Encryption and decryption. Key is 56 bits long. The operations. It encrypts the data in block size of 64 rounds where each round contains bit-shuffling, non-Feistel in the early 70's. It consists of a number of developed by the IBM cryptography researcher Horst Data Encryption Standard is based on a cipher known COMPARISON OF ALGORITHMS

Asymmetric key
In this scheme different keys are used for encryption and decryption it is also known as the secret key encryption

Symmetric-key
In this scheme same key is used for encryption and decryption it is also known as the public-key encryption.

COMPARISON OF ALGORITHMS

DES
Data Encryption Standard is based on a cipher known as the Feistel block cipher. This was a block cipher developed by the IBM cryptography researcher Horst Feistel in the early 70’s. It consists of a number of rounds where each round contains bit-shuffling, non-linear substitutions (S-boxes) and exclusive OR operations. It encrypts the data in block size of 64 bits each. Same algorithm and key are used for encryption and decryption. Key is 56 bits long. The position of 8, 16, 24, 32, 40, 48, 56, 64 are discarded [6]. DES is based on two fundamental attributes of cryptography Diffusion (Substitution) and Confusion (Permutation) consisting of 16 rounds. In each round key and data bits are shifted, permuted, XORed and sent through, 8 s-box. In the first round 64 bit plaintext is handed to initial permutation(IP). Then IP generates two halves left plaintext(LPT) and right plaintext(RPT). Each LPT and RPT goes through 16 rounds. At the last LPT and RPT are rejoined. Decryption is same process perform rounds in reverse order. Algorithm
[1] DES takes an input of 64-bit long plaintext and 56-bit key (8 bits of parity) and generates output of 64 bit block.
[2] The plaintext block is subject to an shift the bits around.
[3] The 8 parity bits are removed from the key by subjecting the key to its Key Permutation.
[4] The plaintext and key are processed in 16 rounds consisting of:
  a. The key is split into two 28 bit halves
  b. Each half of the key is shifted (rotated) by one or two bits, depending on the round.
  c. The halves are recombined and subject to a compression permutation to reduce the key from 56 bits to 48 bits. This compressed key is used to encrypt this round's plaintext block.
  d. The rotated key halves from step 2 are used in next round.
  e. The data block is split into two 32-bit halves.
  f. One half is subject to an Expansion Permutation to increase its size to 48 bits.
  g. Output of step 6 is exclusive-OR'ed with the 48-it compressed key from step 3.
  h. Output of step 7 is fed into an S-box, which substitutes key bits and reduces the 48-bit block back down to 32-bits.
  i. Output of step 8 is subject to a P-box to permute the bits.
  j. The output from the P-box is exclusive- OR'ed with other half of the data block.
  k. The two data halves are swapped and become the next round's input.

Figure 1: Working of DES algorithm.
**Triple DES**

As an enhancement of DES, the tripleDES (Triple DES) encryption standard was proposed. In this standard the encryption method is similar to the one in original DES but applied 3 times to increase the encryption level [8]. It was used to remove the meet-in-the-middle attack occurred in 2-DES and the brute force attacks in DES. It also has the advantage of proven reliability and a longer key length that eliminates many of the shortcut attacks that can be used to reduce the amount of time it takes to break DES.

![Figure 2: Working of Triple DES algorithm.](image)

**RSA**

This is public key encryption algorithm developed by Ron Rivest, Adi Shamir and Len Adlemen in 1977. It is most popular and asymmetric cryptographic algorithm. It may used to provide both secrecy and digital signature [2]. It uses the prime no. to generate the public and private key based on mathematical fact and multiplying large numbers together. It uses the block size data in which plaintext and cipher text are integers between 0 and n for some n values. Size of n is considered 1024bits or 309 decimal digits. In this two different keys are used for encryption and decryption purpose. As sender knows encryption key and receiver knows decryption key.

**Algorithm**

Choose large prime numbers p and q such that p=q.
Compute n=p*q
Compute φ (pq) = (p-1)*(q-1)
Choose the public key e such that gcd (φ (n), e) =1; 1<e< φ (n)
Select the private key d such that d*e mod φ (n) =1
So in RSA algorithm encryption and decryption are performed as:

Encryption

Calculate cipher text C from plaintext message M such that

\[ C = M^e \mod n \]

Decryption

\[ M = C^d \mod n = M^{ed} \mod n \]

**Comparative analysis of algorithms**

We have studied different techniques used for fulfilment of data encryption purpose. There are some comparisons generated on different important features such as:

**Input data size-** Different algorithm required different memory space to perform the operation. The memory space required by any algorithm is determined on the basis of input data size, number of rounds etc. The algorithm is considered best which use small memory and perform best task.

**Time-** The time required by algorithm to complete the operation depends on processor speed, algorithm complexity. Less the time algorithm takes to complete its operation better it is.

**Throughput-** Throughput of the encryption algorithms is calculated by dividing the total plaintext in Megabytes encrypted on total encryption time for each algorithm.

Thus, if throughput increased the power consumption is decreased.

**Theoretical Analysis**

The theoretical analysis is as follow:

<table>
<thead>
<tr>
<th>Features</th>
<th>DES</th>
<th>Triple DES</th>
<th>RSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Used</td>
<td>Same key is used for encryption and decryption purpose.</td>
<td>Same key is used for encryption and decryption purpose.</td>
<td>Different keys are used for encryption and decryption purpose.</td>
</tr>
<tr>
<td>Scalability</td>
<td>It is scalable algorithm due to varying the key size and block size.</td>
<td>It is scalable algorithm due to varying the key size and block size.</td>
<td>No scalability</td>
</tr>
<tr>
<td>Avalanche Effect</td>
<td>No more affected</td>
<td>No more affected</td>
<td>More affected</td>
</tr>
<tr>
<td>Power Consumption</td>
<td>Low</td>
<td>More than DES and Less than RSA</td>
<td>High</td>
</tr>
<tr>
<td>Throughput</td>
<td>Very high</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>High</td>
<td>Very high</td>
<td>Low</td>
</tr>
</tbody>
</table>

**Simulation Analysis**

We have used Java and ASP.net for simulation. We have taken two parameters time and memory for the simulation setup and calculated throughput by dividing the total plaintext encrypted on total encryption time for each algorithm. We have calculated time taken by each algorithm in milliseconds and calculated memory by subtracting size of original data from encrypted data.

The Tables below represents the speed of RSA, Triple DES and DES algorithm to encrypt the data of same length [1]. Throughput of the encryption algorithms is calculated by dividing the total plaintext in Megabytes encrypted on total encryption time for each algorithm. Thus, if the throughput increased than power consumption decreased. So, as speed of the DES encryption is twice the speed of RSA encryption speed. And DES also consumes small power as comparison to RSA power. Finally, Triple DES still requires more time than DES because DES encrypts the data once and Triple DES encrypts the data three times. Triple DES has more power consumption and fewer throughputs than the DES due to its triple phase characteristics. It had been also observed that decryption of DES algorithm is better than other algorithms in throughput and less power consumption. But the aspect the DES and RSA lacks that make Triple DES as our choice of algorithm is security.

**Table1: Execution Time (Milliseconds) of Encryption of different data packet size**

<table>
<thead>
<tr>
<th>Input Size(KB)</th>
<th>3DES</th>
<th>DES</th>
<th>RSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>45</td>
<td>52</td>
<td>39</td>
<td>65</td>
</tr>
<tr>
<td>55</td>
<td>64</td>
<td>49</td>
<td>81</td>
</tr>
<tr>
<td>96</td>
<td>100</td>
<td>85</td>
<td>135</td>
</tr>
<tr>
<td>256</td>
<td>157</td>
<td>121</td>
<td>194</td>
</tr>
<tr>
<td>355</td>
<td>240</td>
<td>199</td>
<td>309</td>
</tr>
<tr>
<td>5345.28</td>
<td>3361</td>
<td>3110</td>
<td>4297</td>
</tr>
</tbody>
</table>

**Table2: Execution Time (Milliseconds) of Decryption of different data packet size**

<table>
<thead>
<tr>
<th>Input Size(KB)</th>
<th>3DES</th>
<th>DES</th>
<th>RSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>45</td>
<td>54</td>
<td>36</td>
<td>55</td>
</tr>
<tr>
<td>55</td>
<td>61</td>
<td>49</td>
<td>81</td>
</tr>
<tr>
<td>96</td>
<td>103</td>
<td>88</td>
<td>135</td>
</tr>
<tr>
<td>256</td>
<td>157</td>
<td>121</td>
<td>194</td>
</tr>
<tr>
<td>355</td>
<td>240</td>
<td>199</td>
<td>309</td>
</tr>
<tr>
<td>5345.28</td>
<td>3361</td>
<td>3110</td>
<td>4297</td>
</tr>
</tbody>
</table>

**Figure 2: Working of Triple DES algorithm.**

CONCLUSION
The advantage of proven reliability and a longer key length that eliminates many of the attacks that can be used to reduce the amount of time it takes to break DES. Confidentiality and scalability provided by Triple DES over RSA and DES is much higher that makes it suitable even though DES consume less power memory and time to encrypt and decrypt the data but on security front DES can be easily broken by brute force technique as compared to Triple DES and RSA making it the least secure algorithm.

REFERENCES
2. Aman Kumar, Dr. Sudesh Jakhar, Mr. Sunil Maakar “Distinction between Secret key and Public key Cryptography with existing Glitches” IJEIM- 0067, vol.1, 2012.
5. Eli Biham and Adli Shamir, "Differential Cryptanalysis of full DES”.
6. Dan Boneh and Glenn Durfee “Cryptanalysis of low exponent RSA”
7. W. Diffie, M. E. Hellman “New Directions in Cryptography”.
10. Himani Agarwal & Manish Sharma “Implementation and analysis of various Cryptography” Dec-2010