Volume 3, Issue 6, June 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

# Impact of Security over System Performance

**Vaibhav Shrivastava, Mr. Gurpal Singh**

*School of Mathematics and Computer Science Dept,*
*Thapar University, Punjab( India )*

***Abstract:** Cryptography is concerned with keeping communications private. Today's cryptography is more than secret writing. The purpose of this paper is the implementation of three encryption algorithms and a comparison between them based on CPU execution time, System time and User time. In bibliography, there are three encryption algorithms RSA, DES and BLOWFISH using two separate modules of encryption and decryption. The objective of this paper is to evaluate the performance of the three cryptography algorithms in terms of the processing time required in the kernel and user space for encryption and decryption operations. The powerful portable programming language Java and JCA (Java Cryptography Architecture) is used in implementing the encryption algorithms. The performance of the implemented encryption algorithms will be evaluated on Windows platforms.*

***Keywords-** DES (Data Encryption Standard) algorithm; BLOWFISH algorithm; RSA (Rivest-Shamir-Adleman) algorithm; Java; JCA;*

## 1. Introduction

Cryptography is mostly referred to as "the study of secret data". Cryptography can play a key role in protecting critical information. It also provides mechanisms for authentication and digital time stamping. The original message is called the plaintext, and the abnormal message is called the cipher text. Encryption is the process of converting plain text to cipher text. Decryption is the process of converting cipher text to plain text in the readable form. Key in the encryption algorithm has a pivotal position, if the key was leaked, it means that anyone can be in the encryption system to encrypt and decrypt information; it means the encryption algorithm is useless.

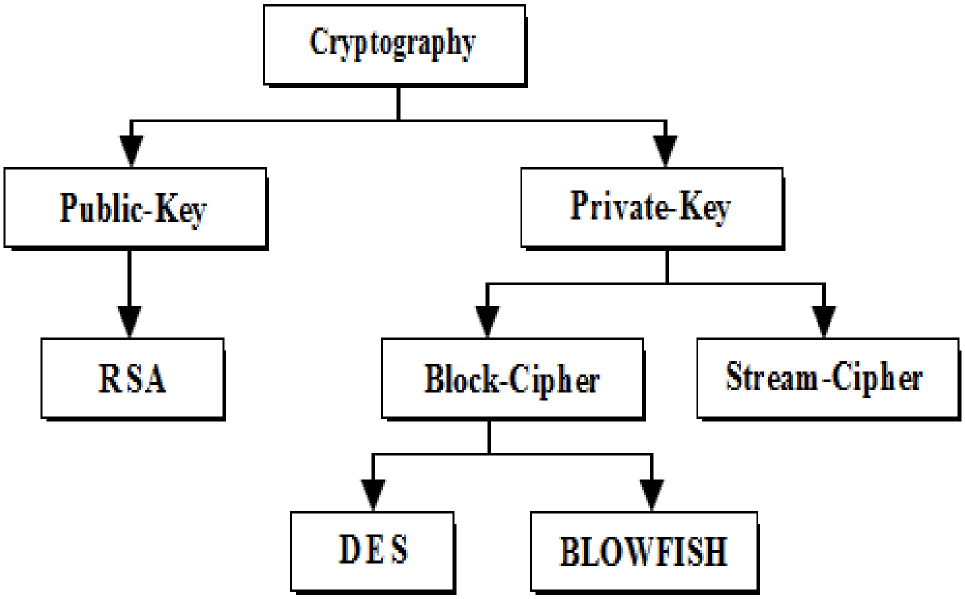

**Figure:** Hierarchy of Cryptography

There are two main types of cryptography in using today – symmetric (or conventional) or secret key cryptography and asymmetric (or public-key) or public key cryptography. Symmetric algorithms are designed in a way such that any two parties interested in encrypting/decrypting data have to use the same (secret) key generated for both encryption and decryption. Encryption algorithms may consume a huge amount of system resources for generating the secret key and for the actual work needed for encrypting or decrypting the data. RSA is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Microsoft and Netscape. At present, the best known and most widely used public key system is RSA, which was first proposed in paper "A method for obtaining digital signatures and public-key cryptosystems". A digital signature binds a document to the processor of particular key, while a digital time stamping binds a document to its creation at a particular time. Cryptography is the science of creating and using such cryptosystems. RSA Asymmetric key cryptosystem is one of the most typical ways that most widely use for public key cryptography in encryption and digital signature standards. One Asymmetric Cryptography has been selected for the work in this paper: RSA. Symmetric key cryptography is the oldest type whereas asymmetric cryptography is only being used publicly since the late 1970's. Symmetric algorithms can be divided into two categories: Block Ciphers[1] and Stream Ciphers[2]. The block ciphers operate on data in groups or blocks. On the other hand, stream ciphers only operate on a single bit at a time which makes them more suitable for real time applications such as multimedia. Two Symmetric Cryptography have been also selected for the work in this paper: (DES) and BLOWFISH.

## 2. RSA Algorithm

The RSA is an asymmetric (public key) cryptosystem based on number theory, which is a block cipher system. Once the keys have been developed, the existing prime numbers are no longer useful and can be discarded. Both the public and the private keys are used for encryption /decryption but only the owner of a private key ever needs to know it. Using the RSA system, the private key never uses to be sent across the Internet. The private key can not be derived from the public key, that enables the publication of the encryption key without the risk of leaking the secrets The most significant approach of public key cryptography algorithm is RSA, which can resist almost all the known passwords attacks so far.

Introduced at the time when the era of electronic email was expected to soon arise, RSA implemented two important ideas:
1. Public-key encryption: This idea omits the need for a "courier" to deliver keys to recipients over another secure channel before transmitting the originally-intended message. In RSA, encryption keys are public, while the decryption keys are not, so only the person with the correct decryption key can decipher an encrypted message
2. Digital signatures: The receiver may need to verify that a transmitted message actually originated from the sender (signature), and didn't just come from there (authentication). This is done using the sender's decryption key, and the signature can later be verified by anyone, sing the corresponding public encryption key[3].

In the algorithm, two large prime numbers are used for constructing the public key and the private-key. It is estimated that the difficulty of guessing the plaintext from signal key and the cipher text equals to that decomposition of the product of two large prime Numbers. RSA public key cryptosystem is one of the most typical ways that most widely use for public key cryptography in encryption and digital signature standards [4]. The private key is used to decrypt text that has been encrypted with the public key. Not only can RSA be used for encryption, but also can be used for authentication. Comparing with Hash signature, in public key algorithms, the generated signature key is stored only on the user's computer, so the safety is at a certain level [5,6].

## 3. DES Algorithm

DES is a block cipher that takes a plaintext string as input and creates a cipher text string of the same length. It uses a symmetric key, which means it involves the use of only one key which is used for both encryption and decryption. A public key algorithm such as RSA uses different keys for encryption and decryption. Private Key algorithms are generally much faster than public key algorithms. The DES was published by the United State's National Bureau of Standards in January 1977 as an algorithm to be used for unclassified data [7]. DES is the most widely used open standard cryptosystem, offering excellent performance. During last two decades, DES has shown noticeable signs of aging. The DES block size is 64 bits. The key size is also 64 bits, although 8 bits of the key are used for parity (error detection), which makes the effective DES key size 56 bits. A 56- bit key length is now considered weak due to advances in computer processing power. The 16-round Feistel network, which contains the cryptographic core of DES, splits the 64- bit data blocks into two 32-bit words, respectively denoted $L_i$ (for left) and $R_i$ (for right). The initial status of these two blocks is denoted $L_0$ and $R_0$. The 32 bits of the $R_0$ block are expanded to 48 bits thanks to a table called an expansion table (denoted E),in which the 48 bits are mixed together and 16 of them are duplicated. In each round, the second word $R_i$ is fed to a function f.

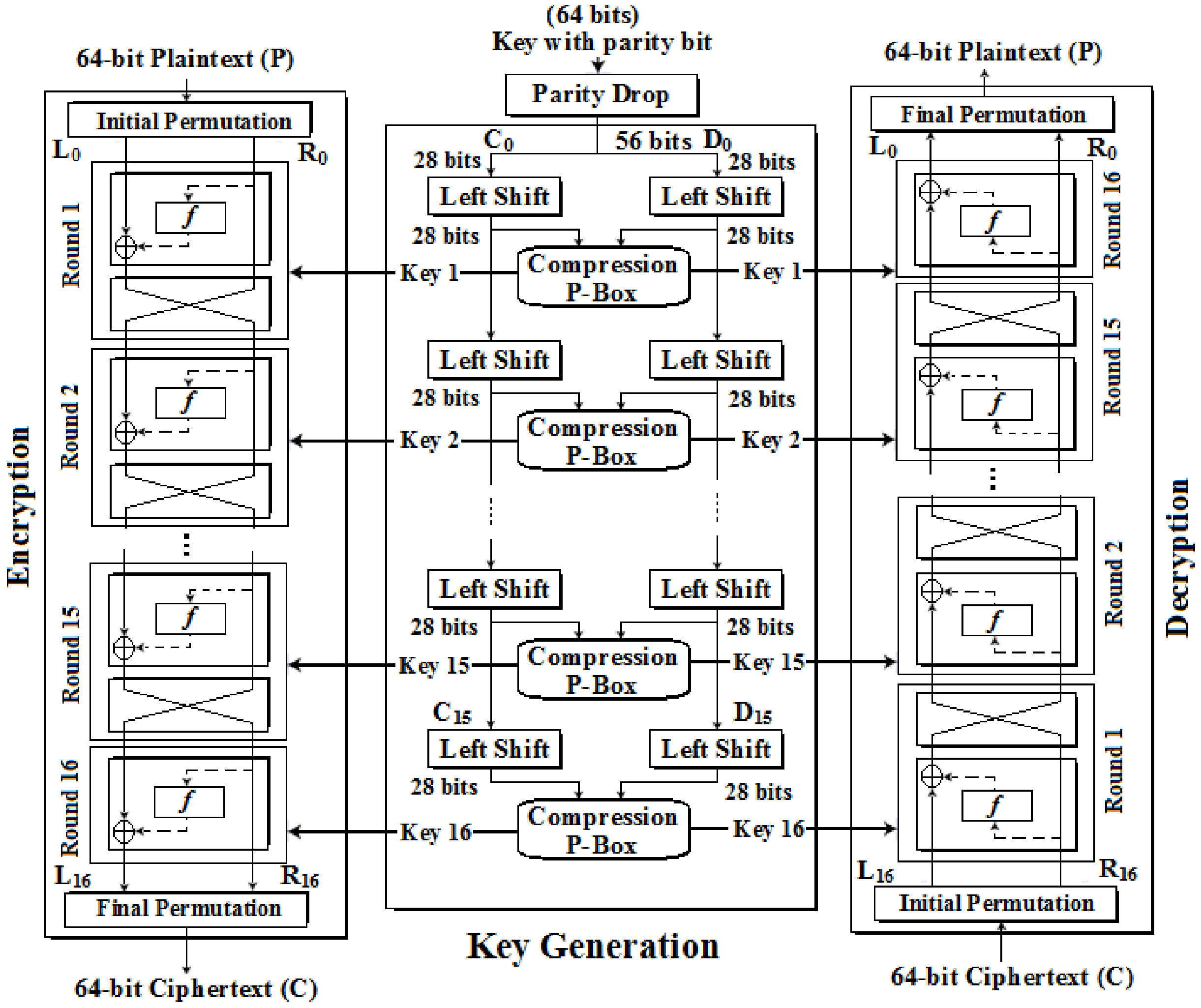

**Figure:** DES Overall Structure

The function f of DES algorithm operates on half a block (32 bits) at a time and consists of four stages:

**1. Expansion (E):** The 32-bit input word is first expanded to 48 bits by duplicating half of the bits and reordering.[8]
**2. Key mixing:** The result is combined with a Subkey using an XOR operation by selecting 48 bits from the 56-bit secret key, a different selection is used in each round.
**3. Substitution:** The 48-bit block is split into eight 6-bit words which are substituted in eight parallel 6×4-bit S boxes. All eight S boxes are different but have the same special structure.
**4. Permutation (P):** The resulting 32 bits are rearranged according to a fixed permutation before being sent to the output.

A 56-bit key length is now considered weak due to advances in computer processing power. With proper hardware, a brute force attack that systematically attempts all 256 (72 quadrillion) different DES keys is possible.

## 4. BLOWFISH Algorithm

Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Bruce Schneier as a fast, free alternative to existing encryption algorithms designed blowfish in 1993[9]. Blowfish is unpatented and license-free, available free and one of the fastest block ciphers in world widely use. Blowfish is a variable-length key block cipher. The Blowfish is a cipher with a different structure and functionality, and has the advantages of low memory requirement and has a simple structure. Blowfish algorithm is suitable and efficient for hardware implementation and hence both hardware and software implementations can be compared. In this 64-bit plaintext message is first divided into 32 bits. The 'left L' 32 bits are XORed with the first element of a P array to create a value called P', run by a transformative function called F, then XORed with the 'right R' 32 bits of the message to produce a new value called F'.

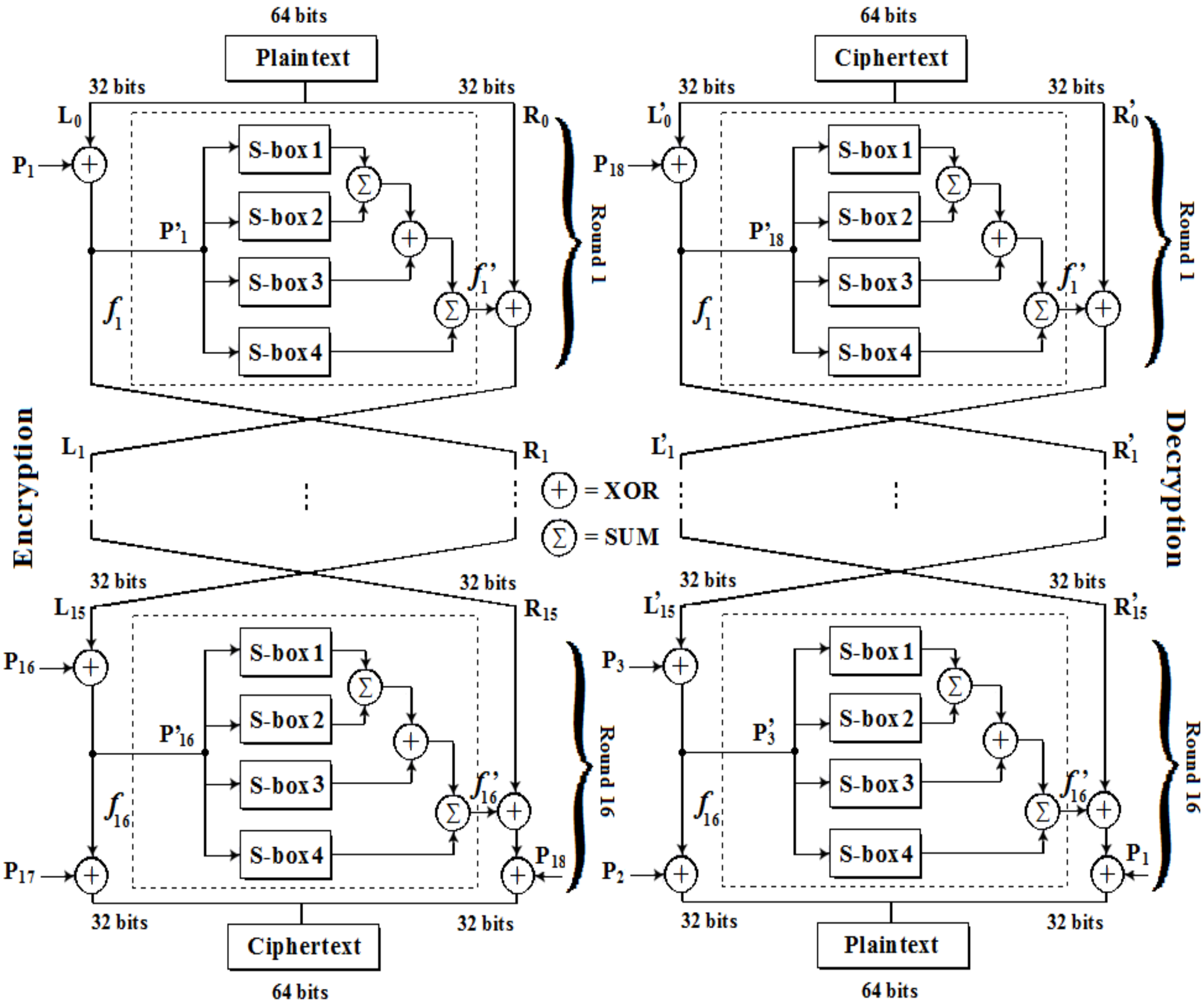

**Figure:** Blowfish Overall Structure

F' then replaces the 'left L' half of the message and P' replaces the 'right R' half, and the process is repeated 15 more times with successive members of the P array. The resulting P' and F' are then XORed with the last two entries in the P array (entries 17 and 18), and recombined to produce the 64-bit ciphertext [10]. The function divides a 32-bit input into four bytes and uses those as indices into an S array. The results are then summed and XORed together to produce the output. Because Blowfish is a symmetric algorithm, the same procedure needed for decryption as well as encryption. The only difference is that the input to the encryption is plaintext; for decryption, the input is cipher text. The P array and S array values used by Blowfish are precomputed based on the user's key. In effect, the user's key is transformed into the P array and S array; the key itself may be discarded after the transformation. The P array and S array need not to be recomputed, but must remain secret.

## 5. Experimental Set-up

Here discussion over Java Cryptography Architecture (JCA) and provide knowledge about structure of the selected cipher algorithms and their implementations.

### JAVA Cryptography Structure(JCA):

The Java Cryptography Architecture (JCA) is a framework for working with cryptography using the Java programming language. It forms part of the Java security API, and was first introduced in JDK 1.1 in the "java.security" package[11]. The powerful portable programming language Java and JCA is used in the implementations.

### Program Implementation:

A secret key has to be generated for each cipher algorithm. The implemented program is constructed into two modules. The first module is the encryption module that takes a secret key generated for the same cipher algorithm and uses this key to encrypt a message (e.g. "vaibhav" which is used in this paper's result). The decryption module is the second module that takes a secret key and decrypts a message. The message will be decrypted successfully only if the key used for decryption is same as use in encryption. In implementation of Encryption and Decryption based on three times with respect to cryptographic algorithms.

"User time": is the time spent running your application's own code.

"System time": is the time spent running OS code on behalf of your application (such as for I/O).

"CPU time": is user time plus system time. It's the total time spent using a CPU for your application. The CPU execution time is broken down to kernel and user time.

The program also does not interact with the user while it is running, instead it expects all of the required parameters to be supplied when invoking the application. This is necessary to obtain accurate measurements of the time spend on each operation The three algorithm were tested on 64 bit - Microsoft windows 7 Operating System and CPU speed of 2.10 GHz with total installed memory(RAM) 2GB.

## 6. Results

DES and Blowfish, two symmetric key encryption algorithms which commonly used for network data encryption. One plain text works on all of these algorithms. Encryption applies on all of these algorithms to convert a plain text into cipher text. Encrypted data is produced by RSA, DES and Blowfish algorithms. Encryption is easily shown in diagram using java and JCA. There is no need for providing any prime numbers for RSA algorithm in java and JCA. It takes automatically using JCA tools. If Key value will be change the entire encrypted data also change for all encrypted algorithm. Here time occurred in nanosecond using JCA and JAVA, but in this paper discussion placed in seconds. The major difference between these algorithms is the CPU time spent while performing the encryption and decryption operations. It is clear, as illustrated in the figure, that the Blowfish algorithm is the fastest algorithm due to the above modules it follows for ciphering data. Second fastest is the DES algorithm by above module mechanism using same data then RSA algorithm.

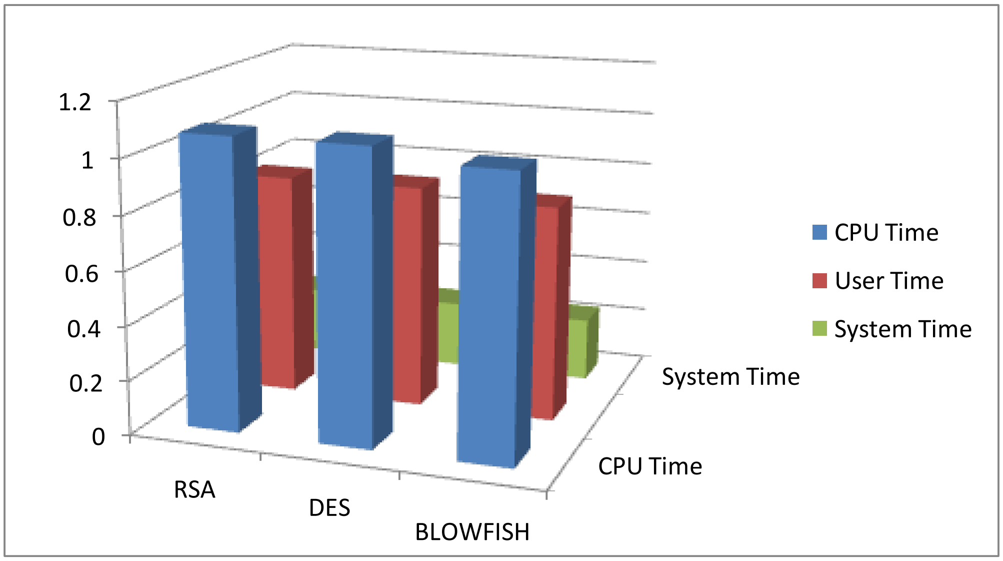

**Figure :** Compare Performance by Times in Encryption Module

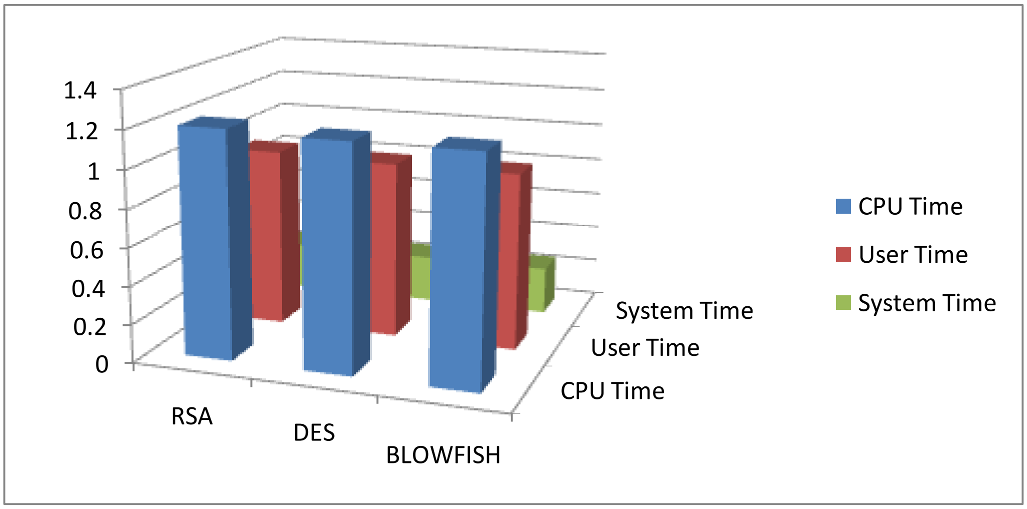

**Figure**: Compare Performance by Times in Decryption Module

## 7. Conclusion and Future Scope

In this paper we presented an implementation of three encryption algorithms using Java and JCA. Two encryption algorithms are in category of symmetric cryptosystem that is DES and BLOWFISH and One encryption algorithm is in category of asymmetric cryptosystem that is RSA. The main objective was to evaluate which one is better for encryption and decryption of these algorithms using Java and JCA in terms of CPU execution time. Conclusion for the same set of data BLOWFISH algorithm is better than DES and RSA algorithm, while DES is better than RSA[12]. The measurements were performed on MicrosoftOS platform. The results obtained may help in the selection of the appropriate encryption algorithm to use for software implementation. In order to increase the speed of these algorithms we propose to have a built-in cipher module within the processor dedicated for security considerations. In future implementation of these three encryption algorithms can be analysis in better simulators to get better results. This encryption analysis can be done in another simulator which is like MATLAB, ns2, ns3, OPNET etc. by taking networking into consideration to show which algorithm performs better in network. For cryptographic applications these simulators will give better results in network.

## Reference

[1] M. J. B. Robshaw, "Block Ciphers", Technical Report, RSA Laboratories, Number TR - 601, July 1994.

[2] M. J. B. Robshaw, "Stream Ciphers" Technical Report, RSA Data Security, Inc., Number TR-701, p. 46, July 1995.

[3] RSA, Introduction to encryption with RSA,[online] pdf information 2013, http://www.math.washington.edu/~morrow/336_09/papers/Yevgeny.pdf.

[4] W. Stallings, Cryptography and Network Security: Principles and Practices, 5th ed., Prentice Hall, 1999.

[5] Rivest, R. L., Shamir, A., Adelmann, L.: "A method for obtaining digital signature and public –key cryptosystems", Commun. ACM, 1978, VOL. 21, pp. 120-126.

[6] Dorothy E. Denning, Digital Signature with RSA and Other Public-Key Cryptosystems, Communications of the ACM, 1984.

[7] National Bureau of Standards. FlPS PUB 46: Data Encryption Standard, January 1997.

[8] DES, Introduction to encryption with DES,[online] Nov 2012, http://en.kioskea.net/contents/crypto/des.php3 (Accessed : 24 April 2013).

[9] Bruce Schneier, "The Blowfish encryption algorithm9", Dr. Dobb's Journal of Software Tools, 19(4), p. 38, 40, 98, 99, April 1994.

[10] "Encryption using the blowfish algorithm", www.cryptosys.net & www.dimgt. com.au, 2002.

[11] Definition of JCA,[online] may 2013,http://en.wikipedia.org/wiki/Java_Cryptography_Architecture.

[12] vaibhav shrivastava, " Computer trends with security by RSA, DES and BLOWFISH algorithm ", International paper, International journal of computer science and technology, Vol 4 Issue 2, July 2013.