I. INTRODUCTION

When we talk about security it is necessary that we know cryptography[1]. Today it is must to secure sensitive data transmitted over network or kept in storage from attackers[2].

Cryptography is a technique that provides mathematical steps to secure data [3]. Encryption word is attached with cryptography[4]. Encryption converts our sensitive data to unreadable form. Doing this we may be sure that no one can understand our data even it is leaked somehow. The form of data which is unreadable is called cipher text. Decryption is opposite to encryption. It converts unreadable data to readable data. Using encryption and decryption only intended parties can see the message.

According to [5] there are two types of cryptography:

✓ Classical cryptography: uses substitution and permutation to encrypt the message.
✓ Modern cryptography: uses various methods to encrypt the message.

Cryptography has following goals [6]:

✓ CONFIDENTIALITY: It is related to secrecy of message.

✓ INTEGRITY- Only authorized parties can alter the message not others.
✓ AUTHENTICATION: only those parties whose identification is checked and found correct can only access the data.
✓ NON-REPUDIATION: This service prevents the parties from denying their previous commitments.

As in [3] there are two types of cryptographic protocols:

✓ SYMMETRIC KEY: Same key is shared by both sender and receiver.
✓ ASYMMETRIC KEY: Sender and receiver have different keys, called public and private keys.

II. DATA ENCRYPTION STANDARD

In the context of symmetric cryptography DES (Data Encryption Standard) is widely used[2]. DES was developed by team of IBM in 1974[7]. It is published in United States National Bureau Of Standards in 1977[8]. DES is a block cipher, it takes 64 bits size block of data and encrypt it into
equal size cipher text. DES is based on XOR operation and left shift rotation. Along these operations permutation and substitution are also used. DES has three phase:

- **KEY GENERATION**: There is 64 bit key from which 16, 48 bits keys are derived. These keys are derived using key generation algorithm. 64 bits key is gone through a parity drop table, where parity bit of the characters is discarded and permutation is done. Now it becomes 56 bits key, it is divided into two halves (C₀, D₀) C₀ and D₀ are left shifted separately. Shifting for round 1, 2, 9 and 16 is one bits and two bits for rest. After shifting C₀ and D₀ becomes C₁ and D₁. These C₁ and D₁ are concatenated into C₁D₁ and then Permutation choice 2 is applied which yields 48 bits round key. This key is key1. For second round C₁ and D₁ are shifted then concatenated and permuted yielding key2 and C₂ and D₂. This process will be continued till round 16. At the end of round 16 we have 16, 48 bits keys. Which will be used later in encryption.

Encryption is performed on block of 64 bits[9]. After initial permutation this is divided into two halves L₀ and R₀, each of 32 bits. After that encryption is performed in following phases:

- **EXPANSION**: R is expanded 32 bits to 48 bits in every round.
- **XOR**: Expanded R and the key is XORed, yielding 48 bits.
- **SUBSTITUTION**: There are eight substitution boxes (s₁, s₂,...,s₈)[6]. Each box has four rows and sixteen columns. XORed 48 bits are divided into eight groups of six digits. Each group is passed through s-box(s₁, s₂,...,s₈). Every substitution box is like a matrix with rows and columns, first and last digits of a six bits group denote row of s-box and middle four bits denote column. After substitution we get four bits from each s-box, thus from eight s-boxes, 32 bits output comes.

Block diagram of the algorithm is given below

![Figure 1: Key generation process](image1)

**Figure 1: Key generation process**

**ENCRYPTION**: There are sixteen rounds of encryption. Sixteen keys(k₁,...,k₁₆) are used in sixteen round(R₁,...,R₁₆) respectively.

![Figure 2: Encryption Process](image2)
PERMUTATION: 32 bits are permuted according to a given array of permuted choice 2.

After permutation 32 bits are XORed with L. Result is become Right side (R) for next round, while old R side becomes new Left side(L). This process is repeated for sixteen rounds using the keys (k1...k16). After round 16, R_{16} and L_{16} are concatenated and then final permutation is done. Now result is 64 bits cipher text.

DECRYPTION: Decryption is reverse process of encryption[5]. Initial permutation is done on 64 bits cipher text. Then it is divided into two halves each of 32 bits (L_{16},R_{16}). Now same process of encryption is repeated from round 1 to round 16, using the key 1 to key 16. In decryption process keys are used in reverse order means key 16 will be used in round 1, key 15 in round 2, key 14 in round 3 and so on. Block diagram for decryption is given in figure 3.

III. LITERATURE REVIEW

In [5] DES is improved using random number generator. Here message is divided into 64 bits blocks and different keys are generated using 56 bits master key. Keys generation is done using random number generator. Keys generated from 56 bits master are also 56 bits. For every block of message bits different key will be used. In this approach although security is enhanced but time taken to finish the process will be long enough.

Authors in [12] changed the XOR operation in DES. They replaced the two state key (0,1) from 4 state key (0,1,2,3). XOR operation is replaced by new operation which uses two 4 states keys. This method provides security but increase complexity.

In [2] authors give a new method of key generation in DES. They used odd even substitution method for key generation. Odd even substitution is applied on 56 bits key at every step.

In [9] authors give a change to existing DES by using two keys, left key and right key. They used method of Blowfish algorithm to generate the keys. This algorithm is called fused DES_BLOW. However security is enhanced due to use of double key but complexity is also increased.
Authors in [10] give the idea of using DES three times with three different keys. This enhanced algorithm is called Triple DES. It became popular from 1978.Security is enhanced due to use of three keys. Problem with this is forty eight rounds for encryption of 64 bits, which is too much time consuming and makes the algorithm slower.

Authors in [11] has used different method of permutation called Simple Columnar Transposition Technique, they arranged plain text in columns to make it cipher text. This columnar transposition rounds may be one, two or three according to required security.

IV. IMPROVED DES

In improved DES key generation part is improved. Encryption and decryption are as usual. In key generation algorithm we have used two arrays of size eight. One is Left Random Array and another is Right Random Array. In these arrays eight values will be filled by a Random number generator, these values are between 0 to 27.

IMPLEMENTATION: Key generation algorithm is implemented in visual c# programming language, software tool is Microsoft Visual Studio 2010, operating system used is windows 10, processor is core i7, with 2.20 GHz frequency. RAM of the system is 8 GB.

Procedure of key generation using random number generator is following:

1. **Key generation Procedure** - We have 64 bits key. After using parity drop table we have 56 bits key. This 56 bits key is divided into two halves $C_0$ and $D_0$. Now using left random array, values in $C_0$, at positions given in random array is flipped.

Suppose the first value of left random array is 25 then 25th bit of $C_0$ is checked if it is zero then it is converted into one or vice versa. Using this eight positions of $C_0$ are flipped.

Now same procedure is repeated for $D_0$ with right random array, yielding $C_1$ and $D_1$.

After this, left shift is done of $C_1$ and $D_1$. Number of left shift for each round are as before in old DES. When left shift is completed $C_1$ and $D_1$ are concatenated and permuted choice 2 is applied which gives us 48 bits key. This is our first key.

Procedure for other rounds (2, 3, ..., 16) is same. For each round left and right array will be used.

At the end of round 16 we get our 16th key. Block diagram is given in Figure 4.

Example: Suppose we have 16 digits hexadecimal key $K=0123456789ABCDEF$ and two left and right random arrays given below:

**RIGHT RANDOM ARRAY**

| 9 | 2 | 3 | 21 | 25 | 15 | 11 | 11 |

**LEFT RANDOM ARRAY**

| 0 | 26 | 5 | 4 | 13 | 4 | 12 | 25 |

Using the random key generation algorithm sixteen keys are generated. Step by step procedure for key generation is given in TABLE III.

Using the random key generation algorithm sixteen keys are generated. Step by step procedure for key generation is given in TABLE III.
ENCRYPTION PROCESS: Method of encryption is the same as in old DES. Plain text is divided into 64 bits blocks[6]. Each block goes through 16 rounds of encryption at the end of 16th round we get cipher text. Encryption process is explained before in this paper. Here we encrypt the text using above 16 keys in figure 5. Encryption process for given example is given in TABLE IV.

Hexadecimal code is used for Cipher text and keys.

<table>
<thead>
<tr>
<th>Round</th>
<th>Encrypted Hex Code</th>
<th>Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00000000500640CB</td>
<td>09A26E575834</td>
</tr>
<tr>
<td>2</td>
<td>500640CB198BD081</td>
<td>F3069D09EBC6</td>
</tr>
<tr>
<td>3</td>
<td>198BD081EA877A92</td>
<td>C59AD5F1E6D0</td>
</tr>
<tr>
<td>4</td>
<td>8EA877A9201C9D115</td>
<td>8FFAB3BC484E</td>
</tr>
<tr>
<td>5</td>
<td>01C9D115D283BE43</td>
<td>2737AFC9F487</td>
</tr>
<tr>
<td>6</td>
<td>D283BE434B9DDDF6</td>
<td>631486B6E8</td>
</tr>
<tr>
<td>7</td>
<td>4BF9DDF65C40D1DF</td>
<td>C088B5EDDB4E</td>
</tr>
<tr>
<td>8</td>
<td>5C40D1DF0C1044AC</td>
<td>0DA277D1D4BF</td>
</tr>
<tr>
<td>9</td>
<td>0C1044AC642094DE</td>
<td>EB671D38DE1C</td>
</tr>
<tr>
<td>10</td>
<td>642094DE29ED765C</td>
<td>D59FDC1C76F3</td>
</tr>
<tr>
<td>11</td>
<td>29ED765CA7612BF9</td>
<td>CEFAB6FAE20</td>
</tr>
<tr>
<td>12</td>
<td>A7612BF96F91F034</td>
<td>26BF2BB06E1A</td>
</tr>
<tr>
<td>13</td>
<td>6F91F034159E61A4</td>
<td>733426BD3212</td>
</tr>
<tr>
<td>14</td>
<td>159E61A442CE77FE</td>
<td>708C95F06023</td>
</tr>
<tr>
<td>15</td>
<td>42CE77FE3ABA0050</td>
<td>CDA07363284F</td>
</tr>
<tr>
<td></td>
<td>3ABA00509A9B0115</td>
<td>CB437FE3A6D3</td>
</tr>
</tbody>
</table>

Table 3: Random Key Generation Procedure

Keys generated from above procedure are given in figure 5.
Table 5: Encryption In Every Round

| Cipher Text: 15F001F0F3A00270 |

DECRYPTION: Decryption process will be same as discussed in previous section. Round Keys are used in reverse order (k16,k15,.....k1).

V. CONCLUSION

Algorithm being used for encryption should be able to secure data and fast enough. DES is fast and popular but needs some improvements regarding its security. In this paper we have tried to improve key generation method of DES, using two random arrays of size eight. Randomness improve the security of algorithm. Every time when this improved key generation algorithm is run, different random arrays will be generated. Now attacker needs 56 bits key as well as two random arrays to generate sixteen keys. Although it is very difficult to find key and arrays yet Any how he knows both key and random arrays, values of random arrays will be changed at that time.

In future work, random arrays for each round may be different, means 32 random arrays for 16 rounds. Two random arrays for each round. Size of array can be enlarged to make it difficult to find.

ACKNOWLEDGMENT

I want to give my sincere thanks to Ms. Preeti Thakur, for her guidance throughout my research. Her deep knowledge and diligence helped me a lot.

I also thanks my family and friends for their kind support. Thanks to everyone who helped me directly or indirectly.

REFERENCES


