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

1.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

2.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).

3.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

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.

2 Background