IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-3, March 2019 E-ISSN: 2347-2693

A Survey on Cryptographic Algorithms and their implementation over Advanced Computer Architectures

Aditya Sahu[1], Md Tausif Zafar[2], Nishi Yadav[3*]

[1,2,3]Department of CSE, School of Studies in Engineering and Technology, Guru Ghasidas Vishwavidyalaya, Bilaspur, India

[*]*Corresponding Author: nishidv@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v7i3.375383 | Available online at: www.ijcseonline.org

Accepted: 22/Mar/2019, Published: 31/Mar/2019

Abstract— Due to the increase in digitalization of sectors like health, banking, e-commerce, education, stock marketing, etc. it is required to share personal as well as sensitive information over the internet. And to protect this information over the Network, various cryptographic algorithms are needed for safe data communication. Mainly, this survey paper consists of two parts. In the first part, we did the comparative analysis of important encryption and decryption algorithms like AES, Blowfish, RSA, DES, 3DES, RC with respect to different attributes such as key size, number of rounds, algorithm structure, block cipher, block size, features, flexibility, security, and attacks. In the second part of this paper, we dealt with the practical implementation of most popular encryption algorithms like AES, Blowfish and RSA over different computer architectures and to check their performance in different Intel processors. The performance is analysed in terms of time taken for encryption and decryption of processes in milliseconds.

Keywords— AES, Blowfish, RSA, Encryption, Decryption, Intel processor

I. INTRODUCTION

Day by Day, our world is being digitalized and everything which was done earlier manually is being done by software today. Whether its cab booking, online food ordering, transferring money or even important tasks like sending any security-related sensitive information, everything is being done with the help of Network. In today's world, the exchange of important data and documents over the internet is increasing at a very high rate. But with the increase in these advancements, the need for security of that data and information being shared is also needed. There is a need for the security services like access control, authentication, confidentiality and integrity of the data. And with the rapid advancement in technology day by day, there is a great risk of our data getting hacked. And, if it goes into the wrong hands, any unforeseen circumstances can occur. Hence, Network Security is of utmost importance today. And, when it comes to the study of Network Security, the Encryption and Decryption of data plays a major role in the transfer of data from one point to another securely. Therefore, the knowledge in cryptography is one of the most demanded skills today in the world of Information Technology. With time, better cryptographic algorithms are being developed and upgraded in order to provide the best algorithm required under given circumstances in order to make them more efficient. So, to enhance security, the study of various cryptographic algorithms is necessary for comparing and selecting the best cryptography algorithm according to our needs.

Cryptography is a science of secret writing [1]. It is the art of protecting the information by transforming it into an unreadable format in which a message can be concealed and only the intended recipient will be able to convert it into the original text. Its main goal is to keep the data secure from unauthorized access. The original message that needs to be sent or the data that can be well understood without any kind or special measures is called plaintext. Encrypting plaintext results in any random format called ciphertext. The process of converting from plaintext to ciphertext is known as enciphering or encryption [1]. The process of restoring the plaintext from the ciphertext is called deciphering or decryption. A system which provides encryption and decryption is called cryptosystems.

A. Goals of Cryptography

Here are the five major goals of cryptography [2]. These are as follows:

- *Confidentiality:* To ensure that every bit of data is being kept a secret is the major goal of Security Systems. By converting the plaintext into ciphertext, the original meaning of the message is hidden. With a proper key,

the sender encrypts the message, so that only the intended receiver can decrypt and read the message.

- *Integrity:* Integrity means to make sure that the message received by the receiver is not being altered in between and is the same message which the sender has sent. To create a unique message digest from the message which is sent along with the message, we make use of hashing. The same technique is used by the recipient to create a second digest to compare with the original one.
- *Authentication:* Authentication is the process of proving the identity of the system.
  It is accomplished using digital certificates.
- *Non-Repudiation:* It is a mechanism which ensures that both the sender and receiver acknowledge the delivery of the report.

B. Encryption and Decryption

Encryption can be termed as the process of changing plain text data into a different format called ciphertext which appears to be random and meaningless. The process of restoring plaintext from ciphertext is also called decryption of deciphering [1].

Each and every encryption algorithm is designed with the goal of making the process of decryption of the generated ciphertext as difficult as possible when done without possessing the valid key. In case of a good encryption algorithm, the only technique which is better than all others to decrypt the generated ciphertext is methodologically trying every possible key in order to get the valid key by chance. In these kinds of algorithms, when the key is chosen is longer, it becomes more and more difficult to get the original plaintext from ciphertext without possessing the key.

C. Symmetric and Asymmetric Encryptions:

On the basis of security keys used to encrypt or decrypt the data, there are two main categories of cryptography which are described below:

1) *Symmetric Encryption:-*

It is also called single key cryptography because only a single key is used in it [2]. The sender and the receiver agree upon a single secret (shared) key in this process of encryption. Encryption encodes the original message (also called plaintext) and produces meaningless data out of it. The same key which is used for encryption is used for the process of decryption.

2) *Asymmetric Encryption:-*

It is also termed as public key cryptography. Two different keys are used in Asymmetric Encryption: the public key and private key [2]. The public key is known to the public and is used for encryption. The private key is only known by the user of that key and is used for decryption. The public and the private keys are related to each other by any mathematical means. In other words, data encrypted by one public key can be encrypted only by its corresponding private key.

D. Various Cryptographic Algorithms:

1) AES:- AES stands for Advanced Encryption Standard. It is also known as Rijndael [2]. In 2001, It was recommended by NIST in order to replace DES. The developers of AES were Vincent Rijmen and Joan Daemen. By using symmetric key length of 128, 192, and 256 bits, any combination of data (128 bits) can be supported by it. During encryption-decryption process, To retrieve the original plaintext or to deliver the final ciphertext, AES system goes through 10,12 and 14 rounds respectively for I28-bit, I92-bit, and 256-bit keys during the process of encryption and decryption [1,3].

Each round of AES is governed by these four transformation functions, except the last round is slightly different. 4x4 matrix of bytes array are as state in these operation function. Four different rounds in AES are as follows [3,4]:

Byte substitution: A non-linear byte by byte substitution is applied with the help of substitution matrix(S-Box).

Shift rows: It involves simple byte transposition where the left shifting of the last three rows in a circular way is done depending on the offset of row index. For 2^{nd}, 3^{rd} and 4^{th} row, 1, 2 and 3-byte circular left shifts are performed respectively [3].

Mix columns: It is very similar to a matrix multiplication of each column. With each column vector, We multiply a fixed matrix. Each byte in the column is converted to a novel value which depends on the value of the other four bytes in the same column.

Add round key: It is a simple bitwise XOR operation between the present state and the round key.

Advantages of AES:-

The most basic advantage of AES is that it is very common. It is supported by most vendors since it is defined as the standard used by the US government.

Disadvantages of AES:-

The disadvantage of AES is that it has a very simple key schedule and simple encryption operations. Many of its attacks are based upon the simplicity of this key schedule.

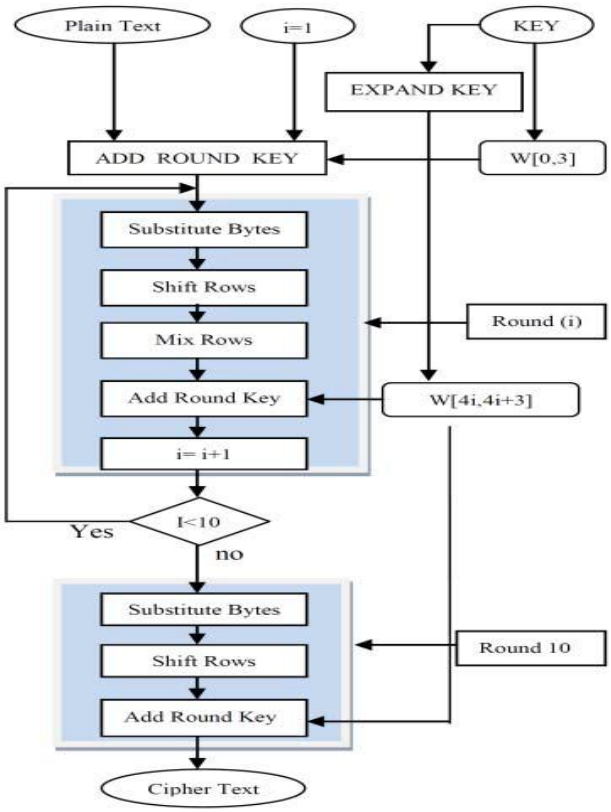

Figure 1. Process of AES (Advanced Encryption Standard) [4]

2) RSA:- RSA is named after its founders Ron Rivest, Adi Shamir, and Leonard Adleman. RSA is designed in 1978 and is one of the first practical public-key cryptosystem [3]. Two keys are generated in it: the public key for encryption and private key to decrypt the message. This algorithm is one of the prominent public key encoding systems for key exchange. It uses a variable size key and a variable size encryption block. It is executed in three steps, first is the generation of the key which is to be used as a key for encryption and decryption.The second step is the process of encryption in which there is the conversion of the plaintext into ciphertext. The third step and the last step consists of decryption, where the encrypted text is converted into plain text. RSA is not commonly used to encrypt user data directly as it is a relatively slower algorithm.

These are the following three steps followed in the implementation of the RSA algorithm:-

Key generation: To enable B to send his encrypted messages, A transmits his public key (n, e) to B via a reliable, but not necessarily secret route. The private key d is not distributed [1].

Following are the Steps used for Key generation [5]:

1. Two large random prime numbers whose sizes are approximately equal are selected. Let they are p and q. And the product, n = p*q is desired bit length.
2. We Compute Ø(n) = (p – 1) * (q – 1).
3. A positive integer e is chosen such that 1 < e < Ø(n), and GCD (e, Ø(n)) = 1.
4. The value of secret Exponent d is computed, where 1 < d < Ø(n), such that e * d = 1(mod Ø(n)).
5. The public key is the pair (e, n) and the private key is the pair (d, n). The values of q, d, p and Ø(n) should be kept as a secret.

Where,

- e is the encryption exponent or public exponent.
- n is the modulus.
- d is the decryption exponent or secret exponent.

Encryption:-
Steps used for Encryption:

1. Obtain the public key (e, n).
2. Represent the plaintext as positive integer m.
3. Compute the ciphertext c = me mod n.
4. Sends the ciphertext c.

Decryption:-
Steps used for Decryption:

1. Use private key (d, n) to compute m = cd mod n.
2. Extract the plaintext from message m.

The only difficulty in RSA is to factorize the modulus n into its prime factors p and q when p and q are very large prime numbers.

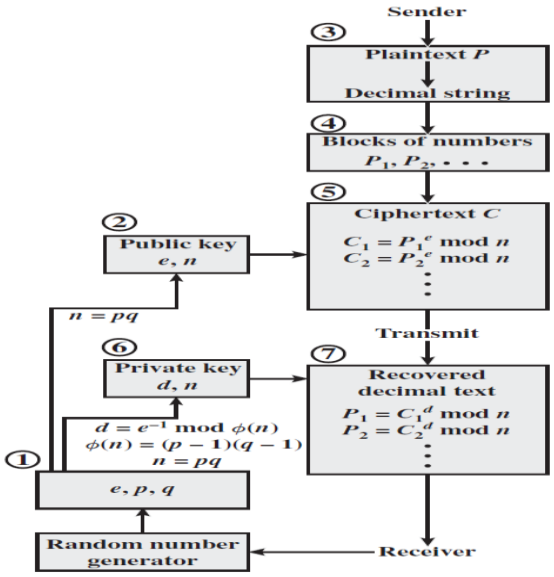

Figure 2. Workflow of RSA Algorithm [1]

3) Blowfish :-

In 1993, Blowfish was first introduced [2]. Blowfish is a symmetric block cipher. It takes a key of variable length from 32 bits to 448 bits, and block size of 64 bits. These are a few of the characteristics which make the Blowfish Algorithm, an ideal algorithm for securing data. Blowfish was designed by Bruce Schneier in order to provide a free and a fast alternative to various encryption algorithms which existed earlier. Most of the encryption algorithms are not available for the public and are protected by patent. But Blowfish is license-free and is not patented. Blowfish is available free for all uses [6]. Blowfish is a Feistel structure which consists of 16 rounds shown in Figure 3. No attack is known to be successful against it, even though it suffers from weak keys problem [2].

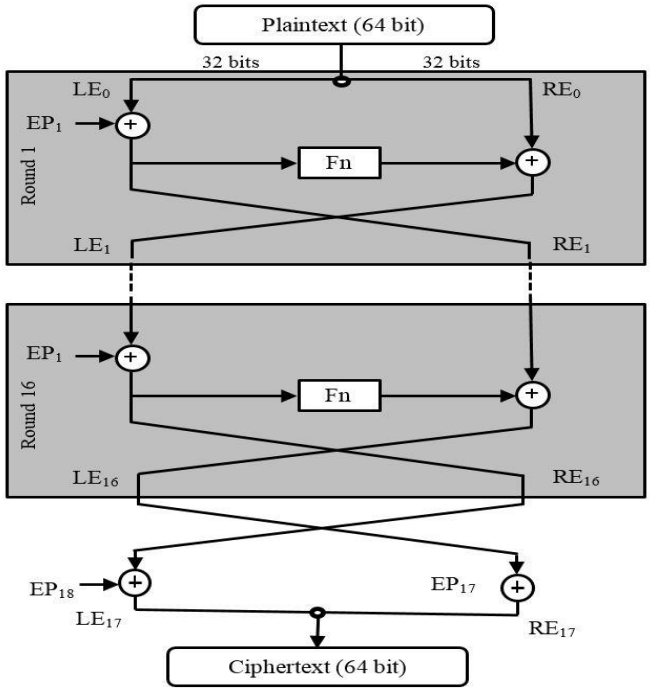

Figure 3. Blowfish Encryption algorithm [6]

Advantages:-

Except when changing keys, Blowfish is one of the fastest block ciphers in general use. Blowfish is not subject to any patents and is therefore freely available for anyone to use and therefore, it is popular.

Disadvantages:-

The disadvantage of Blowfish is that it must get key to the person out of band specifically not through the unsecured transmission channel. With the increase in the number of users, the management of keys becomes complicated since each pair of user needs a unique key. Its decryption process is time-consuming and is serial in throughput.

4) DES:-

DES is the earliest symmetric encryption algorithm developed by IBM in 1972 and adopted in 1977 as Federal Information Processing Standard (FIPS) by the National Bureau of Standard (NBS) which is currently the National Institute of Standards and Technology (NIST) that evaluate and implement the standard encryption algorithm [6]. It takes a key of length 56 bits and block size of length 64 bits. It includes 64 bits key from which 56 bits are directly utilized by the algorithm as key bits and are randomly generated. The remaining 8 bits that are not used by algorithm because it is used for the error detection as set to make a parity of each 8-bit byte [6].

5) 3DES:-

In 1998, IBM firstly proposed Triple Data Encryption Standard (3DES) which is also referred to as the Triple Data Encryption Algorithm (TDEA) . The Triple Data Encryption Algorithm (TDEA or 3DES) was developed to tackle the flaws in DES whilst preserving the same cryptography [5]. 3DES appeared as the replacement of DES due to the improvement in the key length and applies the DES algorithm to the three times in each data block [6]. Earlier, the key length of DES algorithm was adequate at the time of design of the algorithm but as when day by day the computation power is increasing, the brute force attack is feasible. Also, 3DES provides a very simple method by the increment of key length instead of design a complete block cipher [6]. The 3DES also gives protection against the brute force attack, which is the way of continuously trying every possibility and different combinations while accessing keys until one gets successful.

The key length for the 3DES is 112 bits and 168 bits, the number of rounds 48 and the block size is 64 bits [3]. The main objective of this algorithm is to increase the security with a longer key length, so it is challenging to predict the pattern. 3DES algorithm is preferred as compared to the DES algorithm because the 3DES algorithm is three times secure having key size 2^{168} (use keys as a combination or each level with different keys size) as compared to DES algorithm having key size 2^{56}. Although it provides more security but, it also consumes more time in encryption process while being compared to the time consumed by DES algorithm.

6) RC4:-

RC4 is a variable key size stream cipher and symmetric key encoding algorithm which was designed by Ron Rivest in 1987. It is officially termed as "Rivest Cipher 4". As it is a stream cipher, it is more efficient for real-time processing. For both Encryption and Decryption processes, the same algorithm is used as the data stream is simply XORed with the generated key sequence. RC4 takes a variable key length of 128,192 or 256 bits [7].

The algorithm is simple, fast and easy to explain. It can be efficiently implemented in both software and hardware. The algorithm can be broken into two stages: initialization, and operation. In the initialization stage the 256-bit state Table, S is populated, using the key, K as a seed. Once the state Table is set up, it continues to be modified in a regular pattern as data is encrypted.

7) RC6:-

RC6 is a block cipher that applies 128-bit block size and provides 128, 192 and 256-bit key sizes. It was designed in 1997. Additionally, RC6 aims to meet the demands of AES. It offers more security from attacks than what RC5 offers, so many times, it is considered better than RC5. RC6 uses four registers. It also needs fewer rounds and gives more throughput [5].

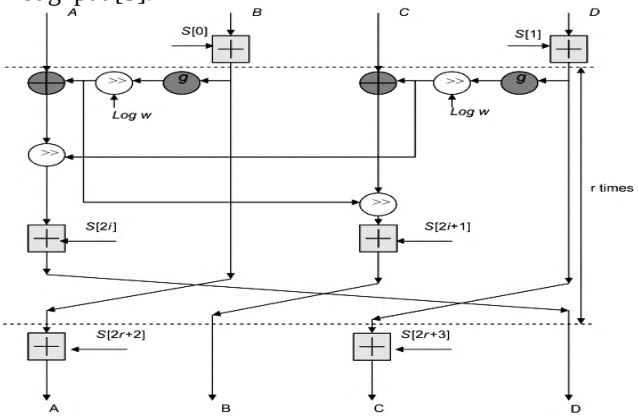

Figure 4. The RC6 Encryption Algorithm [5]

In this paper, Section I contains the introduction of various terminologies related to cryptography and describes various cryptographic algorithms like AES, Blowfish, RSA, DES, 3DES, RC4, and RC6, Section II contains the result of the related works of Nidhi Singhal who did the comparative study of AES and RC4, and the work done by Tingyuan Nie is also studied, Section III contains the proposed works of this paper, in which three cryptographic algorithms AES, RSA, and Blowfish are implemented over advanced computer architectures(Intel-i3, Intel-i5, and Intel-i7), Section IV contains the result and discussion of the proposed work and this section also contain the comparative analysis of AES vs Blowfish algorithms, Section V contains Conclusion and Future Scope of this implementation.

II. RELATED WORK

Several works have been done in the past to find out which algorithm would best suit for our various purposes like being fast, secure and reliable. The work presented by Nidhi Singhal and J.P.S. Raina [7] shows that when a performance evaluation was done for RC4 and AES algorithms, RC4 was found energy efficient and fast for encryption and decryption. In this evaluation, the performance metrics were CPU process time, memory utilization, throughput, encryption and decryption time and key size variation. Hence, in that comparison, RC4 was found better than AES.

Table 1. Comparison of Various Cryptographic

Algorithms	Created By	Year	Key Size (Bits)	Block Size (Bits)	Number of Rounds	Algorithm Structure	Feasible	Security and Feature	Attacks
DES	IBM	1975	64	64	16	Feistel	No	Not strong enough	Brute force attack
3DES	IBM	1998	112 Or 168	64	48	Feistel	Yes	Adequate security & slow speed	Brute force attack
RSA	Rivest Shamir Adleman	1977	1024 To 4096	128	1	Public key Algorithm	No	Excellent Security & slow speed	Random Fault Attacks, Blinding Attacks
AES	Vincent Rijmen, Joan Daemen	2001	128,192, 256	128	10,12, 14	Substitution Permutation	Yes	Excellent Security & fast speed	Side Channel attack
Blowfish	Bruce Schneier	1993	32-448	64	16	Feistel	Yes	Excellent Security	Dictionary attack

								& fast speed	
RC4	Ron Rivest	1987	Variable	40-2048	256	Feistel Stream	Yes	Fast Cipher	Klein's attacks. Royal Holloway attack
RC6	Ron Rivest	1998	128 to 256	128	20	Feistel	Yes	Good security	Statistical attack

Algorithms

Similarly, the work presented by Tingyuan Nie [8], compared DES and Blowfish and evaluated encryption function speed with different memory sizes. On observing the experimental results, it is shown that Blowfish is much faster than DES but the increase in speed for Blowfish is slower compared to DES because it needs much more memory for Sboxes initialization and sub-keys.

The work done by Singh et al. [9] compared the different symmetric algorithms including the DES, 3DES, AES, and Blowfish. It was found that Blowfish was the best amongst the other methods despite their popularity in the field of encoding and decoding. It was also found that the AES algorithm needs higher processing time in comparison to other algorithms.

III. PROPOSED WORKS

ANALYSIS OF DIFFERENT CRYPTOGRAPHIC ALGORITHMS OVER THE ADVANCED COMPUTER ARCHITECTURES

This section is based on the practical implementation of different network security (encryption and decryption) algorithms over different computer architectures. The main motto of this analysis is to check the performance of data encryption and data decryption processes over modern day computers. In this paper, the proposed works are based on the practical implementation of different network security algorithms like AES (Advanced Encryption Standard), RSA and Blowfish over the different modern-day advanced Intel processors which are:

1) *Intel-i3*- (Intel(R) Core(TM) i3-5005U CPU @ 2.00GHz with 4GB RAM),
2) *Intel-i5*- (Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz with 8GB RAM)
3) *Intel-i7*- (Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz with 16GB RAM)

WINDOWS 10 operating system is used in all the computer systems. For RSA, the input data size is taken in bytes (50, 100, 150, 200 & 250). For AES and Blowfish, files are taken as plain text which are of size measured in kilobytes.

AES IMPLEMENTATION WORKS

Table 2. AVERAGE ENCRYPTION TIME AND DECRYPTION TIME ON DIFFERENT INTEL PROCESSORS

File Size (KB)	Encryption Time (milliseconds)			Decryption Time (milliseconds)		
	Intel-i3	*Intel-i5*		*Intel-i3*	*Intel-i5*	
20 KB	687.00	97.75	**20 KB**	687.00	97.75	**20 KB**
40 KB	703.00	99.33	**40 KB**	703.00	99.33	**40 KB**
80 KB	709.00	101.57	**80 KB**	709.00	101.57	**80 KB**
120 KB	719.00	105.3	**120 KB**	719.00	105.3	**120 KB**
160 KB	734.00	110.00	**160 KB**	734.00	110.00	**160 KB**

This Table 2 shows that the average encryption time and decryption time of AES algorithm at different input files size executing on different Intel processors. Every file contains the same sort of data in different sizes as 20KB, 40KB, 80KB, 120KB and 160KB.

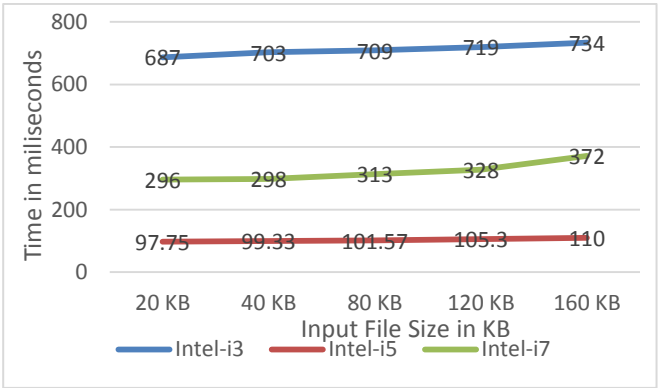

Figure 5. AES Encryption Time graph using different Intel Processors

From Figure 5. it is clear that Intel-i5 processor with 8 GB RAM has minimum encryption time (milliseconds) for all files size, it took a range of 97.75 - 110 milliseconds time to execute the encryption process for different files size ranging between 20KB-160KB which is approximately 2-3 times lesser than Intel-i7 processor and 5-7 times lesser than Intel-i3 processor. Every cryptographic algorithm took less encryption time and decryption time in order to make the encryption and decryption scheme faster and responsive [6].

Hence the performance of AES encryption process in Intel-i5 is very efficient in terms of encryption time as compare to Intel-i3 and Intel-i7.

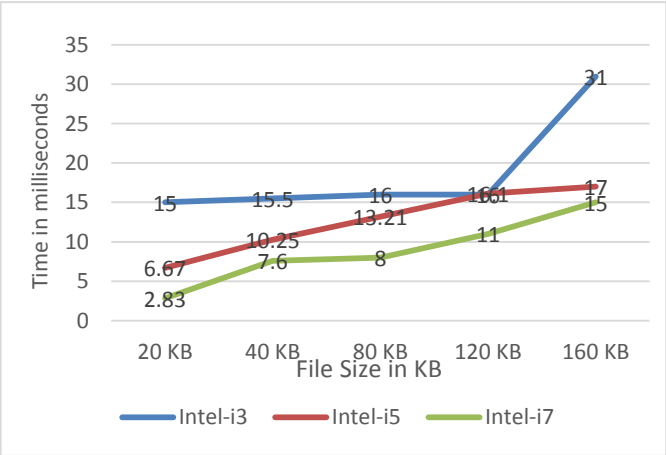

Figure 6. AES Decryption Time graph using different Intel Processors

Figure 6 shows that the Intel-i7 took less time for the decryption process of AES algorithm as compared to Intel-i3 & Intel-i5. In executing a 120KB file, both Intel-i3 and Intel-i5 took approximately the same time (16 milliseconds) but overall Intel-i7 is 2-times faster than Intel-i3 and much faster than Intel-i5 for decrypting the ciphertext into original text.

RSA IMPLEMENTATION WORKS

Table 3. AVERAGE ENCRYPTION TIME AND DECRYPTION TIME ON DIFFERENT INTEL PROCESSORS

Text Size	Encryption Time (milliseconds)			Decryption Time (milliseconds)		
	Intel-i3	*Intel-i5*		*Intel-i3*	*Intel-i5*	
50 Bytes	15.00	3.00	**50 Bytes**	15.00	3.00	**50 Bytes**
100 Bytes	15.00	3.80	**100 Bytes**	15.00	3.80	**100 Bytes**
150 Bytes	16.00	4.00	**150 Bytes**	16.00	4.00	**150 Bytes**
200 Bytes	16.00	4.57	**200 Bytes**	16.00	4.57	**200 Bytes**
250 Bytes	16.00	5.00	**250 Bytes**	16.00	5.00	**250 Bytes**

RSA is an asymmetric key algorithm to encrypt plain text into ciphertext and then decrypt ciphertext into plain text by using public key and private key. RSA has three steps algorithm: key generation, encoding, and decoding. Table 3 shows that plain text is taken as input which are of size 50KB, 100KB, 150KB, 200KB and 250KB respectively. Encryption and decryption time is measured in milliseconds.

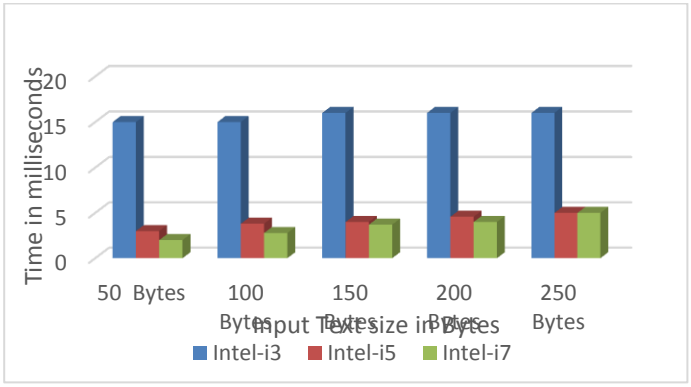

Figure 7. RSA Encryption Time graph using different Intel Processors

Intel-i5 and Intel-i7 took the almost same time for RSA encryption process which converts plain text into ciphertext. On average both Intel-i5 and Intel-i7 took 3-times less encryption time as compared to Intel-i3. Intel-i3 has approximately 15 milliseconds encryption time for all input text sizes.

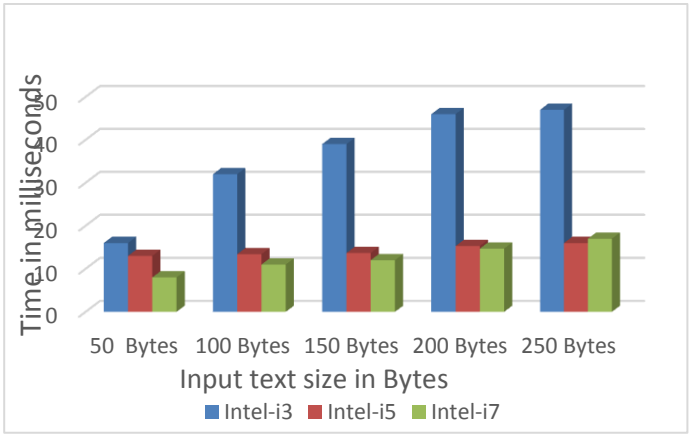

Figure 8. RSA Decryption Time graph using different Intel Processors

This shows that Intel-i5 and Intel-i7 have 2-3 times less decryption time as compare to Intel-i3 processor. For fast and responsive implementation of a cryptographic algorithm, encryption as well as decryption time should be less. These above Figures 7 and 8, show that RSA algorithm would be best implemented in Intel-i5 and Intel-i7 as compared to Intel-i3 in terms of encryption and decryption times of conversion of plain text into ciphertext and ciphertext into plain text again.

BLOWFISH IMPLEMENTATION WORKS

Table 4. AVERAGE ENCRYPTION TIME AND DECRYPTION TIME ON DIFFERENT INTEL PROCESSORS

File Size	Encryption Time (milliseconds)			Decryption Time (milliseconds)		
	Intel-i3	*Intel-i5*		*Intel-i3*	*Intel-i5*	
20 KB	15.00	7.11	**20 KB**	15.00	7.11	**20 KB**
40 KB	22.67	8.86	**40 KB**	22.67	8.86	**40 KB**
80 KB	29.93	15.71	**80 KB**	29.93	15.71	**80 KB**
120KB	32.00	17.00	**120KB**	32.00	17.00	**120KB**
160KB	47.00	22.00	**160KB**	47.00	22.00	**160KB**

This Table shows the time which Blowfish took for encryption and decryption processes over the 64-bit operating system and x64-based Intel processors. Blowfish consists of sixteen rounds. Each round has the XOR process and a task. Also, it is license free, unpatented, free and alternative for the existing encryption algorithms.

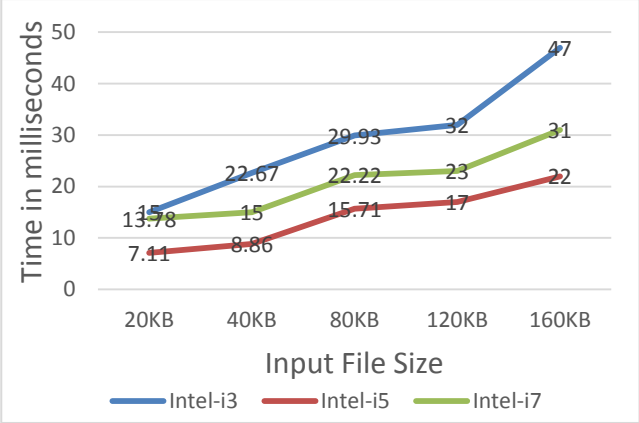

Figure 9. Blowfish Encryption Time graph using different Intel processors

Figure 9 shows that the encryption time for Blowfish algorithm is minimum in Intel-i5 as compared to Intel-i3 and Intel-i7 for the files of all sizes. Also, Intel-i7 gives better performance as compared to Intel-i3.

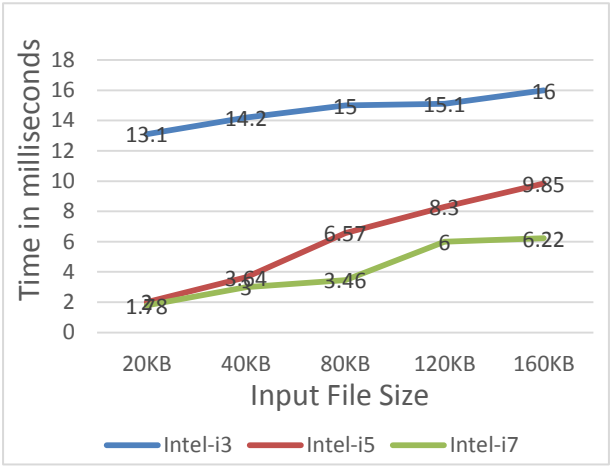

Figure 10. Blowfish Decryption Time graph using different Intel processors

Figure 10 shows that Intel-i5 and Intel-i7 took the same decryption time for 20 KB and 40 KB file but overall Intel-i7 had better performance for 80 KB, 120 KB, and 160 KB files.

IV. RESULT AND DISCUSSION

Analysis of AES Vs Blowfish algorithm with fixed file size (160 KB)

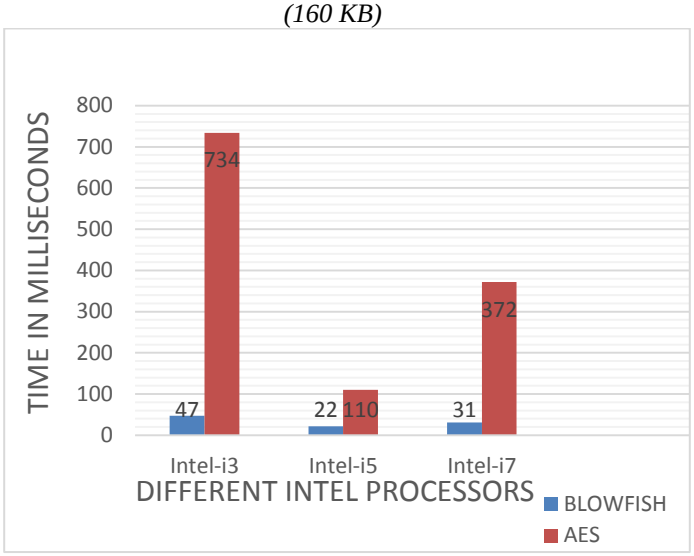

Figure 11. Encryption time of AES and Blowfish after executing a fix file size (160 KB) on different Intel processors

Blowfish took 47 milliseconds in Intel-i3, 22 milliseconds in Intel-i5 and 31 milliseconds in Intel-i7 processors respectively for encrypting the 160 KB file into ciphertext. But AES took 734 milliseconds in Intel-i3, 110 milliseconds in Intel-i5 and 372 milliseconds in Intel-i7 for encrypting the same 160 KB file into ciphertext.

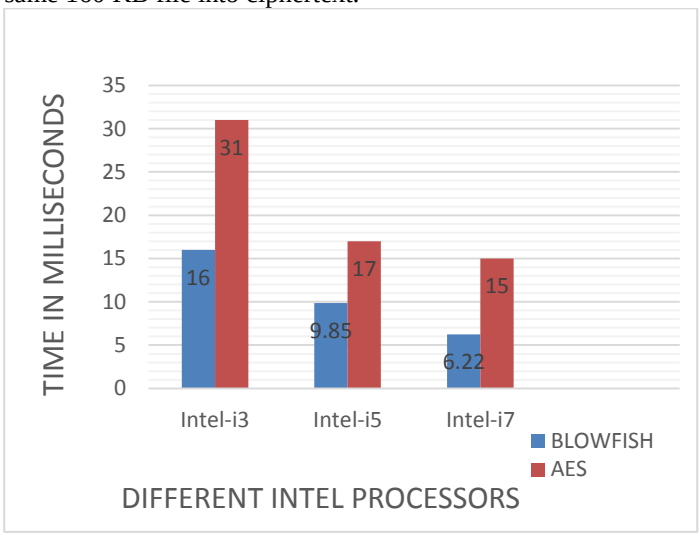

Figure 12. Decryption time of AES and Blowfish after executing a fix file size (160 KB) on different Intel processors

Blowfish took 16 milliseconds in Intel-i3, 9.85 milliseconds in Intel-i5 and 6.22 milliseconds in Intel-i7 for decrypting ciphertext into original text. While AES took 31 milliseconds in Intel-i3, 17 milliseconds in Intel-i5 and 15 milliseconds in Intel-i7 for decrypting the ciphertext into original text.

V. CONCLUSION AND FUTURE SCOPE

Based on the implementation of AES, Blowfish, and RSA over Intel-i3 with 4GB RAM, Intel-i5 with 8 GB RAM and Intel-i7 with 16 GB RAM, it is concluded that Blowfish is a faster cryptographic algorithm. It is even faster than AES because Blowfish took less encryption time as well as less encryption time as compared to AES. It is also concluded that Intel-i5 and Intel-i7 processors are best for both AES and Blowfish implementation because they are being executed approximately more than two times faster as compared to Intel-i3 processor. In the previous research papers, it is also concluded that, based on the performance evaluation, algorithms such as Blowfish and AES provide more security than other algorithms.

REFERENCES

[1] William Stallings, *"Cryptography and Network Security Principles and Practices"*, Fourth Edition, Pearson Education, Prentice Hall, **2009**.

[2] Jawahar Thakur, Nagesh Kumar, *"DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis"*, International Journal of Emerging Technology and Advanced Engineering, Volume **1**, Issue **2**, pp.**1-4**, **2011**.

[3] Gurpreet Singh, Supriya, *"A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security"* International Journal of Computer Applications (**0975 – 8887**) Volume **67**– No.**19**, pp.**1-4**, **2013**.

[4] Akash Kumar Mandal, Chandra Parakash, Mrs. Archana Tiwari, *"Performance Evaluation of Cryptographic Algorithms:DES and AES"*, 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science, pp. **2**, **2012**.

[5] Omar G. Abood, Shawkat K. Guirguis, *"A Survey on Cryptography Algorithms"*, International Journal of Scientific and Research Publications, Volume **8**, Issue **7**, pp.**7-15**, **2018**.

[6] Muhammad Faheem Mushtaq, Sapiee Jamel, Abdulkadir Hassan Disina, Zahraddeen, A. Pindar, Nur Shafinaz Ahmad Shakir, Mustafa Mat Deris, "*A Survey on the Cryptographic Encryption Algorithms",* International Journal of Advanced Computer Science and Applications, Vol. **8**, No. **11**, pp.**3-6**, **2017**.

[7] Nidhi Singhal, J.P.S.Raina, *"Comparative Analysis of AES and RC4 Algorithms for Better Utilization"*, International Journal of Computer Trends and Technology, pp.1-**5**, **2011**.

[8] Tingyuan Nie, Teng Zhang, *"A Study of DES and Blowfish Encryption Algorithm"*, A Project of Shandong Province Higher Educational Science and Technology Program (No. J09LG10), pp.**4**, **2009**.

[9] Gurjeevan Singh, Ashwani Kumar, & K.S. Sandha, *"A Study of New Trends in Blowfish Algorithm"*, International Journal of Engineering Research and Application, Vol. **1**, Issue **2**, pp.**5, 2011**.

Authors Profile

Mrs. Nishi Yadav is currently working as an Assistant Professor in Department of Computer Science, School of Studies in Engineering and Technology, Guru Ghasidas Vishwavidyalaya, Bilaspur, India.

Mr. Aditya Sahu is currently pursuing Bachelor of Technology in Computer Science and Engineering from School of Studies in Engineering and Technology, Guru Ghasidas Vishwavidyalaya, Bilaspur, India. He is currently studying in 3rd year.

Mr. Md Tausif Zafar is currently pursuing Bachelor of Technology in Computer Science and Engineering from School of Studies in Engineering and Technology, Guru Ghasidas Vishwavidyalaya, Bilaspur, India. He is currently studying in 3rd year.

