text into cipher text.

Decryption Algorithm:

It accepts the cipher text as input and the matching key (Private Key or Public key) and produces the original plain text

Public and Private Key:

One key either Private key (Secret key) or Public Key (known to everyone) is used for encryption and other is used for decryption

CRYPTOGRAPHY IN EVERYDAY LIFE

Authentication/Digital Signatures:

Time Stamping:

Electronic Money:

Encryption/Decryption in email: