International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
Recent Trends in Mobile & Cloud Computing
(NCRMC- 08th & 09th October 2015)

RESEARCH ARTICLE OPEN ACCESS

Data encryption standard

Dipak.V.Ingle, Mangesh S. Hule
Computer Engineering Department Matoshri College of Engineering & Research Center, Nashik d.ingle@sanmati.in
Computer Engineering Department P.R.Pote Amravati mangeshhule@gmail.com

ABSTRACT
The Data Encryption Standard (DES) algorithm, adopted by the US government in 1977, is the US government's secret-key data encryption standard and is widely used around the world in a variety applications including banking and wide-area networking applications. It is a block cipher that transforms 64-bit data blocks under a 56-bit secret key, by means of permutation and substitution. It encrypts a confidential message into scrambled output under the control of the secret key. The input message is also known as "plaintext" and the resulting output message as "ciphertext". The idea is that only recipients who know the secret key can decrypt the ciphertext to obtain the original message. DES uses a 56-bit key, so there are 256 possible keys. Due to its importance, DES has received a great deal of cryptanalytic attention. However, besides using the complementation property, there were no short-cut attacks against the cipher until differential cryptanalysis was applied to the full DES.

I. INTRODUCTION

1.1 Cryptography Concept

Computer and network security is a new and fast moving technology and as such, is still being defined. When considering the desired learning outcomes of such a course, one could argue that a network security analyst must be capable of analyzing security from the business perspective in order to adhere to recent security legislation, and from the technical perspective in order to understand and select the most appropriate security solution. Network security originally focused on algorithmic aspects such as encryption and hashing techniques. While these concepts rarely change, these skills alone are insufficient to protect computer networks. As crackers hacked away at networks and systems, courses arose that emphasized the latest attacks. Currently, many educators believe that to train people to secure networks, they must also learn to think like a cracker. The following background information in security helps in making correct decisions: Attack Recognition, Encryption techniques, Network Security Architecture, Protocol analysis, Access control list and vulnerability. For Network security cryptography is present. In cryptography data that can be read and understood without any special measures is called plaintext or clear text. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called cipher text. We use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting cipher text to its original plain text is called decryption. In cryptography three types of algorithms are present. Symmetric key algorithm, asymmetric key algorithm and hash function.

Cryptography is an important and vital application in security, defense, medical, business and many other application areas. The effective measure of a cryptosystem is how long it can be used to encrypt and decrypt messages without the 'key' being broken using cellular automata (CA) rules. A class of cellular automata (CA) based encryption algorithms presents a particular promising approach to cryptography, since the initial state of the CA is the key to the encryption, evolving a complex chaotic system from this 'initial state' which cannot be predicted. The remainder of the paper is organized as follows. Section II introduces the concept of Boolean functions and cellular automata. In Section III, we discuss some works of cryptography applied to one dimensional and two dimensional cellular automata. Section IV, Section V and Section VI describe our new encryption and decryption algorithm by using cellular automata rules.

II. DES

DES relies upon the encryption techniques of confusion and diffusion. Confusion is accomplished through substitution. Specially chosen sections of data are substituted for corresponding sections from the original data. The choice of the substituted data is based upon the key and the original plaintext. Diffusion is accomplished through permutation. The data is permuted by rearranging the order of the

various sections. These permutations, like the substitutions, are based upon the key and the original plaintext. The substitutions and permutations are specified by the DES algorithm. Chosen sections of the key and the data are manipulated mathematically and then used as the input to a look-up table. In DES these tables are called the S-boxes and the P-boxes, for the substitution tables and the permutation tables, respectively. Usually the S- and P-boxes are combined so that the substitution and following permutation for each round can be done with a single lookup. In order to calculate the inputs to the Sand P-box arrays, portions of the data are XORed with portions of the key. One of the 32-bit halves of the 64-bit data and the 56-bit key are used. Because the key is longer than the data half, the 32-bit data half is sent through an expansion permutation which rearranges its bits, repeating certain bits, to form a 48-bit product. Similarly the 56-bit key undergoes a compression permutation which rearranges its bits, discarding certain bits, to form a 48-bit product. The Sand Pbox look-ups and the calculations upon the key and data which generate the inputs to these table look-ups constitute a single round of DES.

2.1 Des system

Virtually all conventional block encryption algorithms, including DES have a structure first described by Horst Feistel of IBM in 1973 & shown in Figure1. There are 16 identical stages of processing, termed rounds. There is also an initial and final permutation, termed IP and IP^{-1}.Before the main rounds, the block is divided into two 32-bit halves and processed alternately; this criss-crossing is known as the Feistel scheme.

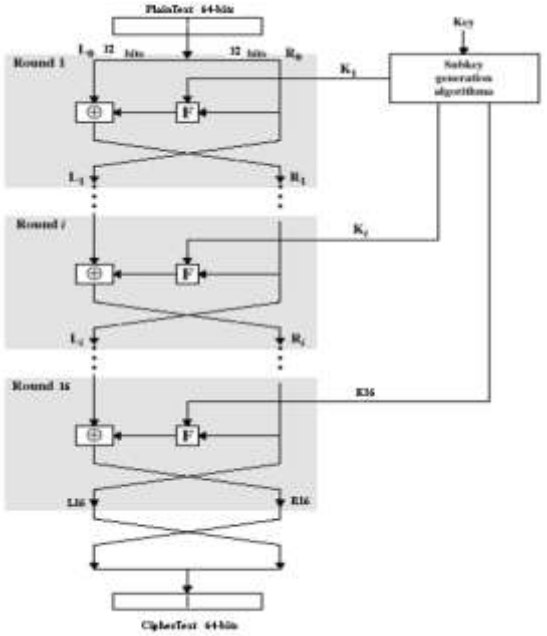

Figure 1: The overall Feistel structure of DES

The Feistel structure ensures that decryption and encryption are very similar processes -the only difference is that the sub keys are applied in the reverse order when decrypting. The rest of the algorithm is identical. This greatly simplifies implementation, particularly in hardware, as there is no need for separate encryption and decryption algorithms. The ⊕ symbol denotes the exclusive-OR (XOR) operation. The F-function scrambles half a block together with some of the key. The output from the F-function is then combined with the other half of the block, and the halves are swapped before the next round. After the final round, the halves are not swapped; this is a feature of the Feistel structure which makes encryption and decryption similar processes.

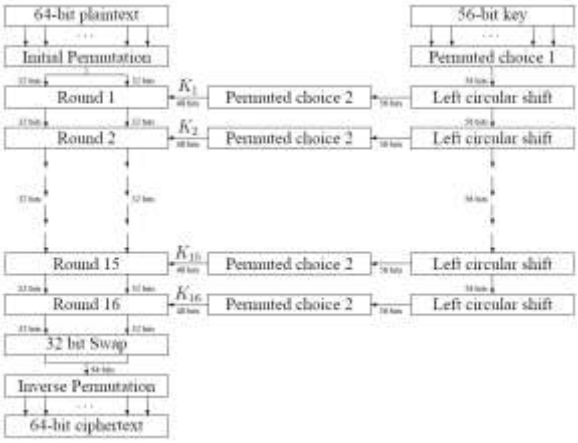

Figure 2: Flow Diagram of DES algorithm

Figure 2 shows the sequence of events that occur during an encryption operation. DES performs an initial permutation on the entire 64 bit block of data. It is then split into 2, 32 bit sub-blocks, Li and Ri which are then passed into what is known as a round (see figure 2.3), of which there are 16 (the subscript i in Li and Ri indicates the current round). Each of the rounds is identical and the effects of increasing their number are twofold - the algorithms security is increased and its temporal efficiency decreased. Clearly these are two conflicting outcomes and a compromise must be made. For DES the number chosen was 16, probably to guarantee the elimination of any correlation between the ciphertext and either the plaintext or key6. At the end of the 16th round, the 32 bit Li and Ri output quantities are swapped to create what is known as the pre-output. This [R16, L16] concatenation is permuted using a function which is the exact inverse of the initial permutation. The output of this final permutation is the 64 bit ciphertext.

III. DES Algorithm

Table 3.1: Algorithm

The Input
T: 64 bits of clear text
k1, K2,..., k16: 16 round keys
IP: Initial permutation
FP: Final permutation
f(): Round function
Output
C: 64 bits of cipher text
Algorithm
T' = IP(T), applying initial permutation
(L0, R0) = T', dividing T' into two 32-bit parts
(L1, R1) = (R0, L0 ^ f(R0, k1))
(L2, R2) = (R1, L1 ^ f(R1, k2))
.....
C' = (R16, L16), swapping the two parts
C = FP(C'), applying final permutation

IV. Features of DES

Table 1: Features of DES

Speed	high
Deposit of keys	needed
Country independence	no
Trojan Horse	not proved
Data block length	64 bits minimum
Key length	56 bits minimum
Use of data space	full, 64 bits (2^64), 8 bytes
Ciphering & deciphering key	same
Ciphering & deciphering algorithm	different

V. Applications of DES

Cryptographic services are required across variety of platforms in a wide range of applications such as secure access to private networks, electronic commerce and health care. The security of conventional encryptions depends on several factors. DES can be used in intensive cryptographic computer application. Applications such as electronic commerce, internet banking sand electronic fund transfer, secure and private communication require better performance cryptographic system.

Data encryption (cryptography) is utilized in various applications and environments. The specific utilization of encryption and the implementation of the DES and TDEA will be based on many factors particular to the computer system and its associated components. In general, cryptography is used to protect data while it is being communicated between two points or while it is stored in a medium vulnerable to physical theft. Communication security provides protection to data by enciphering it at the transmitting point and deciphering it at the receiving point.

File security provides protection to data by enciphering it when it is recorded on a storage medium and deciphering it when it is read back from the storage medium. In the first case, the key must be available at the transmitter and receiver simultaneously during communication. In the second case, the key must be maintained and accessible for the duration of the storage period.

VI. CONCLUSION

This paper presents an overview of DES algorithms, which is used in cryptography for Network security purpose. As we toward a society where automated information resources are increased and cryptography will continue to increase in importance as a security mechanism. Electronic networks for banking, shopping, inventory control, benefit and service delivery, information storage and retrieval, distributed processing, and government applications will need improved methods for access control and data security. The information security can be easily achieved by using Cryptography technique. DES is now considered to be insecure for some applications like banking system. There are also some analytical results which demonstrate theoretical weaknesses in the cipher. So it becomes very important to augment this algorithm by adding new levels of security to make it applicable.

REFERENCES

[1] Data Encryption Standard, Federal Information Processing Standards Publication (FIPS PUB) 46, National Bureau of Standards, Washington, DC (1977).

[2] Eli Biham, Adi Shamir (1993), "Differential Cryptanalysis of the Full 16-Round DES, Advances in Cryptology", proceedings of CRYPTO '92, Lecture Notes in Computer Science740, Springer.

[3] Cryptography & Network Security by William Stallings.

[4] The complete reference Java 2 (Fifth Edition) by Herbert Schildt. Security in computing (Fourth Edition) by Charles P.Pfleeger, Deven N.Shah.

[5] Network Security Essentials by William Stallings.

[6] Gunjan Gupta, Rama Chawla, "Review on Encryption Ciphers of Cryptography in Network Security," proceedings of International Journal of Advanced Research in Computer Science and Software Engineering.

[7] U.Ratna Kumari, T.K.Rasagna, "Implementation of Pipelined Data Encryption Standards for Security Enhancement through Verilog," proceedings of International Journal of Computer Applications and Technology.
[8] Teo Pock Cheung," Implementation of Pipelined Data Encryption Standards (DES) Using Altera CPLD" in Proc. IEEE Trans circuits systs vol.74.no.13, 1759-1763, 2007.
[9] Computer Network (Andrew S. Tanenbaum).
[10] Ahmed Zure Sha'meri, "DES Cryptographic System for Information Security" in Proc. IEEE Trans circuits syst vol.53, no 11, 1165-1169, 2002.