Data Encryption Standard

Sufiya S Kazi[1] Gayatri Bajantri[2]
[1]PG Student [2]Professor
[1,2]Department of Computer Science & Engineering
[1,2]SIET, Vijaypur, KA, India

Abstract— The Data Encryption Standard (DES) was developed by an IBM team in the year around 1974 and it was adopted as a national standard in the year 1977.From that time, many cryptanalysts have tried in order to find different shortcuts for the breaking of the system. In this paper, the examination of one such attempt, the method of differential cryptanalysis, which were published by Biham and Shamir. There are some of the safeguards against differential cryptanalysis that were built into the system from the beginning, with the result that more than 1015 bytes of the chosen plaintext are required for this attack to succeed. Cryptography plays very important role in security of data. Cryptography means to transfer sensitive information across insecure networks like internet so that it cannot be read by anyone except the person whom we want to send it. It basically hides the information. The federal organization used the Data Encryption Standard (DES) which may be used to protect sensitive data. Cryptography algorithms are divided into Symmetric and Asymmetric key cryptography. Symmetric Cryptography is further divided into Block ciphers and Stream Ciphers.

Key words: Data Encryption Standard (DES), Cryptography, Symmetric, Plaintext

I. INTRODUCTION

Cryptography is a method of storing and transmitting data in a form that only those it is intended for can read and process. It is a science of protecting information by encoding it into an unreadable format. It is an effective way of protecting sensitive information as it is stored on media or transmitted through network communication paths. Cryptography has two main types symmetric or secret key cryptography and asymmetric or public key cryptography. Symmetric key cryptography is the oldest type whereas asymmetric cryptography is only being used publicly since the late 1970's1.[1] DES was developed as a standard for communications and data protection by an IBM research team, in response to a public request for proposals by the NBS - the National Bureau of Standards (which is now known as NIST).

Asymmetric cryptography was a major milestone in the search for a perfect encryption scheme. Secret key cryptography goes back to at least Egyptian times and is of concern here. It involves the use of only one key which is used for both encryption and decryption (hence the use of the term symmetric). Figure 1.1 depicts this idea of two types of encryption. It is necessary for security purposes that the secret key never be revealed.

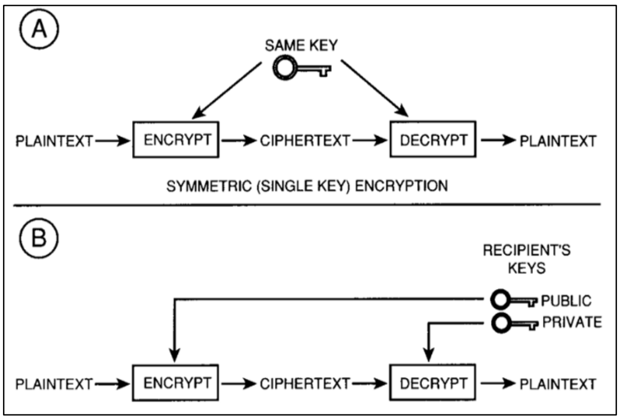

Fig. 1.1: Types of encryption

II. PROBLEM DEFINITION

A. Existing System

In the existing system, the encrypted key is send with the document. If the key is send with document, any user can view the encrypted document with that key. It means the security provided for the encryption is not handled properly. And also the Key byte (encrypted key) generate with random byte. Without the user interaction the Key byte is generated.

Drawbacks

Some of the drawbacks are:

1) Lack of security
2) Key byte is generated without user interaction

Problems in the Existing System:

- They require large data size.
- The existing system will take long computational time.
- They need high computing power.
- Not efficient for networking Systems.

B. Proposed System

To overcome all the problems in the existing system, we develop an "Encryption -Secure Communication Using Public Key and symmetric key" to ease the operation.

A system is required which is being capable of elimination all the problems and become useful to users and thus the new system is derived. Here, User can set the byte of key manually.

1) Benefits:

1) Security is enhanced in well manner.
2) Users set the byte key manually.

Data Encryption Standard or DES for short is a symmetric block cipher. It takes 64-bit plain text and 56 bit key as input and produces 64-bit cipher text as input.

Now, let's take a look at the advantages and disadvantages of DES.

2) Advantages:

1) For encryption, DES uses the 56-bit key. Besides, there are 256 possible keys, which means a brute force attack will never have any impact.

2) Cryptanalyst is free to perform cryptanalysis, so as to exploit the Des algorithm. However, have found it extremely hard to find any major weakness.

III. Literature survey

A. Bo Yang Dept. of Electr. & Comput. Eng., Polytech. Univ. Brooklyn, NY, USA. "Scan based side channel attack on dedicated hardware implementations of Data Encryption Standard"-2004

Cryptographic algorithms are implemented as application-specific integrated circuits (ASICs) or as cryptographic coprocessors to meet high throughput requirements. Scan-based test is the most powerful and largely used design for test (DFT) technique for testability improvement in sequential circuits at fabrication time and in field. It provides high fault coverage and do not need hardware for test pattern generation and signature analysis.

B. IBM Research Division, Thomas J. Watson Research Center, P. O. Box 218, Yorktown Heights, New York 10598, USA " The Data Encryption Standard (DES) and its strength against attacks"-1994

The Data Encryption Standard (DES) was developed by an IBM team around 1974 and adopted as a national standard in 1977. Since that time, many cryptanalysts have attempted to find shortcuts for breaking the system. In this paper, we examine one such attempt, the method of differential cryptanalysis, published by Biham and Shamir. We show some of the safeguards against differential cryptanalysis that were built into the system from the beginning, with the result that more than 10^{15} bytes of chosen plaintext are required for this attack to succeed.

C. Mitsuru Matsui" *The First Experimental Cryptanalysis of the Data Encryption Standard" -2001.*

This paper describes an improved version of linear cryptanalysis and its application to the first successful computer experiment in breaking the full 16-round DES. The scenario is a known-plaintext attack based on two new linear approximate equations, each of which provides candidates for 13 secret key bits with negligible memory. Moreover, reliability of the key candidates is taken into consideration, which increases the success rate. As a result, the full 16-round DES is breakable with high success probability if $2^{4.3}$ random plaintexts and their ciphertexts are available.

The author carried out the first experimental attack using twelve computers to confirm this: he finally reached all of the 56 secret key bits in fifty days, out of which forty days were spent for generating plaintexts and their ciphertexts and only ten days were spent for the actual key search.

*D. M.E. Smid NBS, Gaithersburg, MD, USA, D.K. Branstad NBS, Gaithersburg, MD, USA. "*Data Encryption Standard: past and future"-1998

The authors examine the past and future of the Data Encryption Standard (DES), which is the first, and to the present date, only, publicly available cryptographic algorithm that has been endorsed by the US government of the standard during the early 1970s, the controversy regarding the proposed standard during the mid-1970s, the growing acceptance and use of the standard in the 1980s, and some recent developments that could affect its future.

*E. R. Davis Secretary of Defence for Research and Engineering. "*The data encryption standard in perspective"-1978

The Data Encryption Standard (DES) was approved as a Federal Information Processing Standard (FIPS) by the Secretary of Commerce on November 23, 1976. This Standard was developed as a part of the Computer Security Program within the Institute for Computer Sciences and Technology at the National Bureau of Standards (NBS). This paper places this standard in perspective with other computer security measures that can and should be applied to Federal computer systems either before or coincident to using the Data Encryption Standard. In 1972, NBS initiated the standards development effort leading to adoption of the DES. During this period, NBS solicited for algorithms and information upon which a standard could be based, published for comment the algorithm which best satisfied the requirements of an encryption standard, and coordinated the effort with both the potential using communities and supplying communities. This paper outlines the environment surrounding and the history of the Data Encryption Standard and discusses the objectives of additional standards to be developed within the computer security program.

F. Poonam Garg *(Institute of Management Technology, India). "A Comparison between Memetic algorithm and Genetic algorithm for the cryptanalysis of Simplified Data Encryption Standard algorithm"-2010*

Genetic algorithms are a population-based Meta heuristics. They have been successfully applied to many optimization problems. However, premature convergence is an inherent characteristic of such classical genetic algorithms that makes them incapable of searching numerous solutions of the problem domain. A memetic algorithm is an extension of the traditional genetic algorithm. It uses a local search technique to reduce the likelihood of the premature convergence. The cryptanalysis of simplified data encryption standard can be formulated as NP-Hard combinatorial problem. In this paper, a comparison between memetic algorithm and genetic algorithm were made in order to investigate the performance for the cryptanalysis on simplified data encryption standard problems (SDES). The methods were tested and various experimental results show that memetic algorithm performs better than the genetic algorithms for such type of NP-Hard combinatorial problem. This paper represents our first effort toward efficient memetic algorithm for the cryptanalysis of SDES.

G. Donald W. Davies National Physical LaboratoryTeddington, MiddlesexUK Conference. Paper. "Some Regular Properties of the 'Data Encryption Standard' Algorithm".-1983

A cipher function y = E(k,x) should appear to be a random function of both the key k and the plaintext x. Any regular behaviour is of interest to the users. In the extreme case regular properties might point to a weakness of the cipher. Precautions are needed in the use of a cipher that has regular features. This note describes five regular properties of the

‘Data Encryption Standard’ or DES, two of which have been described elsewhere, are included for completeness.

H. W. Diffie Stanford University. “Special Feature Exhaustive Cryptanalysis of the NBS Data Encryption Standard”-1997

For centuries, cryptography has been a valuable asset of the military and diplomatic communities. Indeed, it is so valuable that its practice has usually been shrouded in secrecy and mystery.

I. Edward Department of Mathematics, Santa Clara University, Santa Clara CA 95053 USA. eschaefer@scuacc.scu.edu. “A SIMPLIFIED DATA ENCRYPTION STANDARD ALGORITHM” *Published online: 04 Jun 2010.*

In this paper we describe a method of teaching the Data Encryption Standard algorithm in an undergraduate cryptology course. We present a simplified version of the Data Encryption Standard algorithm with all parameters reduced as much as possible. This makes the inner workings of the algorithm accessible to undergraduates. Once the simplified algorithm has been explained to a class, it is easier to explain the real one. We suggest class discussions and homework based on this simplified algorithm.

J. A. Ram Kumar1, Shaik Mubeena2, V. Surendra Babu3. “Implementation of Triple Data Encryption Standard Architecture”-2017

Cryptography plays very important role in security of data. Cryptography means to transfer sensitive information across insecure networks like internet so that it cannot be read by anyone except the person whom we want to send it. It basically hides the information. The federal organization used the Data Encryption Standard (DES) and the Triple Data Encryption Algorithm (TDEA), which may be used to protect sensitive data. Cryptography algorithms are divided into Symmetric and Asymmetric key cryptography.

IV. AIMS AND OBJECTIVES

In the proposed project Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

The use of encryption/decryption is as old as the art of communication. In wartime, a cipher, often incorrectly called a "code," can be employed to keep the enemy from obtaining the contents of transmissions. (Technically, a code is a means of representing a signal without the intent of keeping it secret; examples are Morse code and ASCII.) Simple ciphers include the substitution of letters for numbers, the rotation of letters in the alphabet, and the "scrambling" of voice signals by inverting the sideband frequencies. More complex ciphers work according to sophisticated computer a algorithm that rearranges the data bits in digital signals.

In order to easily recover the contents of an encrypted signal, the correct decryption key is required. The key is an algorithm that "undoes" the work of the encryption algorithm. Alternatively, a computer can be used in an attempt to "break" the cipher. The more complex the encryption algorithm, the more difficult it becomes to eavesdrop on the communications without access to the key.

Encryption/decryption is especially important in wireless communications. This is because wireless circuits are easier to "tap" than their hard-wired counterparts. Nevertheless, encryption/decryption is a good idea when carrying out any kind of sensitive transaction, such as a credit-card purchase online, or the discussion of a company secret between different departments in the organization. The stronger the cipher – that is, the harder it is for unauthorized people to break it – the better, in general. However, as the strength of encryption/decryption increases, so does the cost.

V. HARDWARE AND SOFTWARE DESIGN

A. Hardware Specification

Processor: Any Processor above 500 Mhz.
Ram: 128Mb.
Hard Disk: 10 Gb.
Compact Disk: 650 Mb.
Input device: Standard Keyboard and Mouse.
Output device: Encrypted and decrypted data.

B. Software Specification

Operating System: Windows 2000 server Family.
Techniques: JDK 1.5
Software: Net Beans IDE 8.0.2.

VI. METHODOLOGY

The Data Encryption standard is used to protect electronic data. DES algorithm uses symmetric block cipher for encrypting and decrypting data. Encryption converts data into gibberish language called cipher text.

Decrypting the cipher text gives us back the original data that is plaintext. Converting the information from ciphertext to plaintext, we use a standard form of algorithm called Symmetric algorithm.

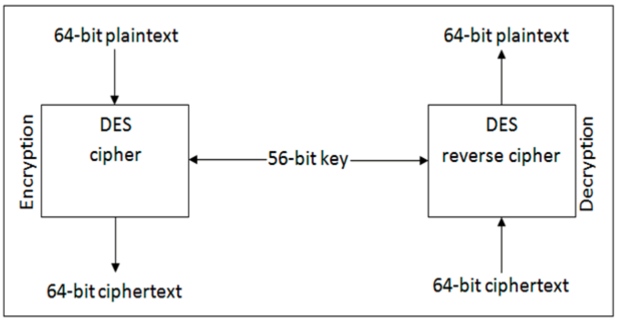

Fig. 6.1: Encryption and Decryption with DES

DES takes an input of 64-bits and the output is also of the same size. As shown in above figure 1, the process requires a second input, which is a secret key with length of 64-bits, every eighth bit is used as parity checking bit. Therefore, 56-bits take part in the algorithm to encrypt data. Block cipher algorithm is used where message is divided into blocks of bits. Block cipher is used for encryption and decryption. These blocks of bits are put through substitution, permutation, and other different mathematical functions

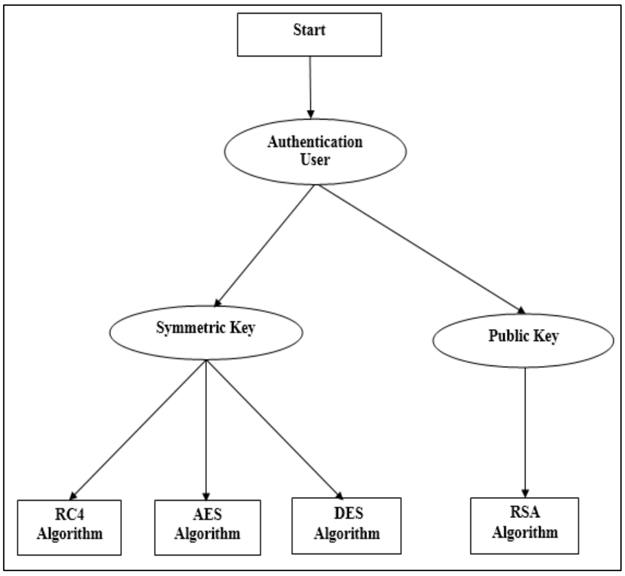

Fig. 6.2: Flow of algorithm

VII. CONCLUSION

The concept of cryptography long with encryption and decryption is explained. DES has 16 rounds of operation. The plaintext is taken to 16 rounds of operation, which produces a cipher text (final output). With DES, it will encryptionand decryption the block and a completely different output is generated with a final combination. As with most encryption schemes, DES expects two inputs - the plaintext to be encrypted and the secret key. The manner in which the plaintext is accepted, and the key arrangement used for encryption and decryption, both determine the type of cipher it is. DES is therefore a symmetric, 64 bit block cipher as it uses the same key for both encryption and decryption and only operates on 64 bit blocks of data at a time5 (be they plaintext or cipher text).

REFERENCES

[1] Bo Yang Dept. of Electr. & Comput. Eng., Polytech. Univ. Brooklyn, NY, USA. “Scan based side channel attack on dedicated hardware implementations of Data Encryption Standard”-2004

[2] IBM Research Division, Thomas J. Watson Research Center, P. O. Box 218, Yorktown Heights, New York 10598, USA “ The Data Encryption Standard (DES) and its strength against attacks”-1994

[3] Mitsuru Matsui” The First Experimental Cryptanalysis of the Data Encryption Standard” -2001

[4] M.E. Smid NBS, Gaithersburg, MD, USA, D.K. Branstad NBS, Gaithersburg, MD, USA. “Data Encryption Standard: past and future”-1998

[5] R. Davis Secretary of Defence for Research and Engineering. “The data encryption standard in perspective”-1978.

[6] Poonam Garg (Institute of Management Technology, India). “A Comparison between Memetic algorithm and Genetic algorithm for the cryptanalysis of Simplified Data Encryption Standard algorithm”-2010

[7] Donald W. Davies National Physical LaboratoryTeddington, MiddlesexUK Conference. Paper. “Some Regular Properties of the ‘Data Encryption Standard’ Algorithm”.-1983

[8] W. Diffie Stanford University. “Special Feature Exhaustive Cryptanalysis of the NBS Data Encryption Standard”-1997.

[9] Edward Department of Mathematics, Santa Clara University, Santa Clara CA 95053 USA. eschaefer@scuacc.scu.edu. “A SIMPLIFIED DATA ENCRYPTION STANDARD ALGORITHM” Published online: 04 Jun 2010.

[10] Ram Kumar1, Shaik Mubeena2, V. Surendra Babu3. “Implementation of Triple Data Encryption Standard Architecture”-2017