ISSN: 2456-6616 (Online)

Design and Implementation of Improved Data Encryption Standard

Shipra Ravi kumar[1], Suman Avdhesh Yadav[2], Akanksha Singh[3]
[1]Department of Computer Science and Engineering JSS Academy of Technical Education Noida
[2]Department of Computer Science and Engineering, AUGN Greater Noida,
[3]Department of Electronics and Communication Engineering, AUGN Greater Noida
[1]shipra.chaudhary85@gmail.com, [2]suman.avdheshyadav@gmail.com, [3]akankshasingh5614@gmail.com

Abstract:
DES is a strong encryption standard that operates on a 64-bits plaintext block and returns a 64-bits ciphertext. Thus, DES results in a permutation among the 2^{64} possible arrangements of 64 bits, each of which may be either 0 or 1. In this paper we prosposed improved security by modifying the key criteria and algorithmic steps of the DES algorithm. Key genaration system generates two keys one is simple and other one is encrypted. The encryption algorithm in first round uses simple key1 and from round 2 to round 15, the algorithm uses encryted key2. At last, in round 16 the simple key1 is again used and secured ciphertext is obtained. This increases vulnerability and improves DES encrytion security. Finally, Differential cryptanalysis can’t be performed on ciphertext.

Keywords: DES (data encryption standard), S-Box (substitution Box), P-Box (Permutation Box), TDES (Triple data encryption standard)

1. Introduction

Cryptography is the process of transforming plain text or original information into an unintelligible form (cipher text) so that it may be sent over unsafe channels or communications. The transformer process is controlled by a data string (key). Anyone getting hold of the cipher text while it is on the unsafe channel would need to have the appropriate key to be able to get to the original information. The authorized receiver is assumed to have that key.

The main mechanism is encryption and decryption that guide the flow of data. Cryptography has two modes of encryption known as public key and secret key. The shared between two parties is actually the secret information which needs to be transferred over the network. The use of secret key is sometimes known as symmetric key and that of an asymmetric key is known as public key. In asymmetric transformation the private or secret key is used to transform the original data into ciphered form, then at the other end the public key is used to convert the data into decrypted data again [1]. The public key provides slow data transformation and it is suitable to be used for converting small amount of data.The main goals of using cryptography are authentication, integrity, confidentiality, non-repudiation and availability [2] [3].

Modern cryptography concerns itself with the following four objectives:

a) *Confidentiality*: The information cannot be understood by anyone for whom it was unintended).
b) *Integrity*: The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected).
c) *Non-repudiation*: The creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information).
d) *Authentication*: The sender and receiver can confirm each other’s identity and the origin/destination of the information).

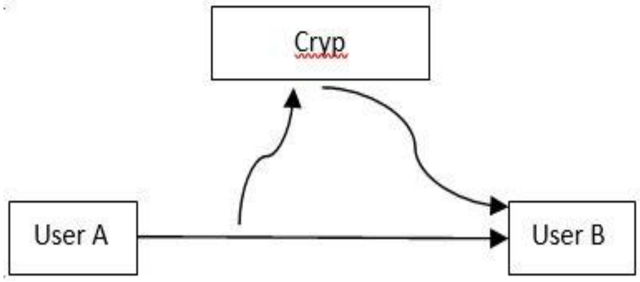

Fig. 1. A cryptanalyst captures the messages from A to B from the communication network

A. *Types of Attacks*

1. Passive attacks:
Which attempt to learn or make use of information from the system but does not affect system resources presented in figure 1 [4].

a. Release of message contents: A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information.

b. Traffic Analysis: In this attack the eavesdropper analyzes the traffic, determines the location, identifies communicating hosts, observes the frequency and length of message being exchanged. Using all this information they predict the nature of communication. All incoming and outgoing traffic of network is analyzed but not altered.

2. Active attacks:

Which attempt to alter system resources or affect their operation is shown in figure 2 [5].

a. Masquerade: In terms of communications security issues, a masquerade is a type of attack where the attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen logon IDs and passwords, through finding security gaps in programs, or through by passing the authentication mechanism. The attempt may come from within an organization

b. Replay: Replay is repetitive transmission of same message producing an unauthorized effect at receiving end.

c. Modification of messages: Some segments of the original message are altered or delayed or shuffled, to produce an unauthorized effect. For e.g. a message meaning *"permit Jack to access the confidential accounts"* is modified as *"permit Daniel to access the confidential accounts"*.

d. Denial of Services: It prevents or inhibits the normal use or managements of communications facilities. This attack may have specific target; for example, an entity may suppress all messages directed to a particular destination and shown in figure 2. Another service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

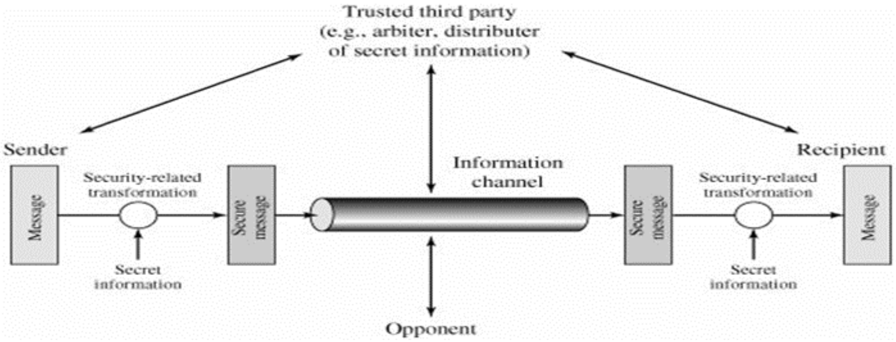

Fig. 2. Model for network Security

B. Cryptanalysis

This means capturing encrypted data and trying to decrypt it when key is not available by any means. It can be utilized to break codes by finding weaknesses in the cryptographic scheme. In addition to being used by hackers with bad intentions, this discipline is also often used by the military [6]. It is also appropriately used by designers of encryption systems to find, and subsequently correct, any weaknesses that may exist in the system under design.

The objective of the cryptanalysis is to obtain the secret key so that all cipher text can be deciphered without the knowledge of underlying algorithm. A brute-force attack is a fine example. In brute force, the cryptanalyst hits every possible combination of keys until the original one is obtained. Long keys like, 128-bit keys, is assumed to be strong, and attack resistant.

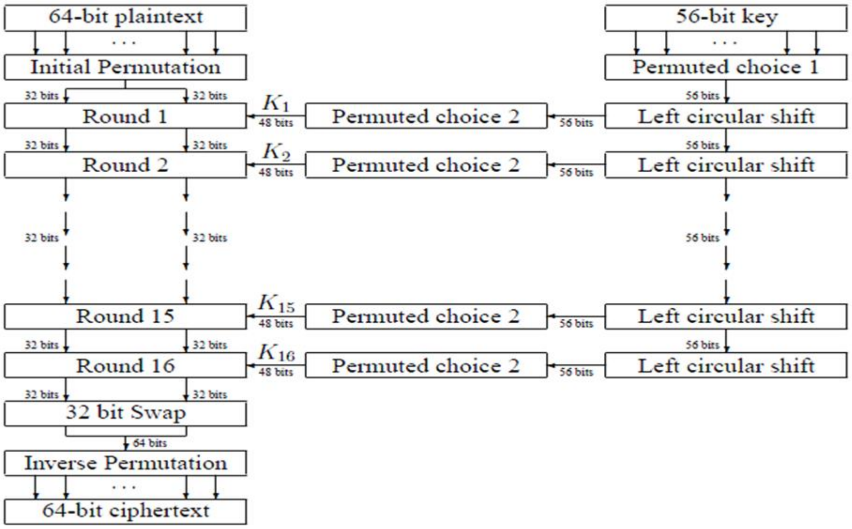

Fig. 3. Working structure of Data Encryption Standard

C. Data Encryption Standard (DES)

The Data Encryption Standards (DES) algorithm was developed by IBM in the early 1970s. 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 time (be they plaintext or cipher text) as shown in figure 3.

Actual input is 64-bits, but we actually use a key of size 56-bits. The least significant bit of each byte is either used for parity (odd for DES) or set arbitrarily and does not increase the security in any way. We sequence the blocks from left to right which makes the eighth bit of each byte the parity bit. Because 256 combinations of the keying variable are possible (and these keying variables can be changed readily), the algorithm is deemed by some experts to be highly secure [7] [8].

The two main components of the DES-based system are an algorithm and a key. The DES algorithm is a complex interactive process comprised of substitutions, permutations, and mathematical operations. The key feature of DES is that the algorithms is fixed and is public information.

However, the actual key used is shared secret between the originator and the receiver of a transmission. Advances in DES include lengthening a key to 128 bits and the multi-pass DES which involves several passes usually three of encryption and decryption using different keys.

2. Related Work

William Mehuron & Raymond G. Kammer, in their paper entitled "Data Encryption Standard". The selective application of technological and related procedural safeguards is an important responsibility of every Federal organization in providing adequate security to its electronic data systems. This publication specifies two cryptographic algorithms, the Data Encryption Standard (DES) and the Triple Data Encryption Algorithm (TDEA) which may be used by Federal organizations to protect sensitive data. Protection of data during transmission or while in storage may be necessary to maintain the confidentiality and integrity of the information represented by the data. The algorithms uniquely define the mathematical steps required to transform data into a cryptographic cipher and also to transform the cipher back to the original form. The Data Encryption Standard is being made available for use by Federal agencies within the context of a total security program consisting of physical security procedures, good information management practices, and computer system/network access controls. This revision supersedes FIPS 46-2 in its entirety.

Eric Conrad in his paper entitled "Data Encryption Standard" proposed although there is no silver bullet when it comes to network security, cryptography can play a key role in protecting critical information. There are three general types of cryptography: symmetric, asymmetric, and hash. This paper focused on one of the key symmetric key algorithms: DES

3. Factors Which Affect the Security of DES

A. Weak Keys:

Because of the way the initial key is modified to get a sub key for each round of the algorithm, certain initial keys are weak keys. The initial keys value is split into two halves and each half is shifted independently. If all the bits in each half are either 0 or 1, then the key used for any cycle of the algorithm is the same for all the cycles of the algorithm. This can occur if the key is entirely 1s, entirely 0s, or if one half of the key is entirely 1s and the other half is entirely 0s. So that makes DES less secure [9].

B. Algebraic Structure:

The DES encryption operation would form a group and encrypting a set of plaintext blocks with k_1 followed by k_2 would be identical to encrypting the blocks with k_3. Even worse, DES would be vulnerable to a meet-in-the-middle known-plaintext attack that runs in only 2^{28} steps [10]. If DES were closed, then for any k_1 and k_2 there would be a k_3 such that

$$E_{k2}(E_{k1}(P)) = E_{k3}(P)$$

C. Key Length:

There is a possibility to speep up the searching process by time-space tradeoff. The possibility of computing and storing 2^{56} possible results of encrypting a single plaintext block under every possible key, Then to break an unknown key, we need to insert data blocks into the encryption stream, recover the resulting cipher text and look the key up [11].

No. of Rounds: No of rounds kept 16 because reduced number of rounds has been successfully attacked. DES with three or four rounds was easily broken. DES with any number of rounds fewer than 16 could be broken with a known plaintext attack more efficiently then by a brute-force attack.

4. Attacks on DES:

4.1 Differential Cryptanalysis:

Its main application lies primarily with block ciphers, but it can also be used to decipher stream ciphers and cryptographic hash functions. In other words, it is the study effect of change in input to change in output. When dealing with block ciphers, differential cryptanalysis is a technique that traces differences through the network, discovering the non-random behavior of cipher and using this information to recover the secret key [12].

4.2 Related-Key Cryptanalysis:

Related-key cryptanalysis assumes that the attacker learns the encryption of certain plaintexts not only under the original (unknown) key K, but also under some derived keys K0 = f(K). In a chosen-related-key attack, the attacker specifies how the key is to be changed; known-related-key attacks are those where the key difference is known but cannot be chosen by the attacker. We emphasize that the attacker knows or chooses the relationship between keys, not the actual key values. Related-key cryptanalysis is a practical attack on key-exchange protocols that do not guarantee key-integrity an attacker may be able to flip bits in the key without knowing the keypad key-update protocols that update keys using a known function: e.g., K, K + 1, K + 2, etc. Related-key attacks were also used against rotor machines: operators sometimes set rotors incorrectly.

4.3 Linear Cryptanalysis:

Linear cryptanalysis is a general form of cryptanalysis based on finding affine approximations to the action of a cipher. Attacks have been developed for block ciphers and stream ciphers. Linear cryptanalysis is one of the two most widely used attacks on block ciphers; the other being differential cryptanalysis.

Linear approximate equations based on the best (n-2)-round expression, and reliability of the key candidates derived from these equations. The former reduces the number of required plaintexts, whereas the latter increases the success rate of our attack.

In the 247-method, we established two linear approximate equations of 16-round DES using the best 15-round expression, where each equation includes one active S-box and hence recovers 7 secret key bits. This paper, however, begins with two new linear approximate equations derived from the best 14-round expression, where each equation has two active S-boxes and can recover 13 secret key bits. These equations give us, therefore, a total of 26 secret key bits, and then the remaining 56 - 26 = 30 secret key bits are within the reach of an exhaustive search."

"As a result, DES is breakable with complexity 243 and success rate 85% if 243 known-plaintexts are available. For another example, success rate is 10% with complexity 250 if 238 known-plain texts are available.

4.4 Brute Force Attack

In cryptanalysis, a brute force attack is a method of defeating a cryptographic scheme by trying a large number of possibilities; for example, exhaustively working through all possible keys in order to decrypt a message.

The selection of an appropriate key length depends on the practical feasibility of performing a brute force attack. For symmetric-key ciphers, a brute force attack typically means a brute-force search of the key space; that is, testing all possible keys in order to recover the plaintext used to produce a particular cipher text. In a brute force attack, the expected number of trials before the correct key is found is equal to half the size of the key space. For example, if there are 264 possible keys, a brute force attack would, on average, be expected to find a key after 263 trials.

If keys are generated in a weak way, for example, derived from a guessable password, it is possible to exhaustively search over a much smaller set, for example, keys generated from passwords in a dictionary.

5. Proposed Solution

After reading the DES and attacks on it, it seems that a new approach should be developed to avoid this vulnerability. Following is provided a new concept and that's called two key concepts. As per our objective I made some changes into the structure of DES so that it can accept a bigger key and resist again the above said cryptanalyst attacks. This concept will work on two 64 –bits keys instead of one 64-bits key ,now the effected key will be of 112 bits length and it will be work fine against the brute force attack ,linear and related key cryptanalysis, but for the differential , we have to work more .So I changed the way keys were shifted and merging.

5.1. The Block Diagram of Two Key Concepts

The two keys were taken up and with the first key the second key encrypted by using a simple XOR operation shown in figure 4.

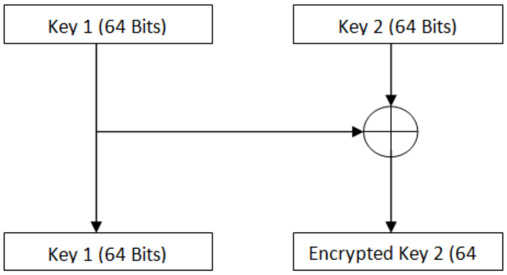

Fig. 4. Representation of new approach with Two Key

The next thing was to some modification in key accepting block diagram of DES, shown in figure 5.

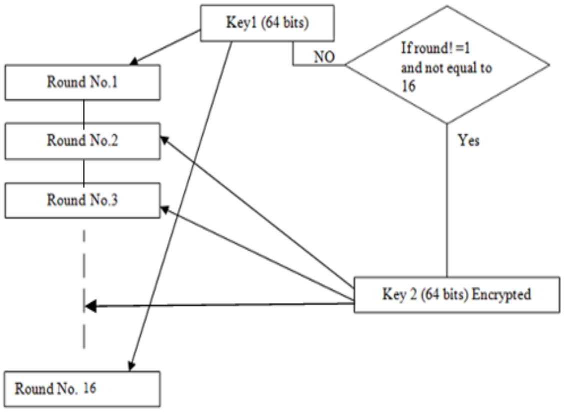

Fig. 5. Working of DES with Two key

5.2 Algorithmic Steps

Algorithmic behavior of the proposed system is presented with the steps under the given sub sections.

5.2.1 Encrypted key generation

```
Step1. Read 64-bit key 1.
Step 2. Read 64- bit key 2.
Step3. Key 1 XOR key 2.
Step4. Store new encrypted key 2 and key 1.
```

5.2.1. Proposed DES algorithm for security

```
Step1. Read 64-bit plain text and 64- bit key 1.
Step2. While (round!=15)
In each round perform permutations and substitutions
If round > 1
Then Use key 2 for round 2 to round 15
Exit
Step3. Use key 1 in round 16
Step4. Store cipher text as output.
```

6. Conclusion

As far as the key length is concern the above methodology gives a suitable solution because the DES will accept the 2 keys; work with the effective key length of 112 bits. As per as execution time is concern, it will be little bit slower than the DES because of the extra computation of the encrypted key and selecting the key for appropriate round. As security is concern, as we have seen that some cryptanalysis works on key and find the key from last round, but after this arrangement it will become difficult to get the key from that area and difference of two plaintext will not lead to a difference of cipher text, because the two keys are altering the plaintext.

REFERENCES

[1] http://csrc.nist.gov/publications/fips/fips46- 3/fips46-3.pdf

[2] http://www.giac.org/cissp-papers/62.pdf

[3] (http://math.scu.edu/~eschaefe/crylec.pdf)

[4] www.facweb.iitkgp.ernet.in/~sourav/DES.pdf

[5] “Cryptography and network security”, by William Stallings.

[6] 6.“Cryptography and network security”, by Behrouz A. Forouzan.

[7] www.itl.nist.gov/fipspubs/fip46-2.htm

[8] www.ee.ic.ac.uk/pcheung/.../ee3.../DES%20Implementation (702).pdf

[9] ieeexplore.ieee.org › ... › IBM Journal of Research

[10] 10.www.cs.au.dk/~carmit/compressing AES_journal_revision_1.pdf

[11] 11.www.cs.dartmouth.edu/cms_file/SYS_tech Report/.../TR88-138.pdf

[12] 12.www.academicjournals.org/ajmcsr/.../Kenekayoro%20Patrick.htm