IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁒ Vol. 11, Issue 3, March 2022

DOI: 10.17148/IJARCCE.2022.11351

A Peculiar Review on Various Cryptography Algorithms

[1]Pooja Singhal,[2]Lucky Chaudhary, [3]Noor Ahmad, [4]Prakhar Mishra, [5]Rayyan Manzar Ansari

[1]Assistant Professor, Indraprastha Engineering College

[2]Student, Indraprastha Engineering College

Abstract— With major advances in field of technology and electronics, a constant obstacle has proved to be a major challenge, namely: data security. To connect securely and quickly via electronic data transfer via the web, the data must be encrypted. Encryption is the process of converting plain text into cipher text. It is not easily understood or changed by unwanted people. It can also be defined as the science that uses mathematics in data encryption and decryption operations. In this research paper, we have discussed some important algorithms used for cryptography of data in all the fields, to conduct comparative study for important algorithms in terms of data security effectiveness, key size, time and complexity, etc. This research paper focused mainly on different types of cryptography algorithms that are existing, like AES, DES, Blowfish, RSA.

Keywords— Cryptography, Information Security, Encryption, Decryption.

I.INTRODUCTION

Information security can be summarized as a set of information, steps, procedures and strategies that are used to prevent and monitor illegal access, troubleshooting, revelation, disturbance and adjustment of computer network sources. Increasing the privacy, reliability and eligibility of the work, it requires a lot of work to strengthen the existing methods from practicing to break them and to improve upon a new way that are resistant to most types of attacks if not all [1]. Accordingly, it was proven that encoding is one of the most reliable strategies used to secure information since ancient times. In the days of the Romans who used similar methods to enable protection on their valuable information and documents. Data encoding is the process of converting the form of data into certain symbols through the use of meaningless codes. The process of encoding and decoding completely depends on a single key which is known as same key cryptography. In this process, the same key is used for both encryption and decryption processes. It requires a secure channel between sender and receiver to transfer the secret key. Double cipher modes are dealt with by a symmetric algorithm: block ciphers and stream ciphers. The block cipher operates on fixed-length groups of named blocks, without transformation specified by a symmetric key. A constant size is controlled by a set of block ciphers. It consists of several identical rounds of processing in which each round, an interchange is performed on one half of the information, followed by a permutation that joins the two halves. The original key becomes larger, so multi-label keys are used for each round. A symmetric key cryptography indicates cryptographic algorithm that requires two separate keys: the first of which is private (hidden) while the other is public [1].

Although they are not the same, but they are mathematically related. The public key is used to encode the plain text, whereas the private (hidden) key is used to decode the cipher text. Asymmetric Encryption strategies are about 1,000 times slower than symmetric encoding, which makes it inefficient when encoding large amounts of information. Additionally, to have the same security power as symmetric algorithms, asymmetric algorithms use more powerful keys than symmetric enciphering steps.

The categories of Cryptography Algorithms are: -

➢ Symmetric Algorithm
- DES
- AES
- Blowfish

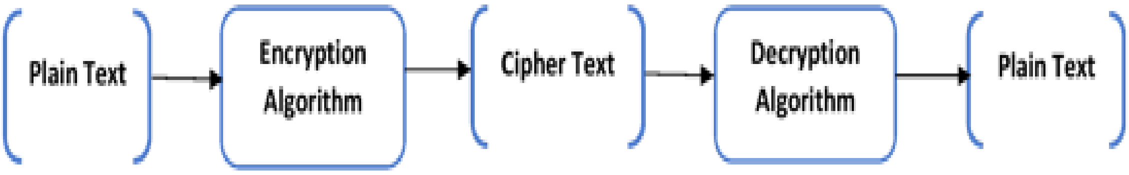
➢ Asymmetric Algorithm
- RSA

A. Encryption and Decryption:

Encryption is turning the database into non-recordable text. Decryption represents the reverse process of encryption where it converts cipher text to plain text. There is a cipher double algorithm, which invents the encoding and decoding

DOI: 10.17148/IJARCCE.2022.11351

processes. The overarching process of a cipher is dominated by an algorithm and a key. It is a secret, a condensed set of symbols, that decode encrypted data.



CRYPTOGRAPHY

B. Goals of Cryptography:

Cryptography is used to achieve many goals and some of the goals are the following list shows:

- **Authentication:** is the process of assigning identity to a person in order to break into a particular resource by using keys.
- **Confidentiality:** the ultimate goal of encryption is to verify that only the cipher-key owner receives the message.
- **Data Integrity:** is the operation that has access to modify the database belonging to a specific group or person.
- **Non-Repudiation:** this ensures that both the sender and the recipient acknowledge the delivery of the report.
- **Access Control:** Verifies that only the group with the correct authentication is eligible to log into the message delivered.

C. Terminology:

Terms	Description
Plain Text	The simple message that will be delivered on the other side.
Cipher Text	The original message is encoded in a symbolic format.
Encryption	It is a technique to convert simple text into unreadable message.
Decryption	This is the opposite operation of the encryption.
Key size	To encode and decode, the key is required, and the length of the key determines the degree of security, the higher the key size, the higher the security.
Block Cipher.	It encapsulates a group of plaintext symbols as a block.
Stream Cipher	It converts a symbol of plain text directly into a symbol of cipher text.
Encryption Time	The time taken to process the original text into an encrypted one.
Decryption Time	The duration of decoding the decrypted message into readable text.
Throughput	The amount of time in encoding are measured in megabytes.

D. Description of Cryptographic Algorithms:

There are two types of encoding and decoding. Those two types are symmetric and asymmetric encoding algorithms. Some of those algorithms are included here such as DES, AES, Blowfish which all are two-way algorithms and RSA which is one-way algorithms.

1. Data Encryption Standard (DES)

DES was first introduced at IBM by Horst Fiestel in 1972. The goal of the DES algorithm is to offer a strategy secure critical financial database. The encipher instructions are:

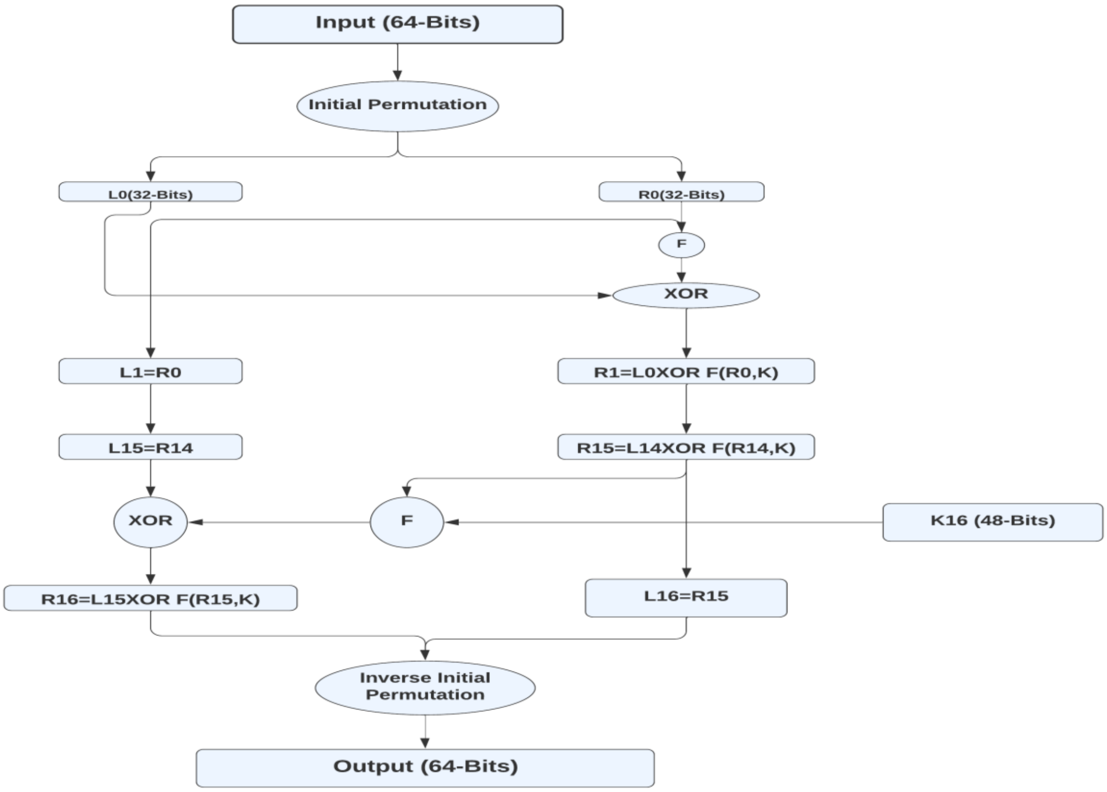
- DES receives 64-bit long simple message and 56-bit key and comes with 64-bit blocks.
- The simple text blocks require bits to be modulated.
- The 8 identical bits are removed from the key by exposing the key to a permutation of the key.

DOI: 10.17148/IJARCCE.2022.11351

The readable message and the key will be displayed as per the following steps:

- The key is divided into two 28 halves.
- The half is rotated by one or two bits per round.
- The two parts are re-joined and go through a round permutation to reduce the key from 56 bits to 48 bits. These pressed keys are used to encode a plaintext block of rounds.
- The next round uses the key parts that were shot from Tip 2.
- Divides the database block into two 32-bit parts.
- One part would be expanded in terms of permutations to increase the size to 48 bits.
- The sixth step results in OR'ed only, with tip numbers three-to-48-bit keys.
- The result set of the 7th instruction is the s-box, which inverts the key bits and truncates the 48-bit block to 32 bits.
- The result of the 8th end will be allowed by the p-box.
- The result of the p-box is OR'ed only, the format will be the next part of the block. The bipartite format parts are exchange and form the reservoir of the subsequent phase.

These steps are explained in the below figure:



DES ALGORITHM FLOWCHART

2. Advanced Encryption Standard (AES)

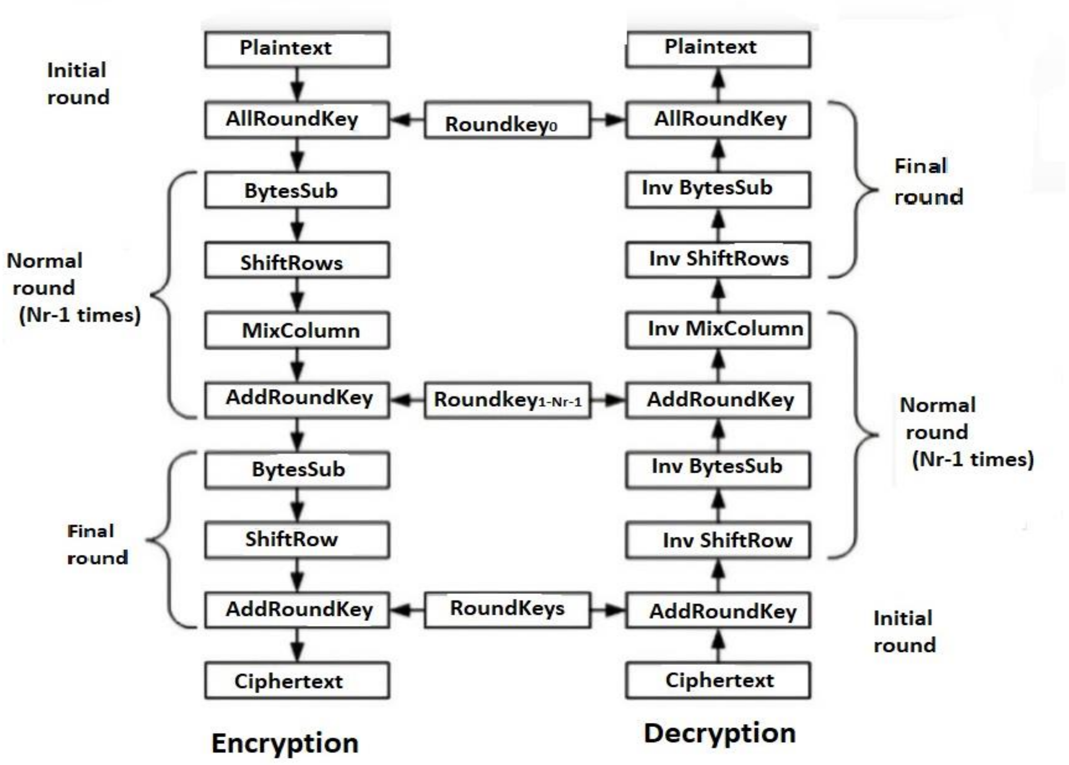
AES is an up-to-date ciphering strategy that was suggested by NIST in 2001 to replace DES. AES can provide any group of databases [2]. During encryption-decryption, the AES process encodes 10 rounds for 128-bit keys. 12 rounds for 192-bit keys and 14 rounds to 256-bit keys to come out with the final encoded message. AES allows in 128-bit information length which can be divided into 4 fundamentally active blocks. Those parts are dealt with as a single line of bytes and 4*4 named "The State". For encoding and decoding, the cipher starts with "Add Round Key Step". However, just before the final round, the output takes 9 basic rounds, each going through 4 transformations; 1) Sub-bytes, 2) Shift-rows, 3) Mix-columns and 4) Add round key. In the tenth round which is the last round, mix columns transformation is done. The whole operation is figured out in the below figure. Decryption is the opposite process and uses opposite steps [3].

a) Substitute Byte transformation:
AES consists of a 128-bit data block, that is, each database item has 16 bytes. In a sub-byte change, every bite of the data item is replaced in another piece by applying an 8-bit replacement box known as a Rijndael S-box.

b) Shift Rows transformation:
This transfer is simple, the bytes in the rest of the three rows of state, reliable on the row's position, are transferred in a one-cycle manner. In second row, a 1-byte circular left shift is performed. while the third and fourth lines, two bytes and three bytes take a circular shift to the left sequential place.

c) Mix columns transformation:
Here the model of the multiplication set for each column of states. A constant matrix is multiplied by each. In this process bytes are dealt with as multi-names.

d) Add round key transformation:
A bit XOR between the 128-bits of the current position and the 128-bits of the round key. This conversion is the opposite.



AES ALGORITHM FLOWCHART

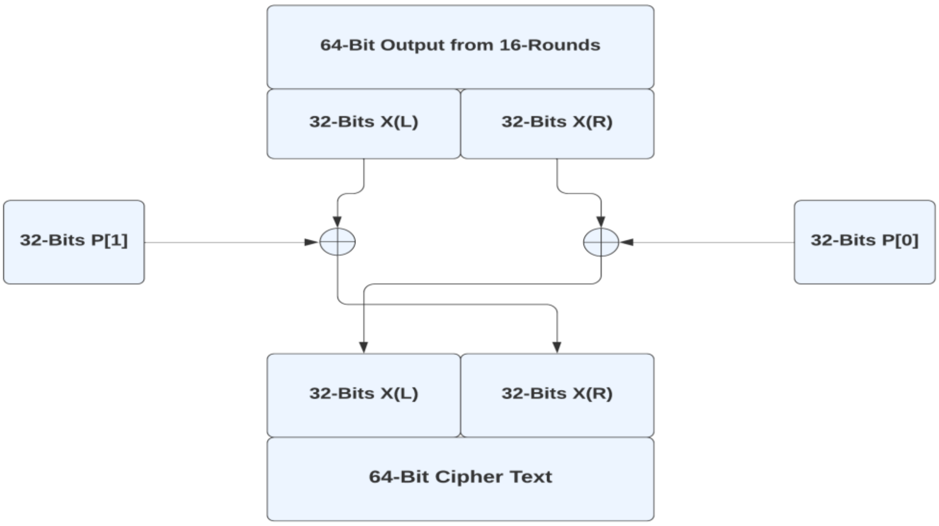
3. Blowfish.
Blowfish is the first symmetric encryption algorithm created by Bruce Schneier in 1993. Symmetric encryption uses a single encryption key to encrypt and decrypt data. Sensitive data and symmetric encryption keys are used within the encryption algorithm to convert the sensitive data into cipher text. Blowfish, along with its successor Two fish, was in the race to replace the Data Encryption Standard (DES), but failed due to the small size of its blocks. Blowfish uses a block size of 64, which is considered completely insecure. Two fish fixed this issue by implementing a block with a size of 128. Blowfish is much faster than DES, but it trades in its
Speed for safety.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 3, March 2022

DOI: 10.17148/IJARCCE.2022.11351



BLOWFISH ALGORITHM FLOWCHART

4. Rivest Shamir Adleman (RSA)

Rivest Shamir Adleman (RSA) was invented by Ron Rivest, Adi Shamir and Leonard Adleman in the year 1978. It is one of the major public keys encoding system for key exchange, digital signature or encryption of blocks of databases. RSA algorithm implements different size encoding blocks and a variable size key. It is an asymmetric encoding system that relies on numeric synthesis. This employs two basic numbers to come up with both the private and public keys. The sender encodes the message by the public key, then message delivered to receiver. So, for the decrypt it uses its own private key. RSA has three steps; Key generation, encoding and decoding. On the other hand, RSA has many flaws, so it is not good for business. Figure below shows the sequence of steps followed by the RSA algorithm for the cryptography of multiple blocks.

a. Key Generation

- Choose two different large random prime numbers p and q such that $p \neq q$.
- Compute $n= p \times q$.
- Calculate: phi (n) = (p-1) (q-1).
- Choose an integer e such that 1<e<phi (n)
- Compute d to satisfy the congruence relation $d \times e = 1$ mod phi (n); d is kept as private key exponent.
- The public key is (n, e) and the private key is (n, d). Keep all the values d, p, q and phi secret.

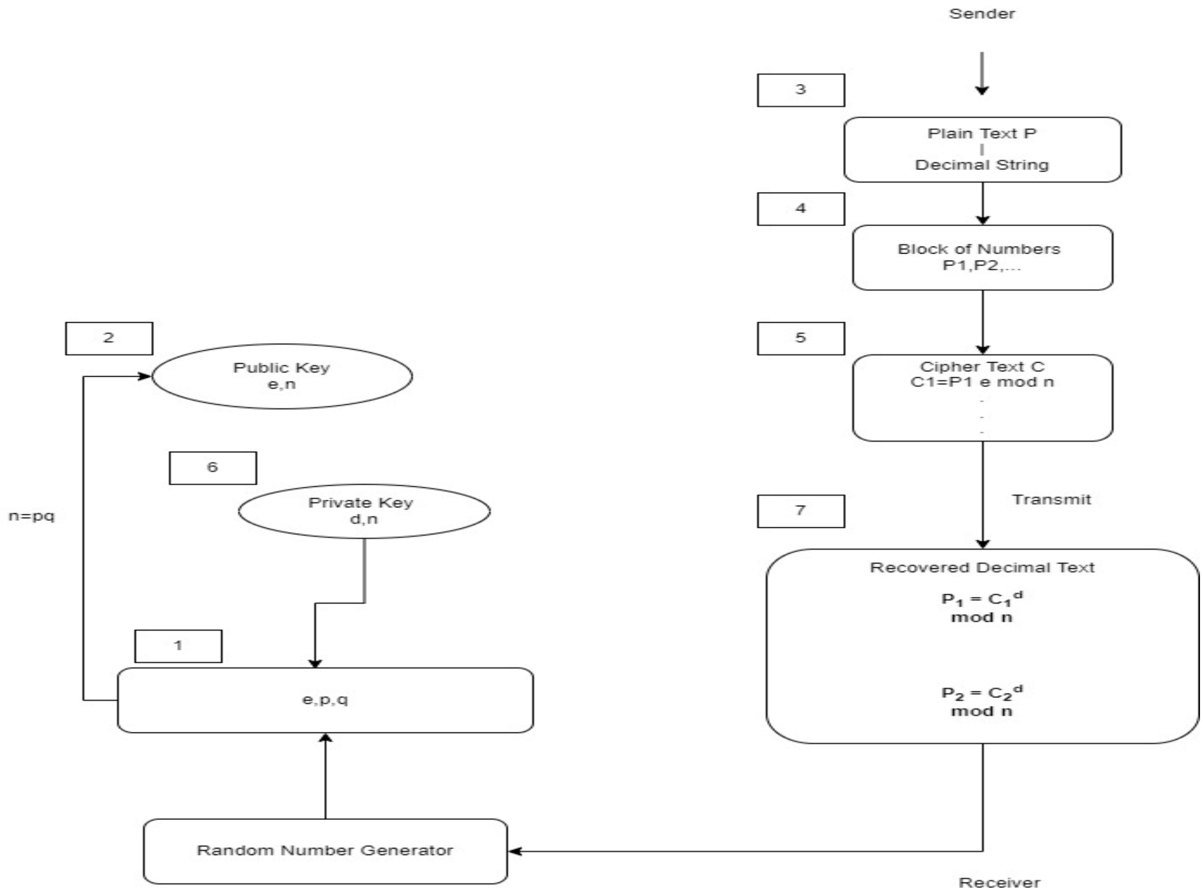
b. Encryption

- Plaintext: P < n
- Cipher text: C= Pe mod n

c. Decryption

- Cipher text: C
- Plaintext: P=Cd mod n.

DOI: 10.17148/IJARCCE.2022.11351



RSA ALGORITHM FLOWCHART

II.RELATED WORK

Several works in the past have attempted to find out which algorithm would work best for encryption and decryption. Work submitted by Singh et al. [5] is a prime example of this is because it is compared between different symmetric algorithms including DES, 3DES, AES and Blowfish algorithms. Accordingly, it was found that the AES algorithm was efficient enough as compared to other algorithms, as it requires high processing time.

Similarly, the work presented by Cornwell [6] found that the blowfish algorithm had the ability to support security for relatively long time without any suspected code violations. Blowfish algorithm is better, according to researcher in terms of safety and efficiency. However, further research needs to be done to re-estimate the results discussed. To provide more evidence on the results by Cornwell research on blowfish.

In another work submitted by Dhawan [4], it was found that AES outperformed other algorithms seeking number one second operating in different user loads and with multiple user load conditions the response time.

Singh et al. [7] presented a work that compared between the most popular encoding algorithms. according to work, the most popular algorithms in terms of security and energy consumption were AES, DES, 3DES and Blowfish. The results of the comparison are in contrast to some previous studies and show that AES is fundamentally better than Blowfish algorithm.

Similarly, Seth et al. [2] [7] Comparison of three algorithms: DES, AES and RSA. He estimated that RSA needed the longest encoding time and higher memory than the other two algorithms; However, with a minimum output byte in the RSA algorithm. Meanwhile, they also found that DES uses the minimum encryption time while AES requires the smallest storage memory. Furthermore, the encoding time is almost the same in both the AES algorithm and the DES algorithm.

Mandal et al. [8] showed that AES is distinguished in throughput and decoding time compared to other 3DES and DES their work.

Apoorva et al. [9] concluded that Blowfish is among the best algorithms to use in terms of security and process time because it takes less time than the rest.

DOI: 10.17148/IJARCCE.2022.11351

III.COMPARISON OF ALGORITHMS

Algorithm	Created By	Year	Key Size	Block Size	Round	Structure	Flexible	Features
DES	IBM	1975	64 bits	64 bits	16	Festial	No	Not Strong Enough
AES	Joan Daeman & Incent Rijmen	1998	128, 192, 256 bits	128 bits	10,12,14	Substitution Permutation	Yes	Security is excellent. It is best in security and Encryption Performance
Blowfish	Bruce Schneier	1993	32-448 bits	64 bits	16	Festial	Yes	Fast Cipher in SSL
RSA	Rivest Shamir Adleman	1977	1024 to 4096	128 bits	1	Public Key Algorithm	No	Excellent Security and Slow Speed

IV.RESULT AND DISCUSSION

From above, comparison algorithms are based on manufacturer year, key size, block size, round, structure, etc. flexibility and features. The results show that the algorithms AES, Blowfish and TDES are the fastest. Encryption time, speed, flexibility. The results also prove that the AES algorithm is the best in security, flexibility and strongest encryption performance. It is most efficient as compared to others.

V.CONCLUSION

This paper presents a survey of the most important cryptography algorithms to date. These are cryptographic algorithms well studied and analysed to help enhance the performance of current cryptographic methods.

The result shows techniques that are useful for real-time encryption. All encryption methods have proven that their advantages and shocks and has proven to be suitable for various applications. comparison between symmetric and asymmetric algorithms show that symmetric algorithms are faster than their asymmetric counterparts. Through the last and in the result of study and comparison, we find that the most reliable algorithm is AES in terms of speed encryption, decoding complexity, key length, structure and flexibility.

REFERENCES

1) RIMAN, C., and Abi-Char, P. E.: Comparative Analysis of Block Cipher-Based Encryption Algorithms: A Survey. Information Security and Computer Fraud, Vol.3, No.1, 1-7, (2015).

2) Singh, G.: A Study of Encryption Algorithms (RSA, DES, and AES) for Information Security. International Journal of Computer Applications, Vol. 67, No. 19, (2013).

3) Mandal, A. K., Parakash, C., & Tiwari, A.: Performance Evaluation of Cryptographic Algorithms: DES and AES. In Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on, 1-5, (March 2012).

4) Dhawan, P.: Performance Comparison: Security Design Choices, Microsoft Developer Network, Tech. Rep. (2002).

5) Singh, G., Kumar, A., & Sandha, K. S.: A Study of New Trends in Blowfish Algorithm. International Journal of Engineering Research and Application, (2011).

6) Cornwell, J.W., & Columbus, G.A.: Blowfish Survey. Department of Computer Science. Columbus: GA Columbus State University, 1-6, (2012).

7) Seth, S. M., & Mishra, R.: Comparative Analysis of Encryption Algorithms for Data Communication 1. (2011).

8) Mandal, P.C.: Superiority of Blowfish Algorithm. International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, No. 9, 196-201 (2012).

9) Apoorva, Y.K.: Comparatively Study of Different Symmetric Key Cryptography Algorithms. International Journal of Application or Innovation in Engineering and Management, Vol. 2, No. 7, 204-6, (2013).