DATA ENCRPTION STANDARD

May 2, 2017

1 Introduction

1.1 Cryptography

Cryptography is practice and study of techniques for secure communication in insecure networks. The Word cryptography is derived form Greek words kryptos (hidden) and graphein (write). [**?**]
It uses mathematical techniques to encrpt and decrypt data. In recent times,Cryptography is every where In Secure Communications i.e, in web traffic (HTTPS) and wireless (GSM,Bluetooth). It is used for files on disk (EFS,TrueCrypt) and for Content protection like DVD, Blueray (CSS,AACS) and more.

1.1.1 History

The first known use of cryptography is found in non-standard hieroglyphs which is an inscription carved into the wall of a tomb around 1900 B.C in Egypt.[**?**]
There are three era's in cryptography:
1.Manual Era
2.Mechanical Era
3.Modern Era

- Manual Era

In this era,there was only usage of pen and paper i.e,everything was done manually. The first inscription also comes under this. Later, there were many forms that came into existence like Scytale, Atbash, Caesar.
SCYTALE is a tool used to perform a transposition cipher.It consists of a cylinder with a strip of parchment wound around it on which a message is

written.The ancient Greeks and the Spartans in particular used this cipher to communicate during military campaigns.The recipient uses a rod of the same diameter on which the parchment is wrapped to read the message. It has the advantage of being fast and not prone to mistakesa necessary property when on the battlefield. However,It can be easily broken.Since the strip of parchment hints strongly at the method,the ciphertext would have to be transferred to something less suggestive,somewhat reducing the advantage noted.

ATBASH cipher is a very specific case of a substitution cipher where the letters of the alphabet are reversed. In otherwords, all As are replaced with Zs, all Bs are replaced with Ys, and so on. Because reversing the alphabet twice will get you actual alphabet, you can encipher and decipher a message using the exact same algorithm.
Example:
Plaintext: This is a secret message
Ciphertext: Gsrh rh z hvxivg nvhhztv

CAESAR cipher is a substitution cipher where each letter in the original message is replaced with a letter corresponding to a certain number of letters up or down in the alphabet. The most used number was 3.The caesar cipher is also called as shift cipher.This is the most simplest forms of encryption.
Example:
Plaintext: Attack
Ciphertext: dwwdfn

▶ Mechanical Era

Use of machines for encryption started in 18th century during this era. Many machines were made at that time.some of them are Deisus Wadsworth(1817), Jeffersons encryptor and many more.In those the most used and Well reputed machine was Enigma(1920).

▶ Modern Era

This era of cryptography refers to computers. There are many number of cryptosystems that came into existence like RSA, DES, AES and more.

1.1.2 Types of Cryptography

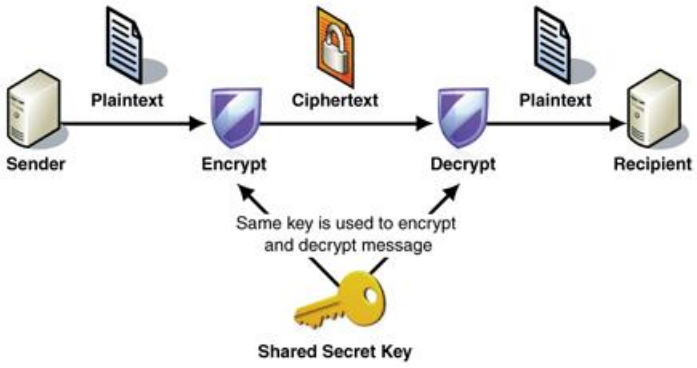


Figure 1: symmetric cryptography

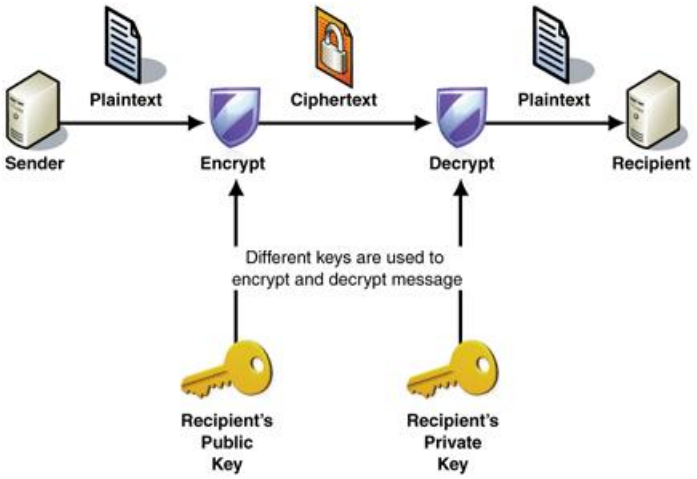


Figure 2: Asymmetric cryptography

1.2 DES

The Data Encryption Standard (DES) is a symmetric-key algorithm for the encryption of electronic data. Although now considered insecure, It was highly influential in the advancement of modern cryptography.It is a block cipher.

1.2.1 History of DES

The origins of DES go back to the early 1970s. In 1972, after concluding a study on the US government's computer security needs, the US standards body NBS(National Bureau of Standards) now named NIST(National Institute of Standards and Technology) identified a need for a government-wide standard for encrypting unclassified,sensitive information. Accordingly, on 15 May 1973, after consulting with the NSA,NBS solicited proposals for a cipher that would meet rigorous design criteria. None of the submissions,however,turned out to be suitable.A second request was issued on 27 August 1974. This time, IBM submitted a candidate which was deemed acceptable,a cipher developed during the period 19731974 based on an earlier algorithm, Horst Feistel's Lucifer cipher.
→ In 1970s,IBM created a crypto system called Lucifer for encryption of customers data.
→ In 1973, NIST made a proposal for national symmetric key cryptosystem.
→ IBM submitted Lucifer for validation.
→ Later on, changes were made by Walter Tuchman and that was accepted and called as DES.
→ DES is a symmetric block cipher, it encrypts 64 bits plain text with 64 bit key at a time.
→ Block cipher is an encryption algorithm that encrypts a fixed size of n-bits of data which is known
→ The usual sizes of each block are 64,128 and 256bits.[**?**]

3 The DES Cryptosystem

3.1 Description

The DES is a block cipher.It encrypts data in 64-bit blocks.this is a symmetric algorithm. A 64-bit block of plaintext goes in one end and a 64-bit block of ciphertext comes out the other end.Here,same algorithm and key are used for encryption and decryption.
The key length is 56-bits.The key is usually expressed as a 64-bits,but every eighth bit is used for parity checking and is ignored.These parity bits are the least significant bits of the key bytes.The key can be any 56-bit number

2 Background

2.1 Notation

In Cryptography,the simple XOR is used.It is an encryption algorithm that operates according to these principles:

$A \oplus 0 = A$,
$A \oplus A = 0$,
$(A \oplus B) \oplus C = A \oplus (B \oplus C)$,
$(B \oplus A) \oplus A = B \oplus 0 = B$

Here,XOR denotes the exclusive disjunction operation.
The logic behind this is,a string of text can be encrypted by applying the bitwise XOR to every character using a given key.
To decrypt it,we reapply the XOR function with the key so that it removes the cipher.

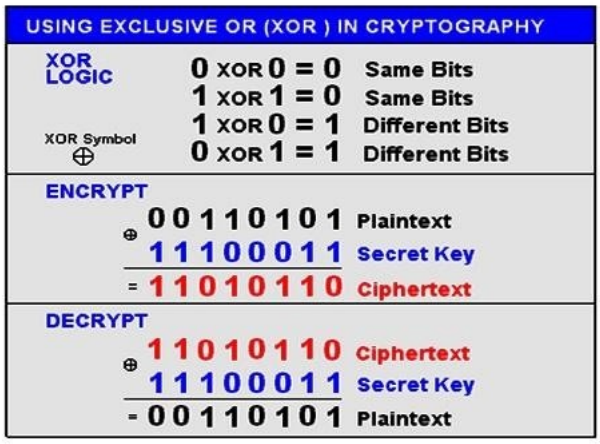


Figure 3: Xor operation.

2.2 Permutation

Permutation is the process of rearranging the bits in specified order. In DES, we have Initial and final permutations which are called as p-boxes.Each of these permutations takes a 64-bit input and permutes them according to a predefined rule. For example,In the initial permutation,the 58th bit in the input becomes the first bit in the output.Similarly,In the final permutation,the first bit in the input becomes the 58th bit in the output. In other words,if the rounds between these two permutations do not exist,the 58th bit entering the initial permutation is the same as the 58th bit leaving the final permutation.

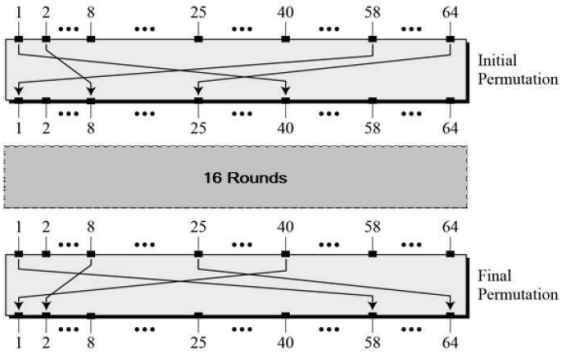
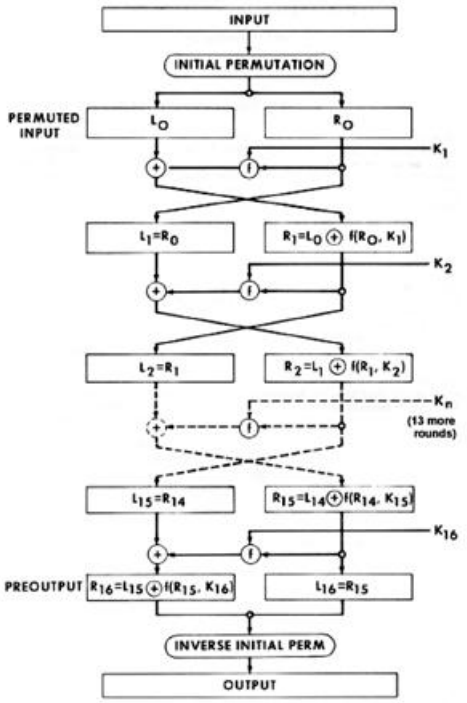


Figure 4: Initial and Final Permutation.

and can be changed at anytime.
The DES is a combination of a substitution followed by a permutation on the text,based on the key.This is known as a round.DES has 16 fiestel rounds,It applies the same combination of techniques on the plaintext 16 times.

3.2 Working of DES

DES operates on a 64-bit block of plaintext.After an initial permutation,the block is made into right half and left half each 32bits long. In each round,the key bits are shifted,and then 48 bits are selected from 56 bits of the key.The right half of the data is expanded to 48 bits through an expansion permutation, combined with 48 bits of a shifted and permuted key through an XOR,sent through 8 S-boxes producing 32 new bits,and permuted again.These four functions make Function f. The output of function f is then combined with the left half via another XOR.The result of these operations becomes the new right half and the old right half becomes the new left half. These operations are repeated for 16 times.



DES.

The DES encryption process consists of three main steps:
▶ Initial Permutation
▶ 16 Fiestal Rounds
▶ Final Permutation

Initial Permutation occurs before round 1,it transposes the input block.For example,the initial permutation moves bit 58 of the plaintext to bit position 1, bit 50 to bit position 2 and so on.

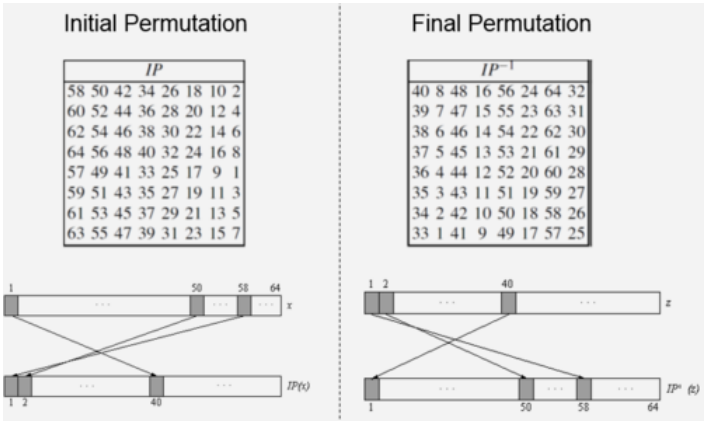


Figure 5: Initial and Final permutation.

In the fiestel round,the input is expanded and XORed with key and again compressed to its original size. Here the 32-bit input is expanded to 48-bit using expansion permutation by duplicating half of the bits. For each 4-bit input block,the first and fourth bits each represent two bits of the output block,while the second and third bits each represent one bit of the output block. For example,the bit in position 3 of the input block moves to position 4 of the output block and the bit in position 21 of the input block moves to positions 30 and 32 of the output block.

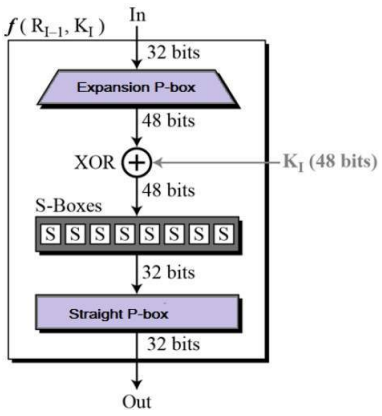


Figure 6: Expansion Box.

3.2.1 The Key Generation

Initially,the 64-bit DES key is reduced to a 56-bit key by ignoring every eighth bit.These bits can be used as parity check to ensure the key is error-free. After the 56-bit key is extracted,a different 48-bit subkey is generated for each of the 16 rounds of DES. Firstly,the 56-bit key is divided into 28-bit halves.Then,the halves are circularly shifted by either one or two bits,depending on the round. After being shifted,48 out of the 56 bits are selected.Because this operation permutes the order of the bits as well as selects a subset of bits, It is called as compression permutation.
Eventually,16 keys are generated and are saved for each fiestel round.

3.2.2 The S-box Substitution

The substitutions are performed by