Abstract: Steganography is the art of writing hidden messages in such a way that no one apart from sender and intended receiver suspects the existence of the message, a form of security through obscurity. It is an area which is used for secure data transmission over any public media. The present work focus on cryptography to secure the data while transmitting over network. Firstly, the data which is to be transmitted from sender to receiver in the network must be encrypted using the encryption algorithm. Secondly, decryption technique is used by the receiver to view the original data. In this paper, I present the performance of two encryption algorithms DES, RSA algorithm and as well as their comparison. Experimental results are given to analyses the effectiveness of each algorithm.

Keywords: DES, RSA, Cryptography.

1. INTRODUCTION

Information Security plays a pivotal role during internet communication in today’s era of technology. As the technology is upgrading day by day, people are getting more involved to their work and they have little time for the things which seen negligible at the starting but can be very dangerous in future. In today’s world 99% people are more interested in sending and receiving data through internet and mobile data storage devices. But among these 90% people donot encrypt their data though they know that the data contains personal information and the chances of data lose is very high. Sending data through internet has high chances of getting hacked. Because the number of hackers are increasing day by day and hackers can hack the unencrypted data from the internet. There are various cryptography methods that provide a means for secure communications and protecting passwords. Cryptography has many commercial uses and applications such as to allowing someone to order a product online without the fear of their credit card number is being intercepted, confidential company information.

Cryptography concerns itself with the four objectives:

1. Confidentiality: the information cannot be understood by anyone for whom it was unintended.
2. Integrity: the information cannot be altered in storage or transit between sender and intended receiver without alteration being detected.
3. Non-Repudiation: the creator or sender of the information cannot deny at the later stage his or her intentions in the creation or transmission of the information.
4. Authentication: the sender or receiver confirm each other’s identity and the origin or destination of the information.

2. ENCRYPTION AND DECRYPTION

Fig 1: Process of encryption and decryption
It is clear from the above fig.1 that:

1. A message being sent is called a plain text. Then the message is coded using cryptographic algorithm. This process is called Encryption.
2. A Encrypted message is called ciphertext and is turned back to the plaintext by using the process of decryption. The send uses the encryption algorithm.
3. A key is supplied to the recipient so that they can then decipher the message. Keys for encryption algorithms are described in terms of the number of bits. The higher the number of bits the more difficult that cryptosystem would be to break.
4. To decrypt a message we need a decryption algorithm, description key and ciphertext. This reveal the original plain text.

There are two types of keys:
1. symmetric key that is also called secret-key cryptography algorithms and
2. asymmetric that is also called public-key cryptography algorithms.

3. **ALGORITHMS: DES ALGORITHM**

DES stands for Data Encryption Algorithm. This type of algorithm is secret key based algorithm in which same key is used for encryption and decryption. Following are the steps of DES algorithm[4].

1. It takes 64 bit long plain text data block as input and 56 bit key and generates output of 64 bit block.
2. The plain text undergoes an initial permutation when it enters the encryption function, IP. It undergoes reverse final permutation at the end.
3. The 64 bit plain text passes through initial permutation that rearranges the bit to produce permutated bit.
4. The IP produces 2 halves of permutated block-left plain text and right plain text.
5. 16 rounds of encryption is done each with its own keys.
6. The output of above 16 rounds consists of 64 bits that are function of input plain text and key.
7. At last output is passed through final permutation (FP) also called inverse IP to produce 64 bit ciphertext.

Process of DES Algorithm is shown below:

![Fig 2: DES Process](image)

**RSA ALGORITHM**

RSA algorithm is public key encryption algorithm developed by Ron Rivest, Adi Shamir and Len Adleman in 1977. It is most popular and asymmetric key cryptographic algorithm. It is used in digital signature. It uses the prime number to generate the public and private key based on mathematical fact and multiplying large numbers together. RSA algorithm is usually used to encrypt the data to provide security so that only the concerned users can access it. RSA algorithm involves three steps: [3]

1. **Key generation**
2. **Encryption**
3. **Decryption**

As RSA is asymmetric key cryptographic algorithm so that there are different keys for encryption and decryption as shown below:

![Fig. 3: working of RSA algorithm](image)

Following are steps of RSA Algorithm:

a.) Choose two large prime numbers P and Q (say) such that P is not equal to Q.

b.) Calculate N by multiplying P and Q: 

   \[ N = P \times Q \]

   c.) Now calculate T by formula, 

   \[ T = (P-1) \times (Q-1) \]

   d.) Select a public key E such that E is not the factor of T.

   e.) Next is to select private key D such that 

   \[ (D \times E) \mod T = 1 \]

   f.) To calculate ciphertext(C): 

   \[ C \mod N \]

   g.) To calculate plain text(M): 

   \[ M \mod N \]

Then the cipher text is sent to receiver and at receiver decrypts it in plain text.

4. **COMPARISON**

Comparison of secret key and public key based DES and RSA algorithm is shown in table below. DES algorithm is widely used because RSA algorithm solves the problem of key agreement and key exchange problem generated in secret key cryptography but still its confidentiality is low. RSA and DES algorithm differ from each other in certain factors:

<table>
<thead>
<tr>
<th>S.no</th>
<th>Factors</th>
<th>DES</th>
<th>RSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Type of Cryptography</td>
<td>Symmetric</td>
<td>Asymmetric</td>
</tr>
<tr>
<td>2</td>
<td>Key Size</td>
<td>56 bits</td>
<td>&gt;1024 bits</td>
</tr>
<tr>
<td>3</td>
<td>Block Size</td>
<td>64 bits</td>
<td>Minimum 512 bits</td>
</tr>
<tr>
<td>4</td>
<td>Ciphering</td>
<td>Same</td>
<td>Different</td>
</tr>
</tbody>
</table>
5. CONCLUSION
In this research paper, comparison between DES and RSA algorithm has been studied and summarized. Many differences between both the techniques are mentioned above in Figure 3. As DSA is a secret key based algorithm suffers from key distribution and key agreement problems, this problem is overcome in RSA algorithm but encryption and decryption takes more time in RSA algorithm as compared to DES algorithm. So these algorithms have merits and demerits.

6. FUTURE SCOPE
Our future work will focus on compared and analysed existing cryptographic algorithm like DES, RSA and AES. It will include experiments on image and audio data and focus will be to improve encryption time and decryption time.

7. REFERENCES


