Scientific Journal of Impact Factor (SJIF): 3.134

ISSN (Print): 2348-6406
ISSN (Online): 2348-4470

International Journal of Advance Engineering and Research Development

CRYPTOGRAPHY AND ENCRYPTION ALGORITHMS FOR INFORMATION SECURITY

Ms. Arati Appaso Pujari[1], Mrs. Sunita Sunil Shinde[2]

[1]*Department of Electronics and Telecommunication, ADCET, Ashta, India, aratipujari218@gmail.com*
[2]*Department of Electronics and Telecommunication, ADCET, Ashta, India, shindesunita@yahoo.co.in*

Abstract *—In today's world of Computer and Internet; most of the data travel over computer network and it becomes challenging task to secure this data. So there is need of an efficient and simple way of securing the electronic documents from being read or used by people other than authorized one. Some of the mechanisms used to secure data are: authenticating the user, using access control mechanism (such as profiling), restricting physical access (i.e. keeping media locked) and encrypted communication between two hosts. Cryptography is one of the main categories of information security.*

Keywords*-Network security, Encryption, Decryption, Cryptography, AES, DES and Blowfish.*

I. INTRODUCTION

Cryptography is the art and science of achieving security by encoding message to make them non readable form [8]. In cryptography the original message is transformed into non readable message by applying some mathematical operations. The basic idea behind the cryptography is: at sender side it converts plaintext into cipher text by using encryption algorithms, Cipher text is transmitted over the transmission medium and finally at receiver side cipher text is converted back to the original plain text by using decryption algorithm.

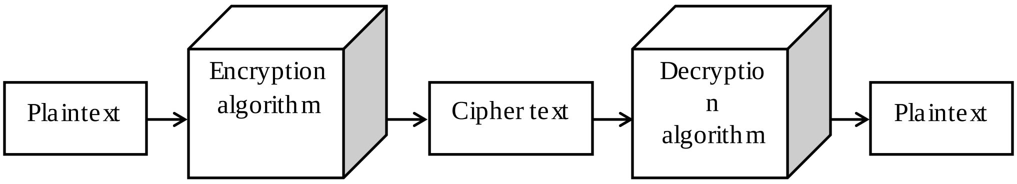

Figure1. Encryption/Decryption process

Ingredients of Encryption scheme:

- Plaintext: This is the original message or data that can be read and understood easily.
- Encryption algorithm: Encryption algorithm encodes plaintext to hide its content by performing mathematical operations such as substitutions and transformations.
- Cipher text: This is the scrambled message produced by encrypting plaintext.
- Decryption algorithm: This is essentially the encryption algorithm run in reverse. It converts cipher text to its original plaintext.

This research paper is a comparative performance analysis of symmetric e encryption algorithms such as AES, DES and Blowfish. The paper is organized into different sections. Section two describes various algorithms in detail and section three is analysis of their performance.

II. ENCRYPTION ALGORITHMS

Many encryption algorithms are extensively available and used in information security. They are categorized into asymmetric and symmetric encryption algorithms. Symmetric key encryption uses same key to encrypt and decrypt data while in asymmetric key encryption two keys are used; private keys and public keys. Public key is used for encryption and private key is used for decryption [7, 8]. Asymmetric encryption algorithms are almost 1000 times slower than symmetric encryption algorithms, because they require more computational processing power [2].
There are many symmetric encryption algorithms are available for information security such as DES, Triple DES, AES, Blowfish, and RC5.

2.1 AES (Advanced Encryption Standard):

AES [2, 8] is a non-Feistel, Symmetric cipher that can encrypt 128 bits data block using symmetric keys 128, 192 or 256 bits. AES has three different versions, with 10, 12 and 14 rounds and each uses 128, 192 and 256 bits key size respectively **[7]**. Figure 2 shows the overall structure of the AES.
AES uses basic techniques of substitution and permutation. There are three operations performed in AES algorithm such as Encryption, Decryption and Key Generation.

2.1.1Algorithm for Encryption

Step 1: Get the key size and key along with plaintext that has to be encrypted.
Step 2: Apply S-box to perform a byte-by-byte substitution of the block.
Step 3: Rotate row k of the plain text block (i.e. state) by k bytes.
Step 4: Perform a mix column operation.
Step 5: XOR the state with the key block.
Step 6: Repeat the steps from 2 to 5 for ‘n' number of rounds where n depends on key size.
Step 7: After 'n' number of rounds, get the ciphertext.

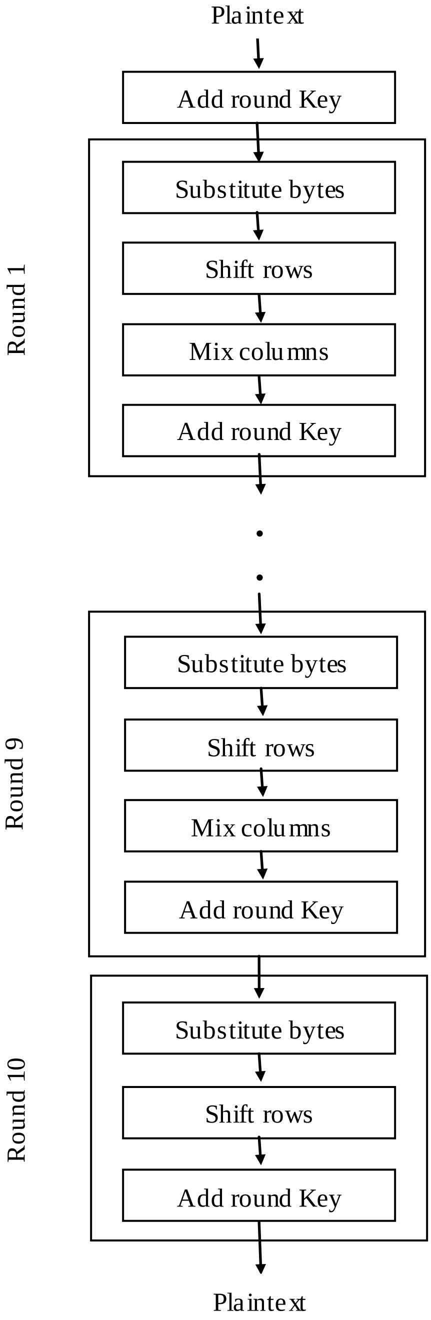

Figure2. General structure of AES algorithm

2.1.2 Algorithm for Decryption

Perform all the steps of Encryption in reverse order.

2.1.3Algorithm for Key Generation

Step 1: Get the key.
Step 2: Calculate the number of words needed based on number of rounds.
Step 3: The first four words are made from key, where word is an array of 4 bytes.
Step 4: Perform Rotword and Subword to get the next word.
Step 5: Repeat step 4, until the required number of words reached.

2.2 DES (Data Encryption Standard):

DES is a block cipher. It encrypts a 64 bits data block by using 56 bits key and produces 64 bits cipher text. The same algorithm and key are used for encryption and decryption [8]. Figure3 shows the general structure of the DES.
DES is based on two fundamental attributes of cryptography: substitution and transposition. It consists of 16 steps, each of which is called as round. Each round performs the steps of substitution and transposition [8].

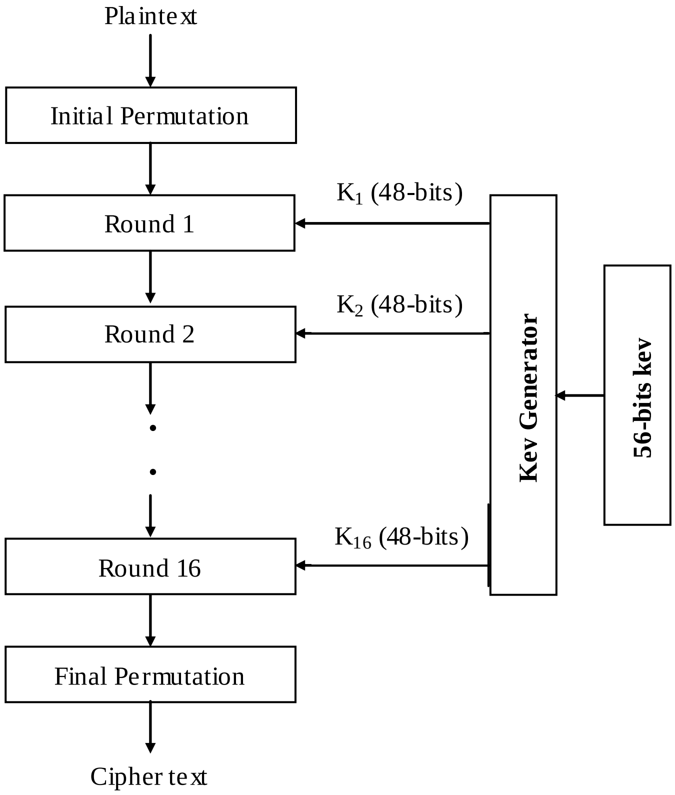

Figure3. General structure of DES algorithm

There are three operations performed in DES algorithm. They are Encryption, Decryption ad Key Generation.

2.2.1 Algorithm for Encryption

Step 1: Get 64-bit key and the plaintext to be encrypted.
Step 2: Perform initial permutation using the plain text
Step 3: Divide the plain text into two 32-bit parts.
Step 4: Perform 16 rounds using round key which is generated by key generator.
Step 5: Finally, use the output of step 4 to perform final permutation.

2.2.2 Algorithm for Decryption

Perform all the steps of Encryption in reverse order.

2.2.3Algorithm for Key Generation

Step 1: Get the 64-bit key
Step 2: Perform parity bit drop to reduce it to 56-bits.
Step 3: Divide it into two 28-bit parts.

Step 4: Perform shift left operation of the 28-bit data depending upon the round number.
Step 5: Use the output of step 4 to perform the compressed permutation.
Step 6: Repeat Step 4 and 5 to produce 16 round keys which are used for encryption.

2.3 Blowfish

Blowfish is symmetric block cipher designed in 1993 by Bruce Schneier. Blowfish has a 64 bit block size and variable key length from 32 up to 448 bits. It is a 16 round Fiestel cipher and uses a large key dependent S-boxes [8]. Figure 4 shows the general action of Blowfish algorithm.

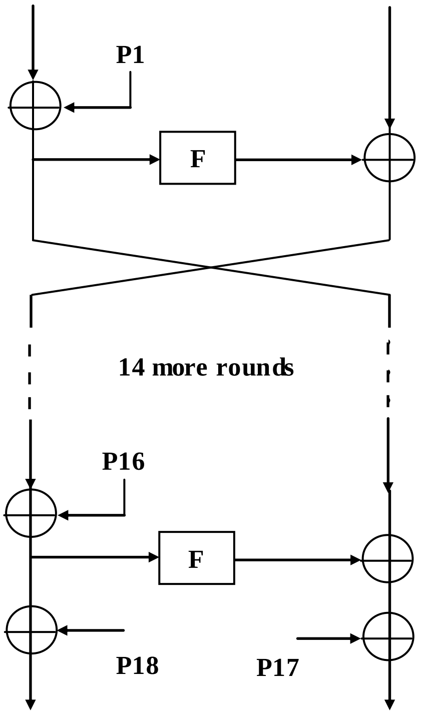

Figure4. General structure of Blowfish algorithm

There are three operations performed in Blowfish algorithm. They are Encryption, Decryption and Subkey generation.

2.3.1Algorithm for Encryption:

```
Step 1: Divide 64-bit plaintext (X) into two 32-bit halves: XL, XR.
Step 2: Then the following operations are performed
For i =1 to 16.
XL = XL XOR Pi
XR = F (XL) XOR XR
Swap XL, XR
Next i
Step 3: Swap XL, XR (Undo the last swap.)
Step 4: XR = XR XOR P 17, XL = XL XOR P 18
Step 5: Combine XL and XR. This result is 64-bit Ciphertext(Y).
```

2.3.2 Algorithm for Decryption:

```
Step 1: Divide 64-bit Ciphertext(Y) into two 32-bit halves: YL, YR
Step 2: Then the following operations are performed
For i =1 to 16.
YL = YL XOR P19-i
YR = F (YL) XOR YR
Swap YL, YR
Next i
Step 3: Swap YL, YR (Undo the last swap.)
Step 4: YL = YL XOR P1
        YR = YR XOR P2
```

Step 5: Combine YL and YR. This result is 64-bit Original plaintext(X).

2.3.3 Subkey and S-Box Generation:

Blowfish makes use of a key that ranges from 32-bits to 488-bits. That key is used to generate 18 32-bit sub keys and four 8×32 S-boxes.
The keys are stored in a K-array:
K1, K2, …, Kj $1 \le j \le 14$
The subkeys are stored in the P-array:
P1, P2, …, P18

There are four S-boxes, each with 256 32-bit entries:
S1,0, S1,1, …, S1,255
S2,0, S2,1, …, S2,255
S3,0, S3,1, …, S3,255
S4,0, S4,1, …, S4,255

The steps in generating the P-array and S-boxes are:
Step 1: Initialize first the P-array and then four S-boxes in order using the bits of the fractional part of constant π.
For example, in hexadecimal:
P1 = 243F6A88
P2 = 85A308D3
. . .
S4, 254 = 578FDFE3
S4, 255 = 3AC372E6
Step2. Perform a bitwise XOR the P-array and the K-array, reusing words from the K-array as needed. For example:
P1 = P1 XOR K1
P2 = P2 XOR K2
. . .
P14 = P14 XOR K14
P15 = P15 XOR K1
P16 = P16 XOR K2
P17 = P17 XOR K3
P18 = P18 XOR K4
Step3. Encrypt the 64-bit block of all zeros using the current P-array and S-arrays, Replace P1 and P2 with the output of the encryption.
Step4. Encrypt the output of step 3 using current P-array and S-arrays, Replace P3 and P4 with the resulting ciphertext.
Step5. Continue the process to update all elements of P and then, in order, all elements of S, using each step the output of the continuously-changing Blowfish algorithm

III. PERFORMANCE ANALYSIS

Table1. Performance comparison of AES, DES and Blowfish algorithms

<table>
<tr><th>Sr. No.</th><th>Paper</th><td colspan="8">DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis by Jawahar Thakur and Nagesh Kumar (IJETAE, ISSN 2250-2459, Volume 1, Issue 1, November 2011)</td></tr>
<tr><td rowspan="6">1</td><th rowspan="3">Algorithms</th><th colspan="8">Parameters</th></tr>
<tr><th rowspan="2">Data size(bits)</th><th rowspan="2">Key size(bits)</th><th colspan="6">Execution time(sec) for 160 KB data block</th></tr>
<tr><th colspan="2">ECB mode</th><th>CBC mode</th><th colspan="2">OFB mode</th><th>CFB mode)</th></tr>
<tr><td>AES</td><td>128</td><td>128</td><td colspan="2">1.6</td><td>1.6</td><td colspan="2">1.6</td><td>1.6</td></tr>
<tr><td>DES</td><td>64</td><td>64</td><td colspan="2">1.6</td><td>1.5</td><td colspan="2">1.7</td><td>1.5</td></tr>
<tr><td>Blowfish</td><td>64</td><td>128</td><td colspan="2">1.4</td><td>1.4</td><td colspan="2">1.4</td><td>1.4</td></tr>
<tr><td rowspan="6">2</td><th>Paper</th><td colspan="8">Performance Analysis of Encryption Algorithms for Information Security by A.Ramesh and Dr.A.Suruliandi (ICCPCT 3013)</td></tr>
<tr><th rowspan="2">Algorithms</th><th colspan="8">Parameters</th></tr>
<tr><th>Data size(bits)</th><th>Key size(bits)</th><th colspan="2">Execution time(sec) for 4500 KB</th><th colspan="2">Memory usage(Kbytes)</th><th colspan="2">Throughout (in bytes/sec)</th></tr>
<tr><td>AES</td><td>128</td><td>128,192, 256</td><td colspan="2">71.7</td><td colspan="2">32.5</td><td colspan="2">558.2886</td></tr>
<tr><td>DES</td><td>64</td><td>64</td><td colspan="2">28.4</td><td colspan="2">43.2</td><td colspan="2">1268.765</td></tr>
<tr><td>Blowfish</td><td>64</td><td>128,192, 256</td><td colspan="2">17.67</td><td colspan="2">25.2</td><td colspan="2">2270.268</td></tr>
<tr><td rowspan="7">3</td><th>Paper</th><td colspan="8">Superiority of Blowfish Algorithm by Pratap Chnadra Mandal (IJARCSSE, ISSN: 2277 128X, Volume 2, Issue 9, September 2012)</td></tr>
<tr><th rowspan="3">Algorithms</th><th colspan="8">Parameters</th></tr>
<tr><th rowspan="2">Data size(bits)</th><th rowspan="2">Key size(bits)</th><th colspan="2">Execution time(sec)</th><th colspan="2">Power consumption(µJoule/Byte)</th><th colspan="2">Throughout (in KB/sec)</th></tr>
<tr><th>Encryption</th><th>Decryption</th><th>Encryption</th><th>Decryption</th><th>Encryption</th><th>Decryption</th></tr>
<tr><td>AES</td><td>128</td><td>128,192, 256</td><td>399.4</td><td>274.4</td><td>4.3</td><td>4.3</td><td>9.35</td><td>13.61</td></tr>
<tr><td>DES</td><td>64</td><td>56</td><td>432</td><td>295.2</td><td>4.8</td><td>4.8</td><td>8.64</td><td>12.65</td></tr>
<tr><td>Blowfish</td><td>64</td><td>32-448</td><td>72.4</td><td>88.7</td><td>0.6</td><td>0.6</td><td>51.59</td><td>42.11</td></tr>
</table>

IV. CONCLUSION

Among AES, DES and Blowfish symmetric encryption algorithms Blowfish algorithm has better performance because Blowfish has not any known security weak points so far. Blowfish performs faster than DES and AES. Blowfish performs approximately 4 times faster than AES and 2times faster than DES. Blowfish has higher throughput than AES and DES. Also Blowfish consumes less memory compared with DES and AES. Blowfish consumes 25.2Kb of memory. DES consumes 18 Kb extra memories compared to Blowfish. AES consumes 7.1 Kb extra memories compared to Blowfish. Hence Blowfish is superior to other common symmetric encryption algorithms.

References

[1]Jawahar Thakur, Nagesh Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 1, Issue 2, December 2011

[2]A.Ramesh, Dr.A.Suruliandi, "Performance Analysis of Encryption Algorithms for Information Security",Intrnational Conference on Circuits, Power and Computing Technologies, 2013

[3]Pratap Chnadra Mandal, "Superiority of Blowfish Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 2, Issue 9, September 2012

[4]Ajit Singh, Swati Malik, "Securing Data by Using Cryptography with Steganography", ISSN: 2277 128X, Volume 3, Issue 5, May 2013

[5]Ratinder Kaur, V. K. Banga, "Image Security using Encryption based Algorithm", International Conference on Trends in Electrical, Electronics and Power Engineering (ICTEEP'2012) July 15-16, 2012

[6]Sumedha Kaushik, Ankur Singhal, "Network Security Using Cryptographic Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 2, Issue 12, December 2012

[7]William Stallings, "Cryptography and Network Security: Principals and Practices", Prentice Hall publication, fourth edition, 2006.

[8]Atual Kahate, "Cryptography and Network Security", Tata McGraw-Hill, second edition, 2008

[9] Aamer Nadeem, "A Performance Comparison of Data Encryption Algo". IEEE 2005.