Performance Evaluation of Cryptographic Algorithms

Mohit Mittal
Computer Science & Engineering
Guru Nanak Dev University, Amritsar

ABSTRACT
In this paper, we compare the various cryptographic algorithms. On the basis of parameter taken as time various cryptographic algorithms are evaluated on different hardware's. Different hardware's are having different processing speed on which various size of file are processed. Calculation of time for encryption and decryption in different processors such as intel i5 , intel i3 , intel dual core ,intel atom having processing speed 2.27 GHz, 2.53 GHz, 2.00 GHz ,1.66 GHz respectively. Encryption processing time and decryption processing time are compared between various cryptographic algorithms which come out to be not too much. Overall time depend on the corresponding processing speed. Throughput analysis is also done.

Keywords
Introduction, Various Cryptographic algorithms, Objective, Simulation Procedure, Conclusion, Future Scope.

1.INTRODUCTION
Cryptography is the study and implementation of techniques to hide information from being read. Data that can be read and understood without any special measures is called plaintext. The method of representing plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable form is called cipher-text. The process of reverting cipher-text to its original plaintext is called decryption. The following figure 1 shows this process.

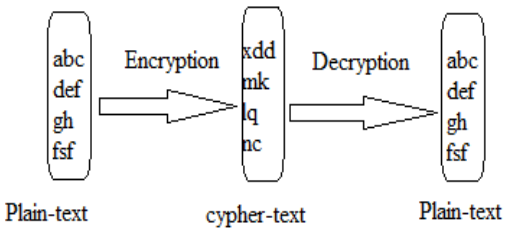

Figure1: Encryption and Decryption of plain text

2.VARIOUS CRYPTOGRAPHIC ALGORITHMS

DES: The Data Encryption Standard has been in use since the mid-1970s, adopted by the National Bureau of Standards (NBS) as Federal Information Processing Standard 46 and by the American National Standards Institute (ANSI) as X3.92. DES uses the Data Encryption Algorithm, a private key block-cipher employing a 56-bit key operating on 64-bit blocks.

TRIPLE DES: Triple DES is simply another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. We simply type in the entire 192-bit (24 character) key rather than entering each of the three keys individually. The procedure for encryption is exactly the same as regular DES, but it is repeated three times. The data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key the procedure for decrypting something is the same as the procedure for encryption, except it is executed in reverse.

AES: Advanced Encrypted Standard (AES) is an iterated cipher which was proposed by Joan Daemen and Vincent Rijmen (Rijndael). The proposed algorithm could support variable length block and key sizes e.g. multiple of 32 bits. However, only the 128 bit block size and 128, 192 and 256 bits keys are specified as AES standard. Entire 128 bits input block is organized as 4x4 bytes array called State and is processed in several rounds. Number of rounds to be used depend on the length of key e.g. 10 round for 128 bit key, 12 rounds for 192-bit key and 14 rounds for 256 bit keys.

3.OBJECTIVES
The main objectives of this paper are:

1. To investigate the performance of encryption and decryption of cryptographic algorithms over different hardware processors.
2. To find out the throughput of encryption and decryption of various cryptographic algorithms.

4. SIMULATION PROCEDURE
Our goal is to measure the Encryption and Decryption processing time of each algorithm for different Hardware. Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. The throughput of the encryption scheme is calculated by dividing the total plaintext in Megabytes encrypted on the total encryption time for each algorithm in. The various cryptographic algorithms are implemented on dot net frame work. Toby Emden has implemented the various cryptographic algorithms by creating the class crypt helper class which supports all of the major block cipher algorithms. In this given project, I have implemented time calculation coding. By this we can calculate the time of encryption and decryption processing. Our parameter time for encryption and decryption is calculated successfully.

Table 4.1:Hardware description

S. No.	Processor	RAM	Operating system
1	Intel® atom™ CPU N450@1.66GHz	1 GB	32 bit XP sp3
2	Intel® Pentium® Dual CPU E2180 @2.00GHz	1.50 GB	32bit Window 7
3	Intel® core™ i3 CPU @2.53GHz	3.00 GB	64bit Window 7
4	Intel® core™ i5 CPU @2.27GHz	3.00 GB	32bit Window 7

Table 4.2: Algorithm description

S. No.	Algorithms	Type	Block bits
1	DES	BLOCK	64
2	3DES	BLOCK	192
3	AES(RIJNDAEL)	BLOCK	256

5.GRAPHICAL DESCRIPTION

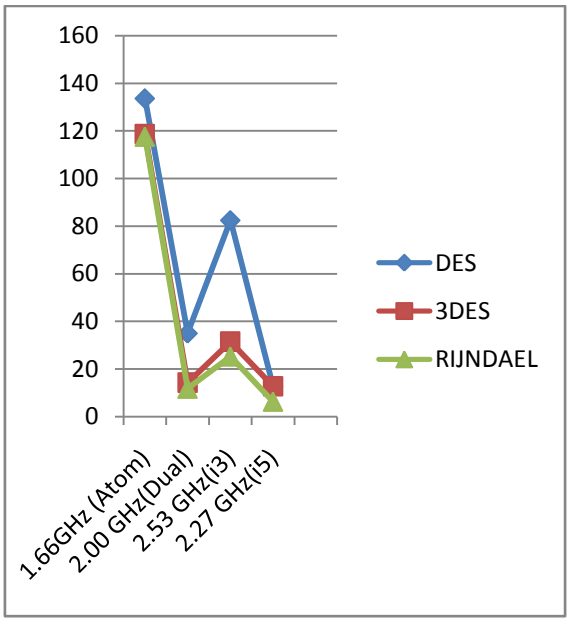

Figure 2: Processing time of encryption algorithm (hexadecimal encoding with string 1 KB)

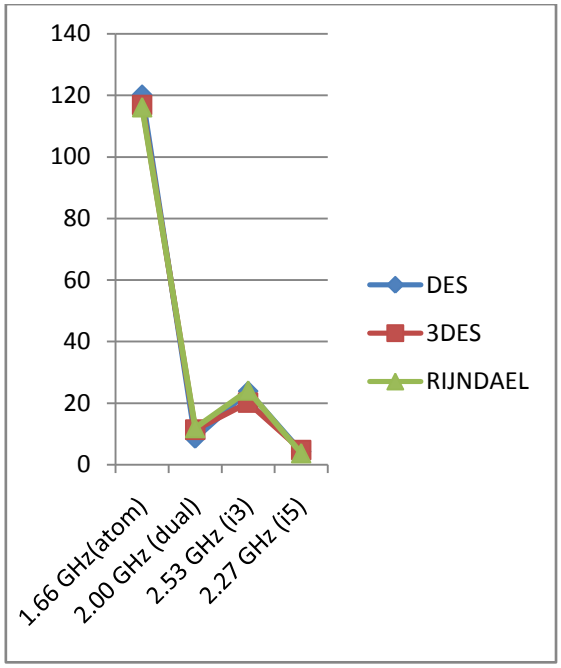

Figure 3: Processing time of encryption algorithm (base64 encoding with string 1 KB)

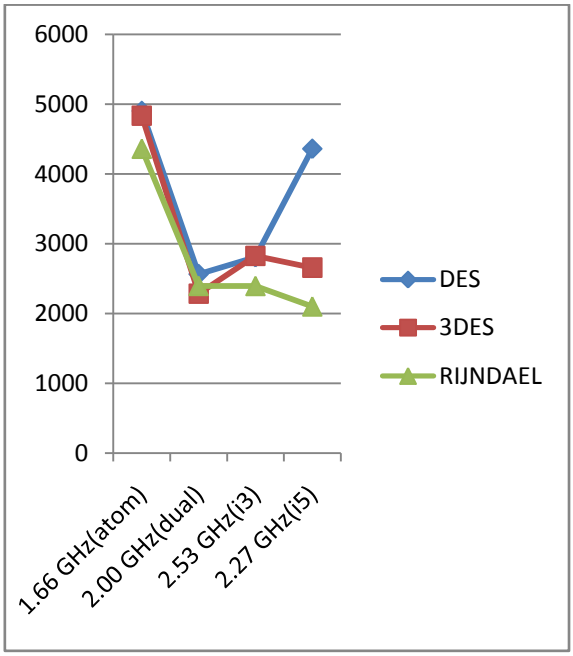

Figure 4: Processing time of encryption algorithm (hexadecimal encoding with string 1 MB)

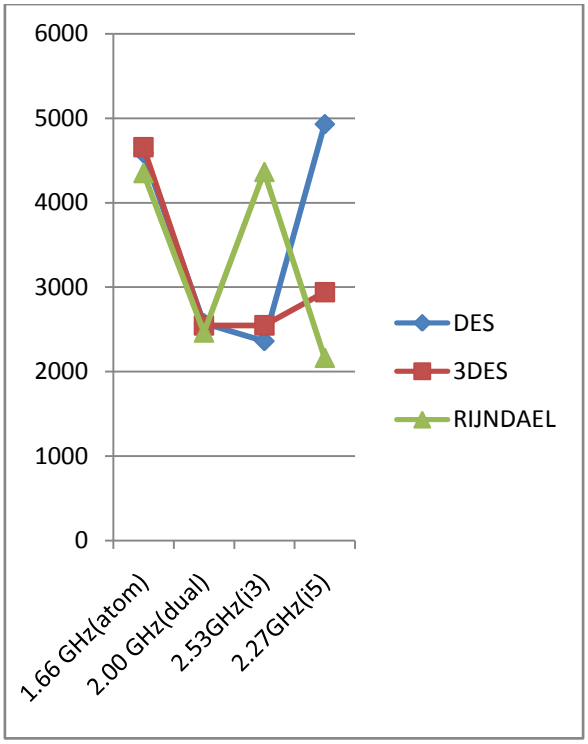

Figure 5: Processing time of encryption algorithm (base 64 encoding with string 1 MB)

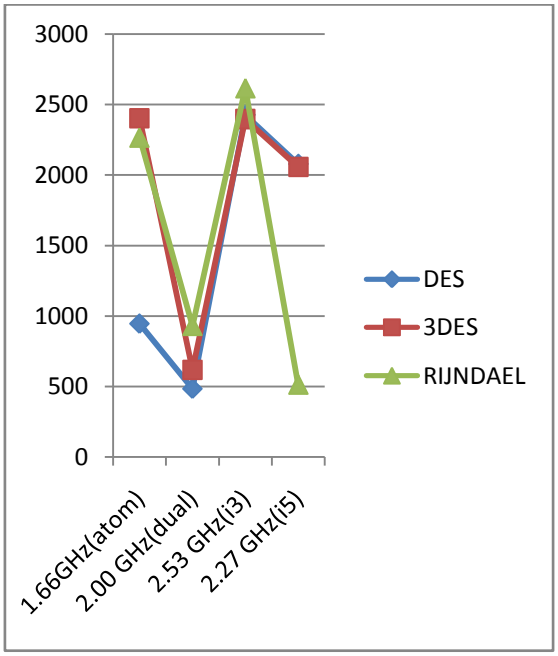

Figure 6: Processing time of encryption algorithm (hexadecimal encoding with file all zeros 3KB)

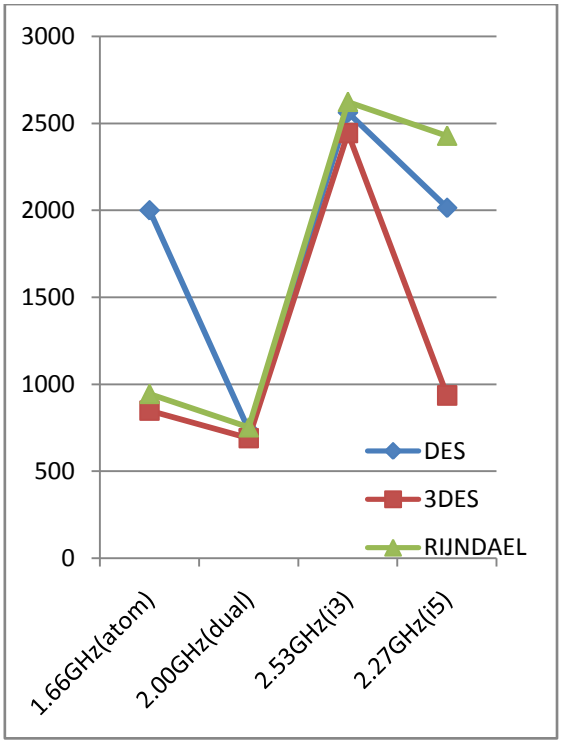

Figure 7: Processing time of encryption algorithm (base 64 encoding with file all zeros 3KB)

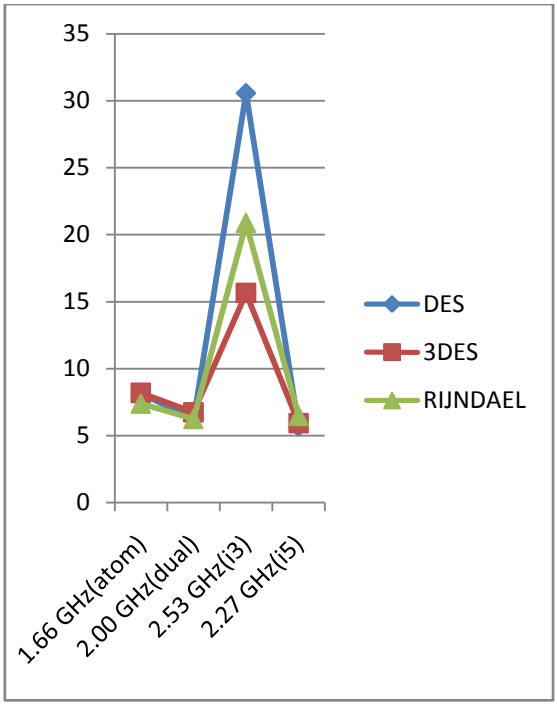

Figure 8: Processing time of decryption algorithm (hexadecimal encoding with string 1KB)

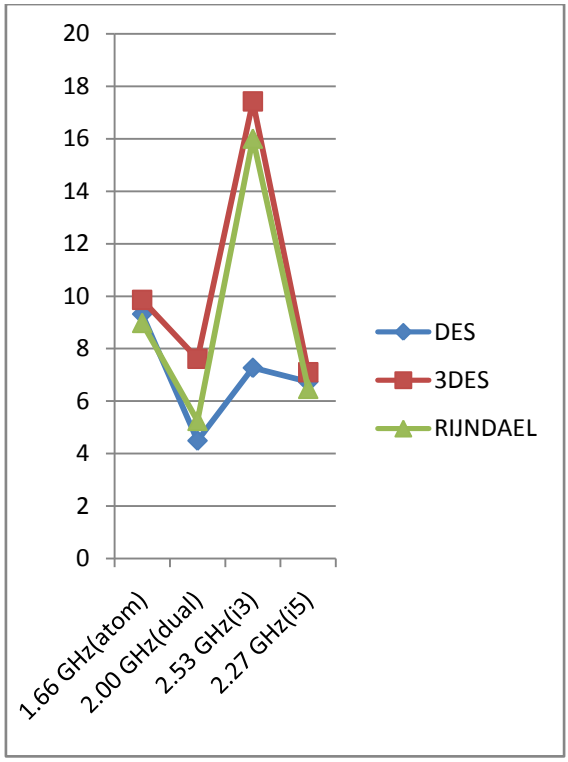

Figure 9: Processing time of decryption algorithm (base64 encoding with string 1KB)

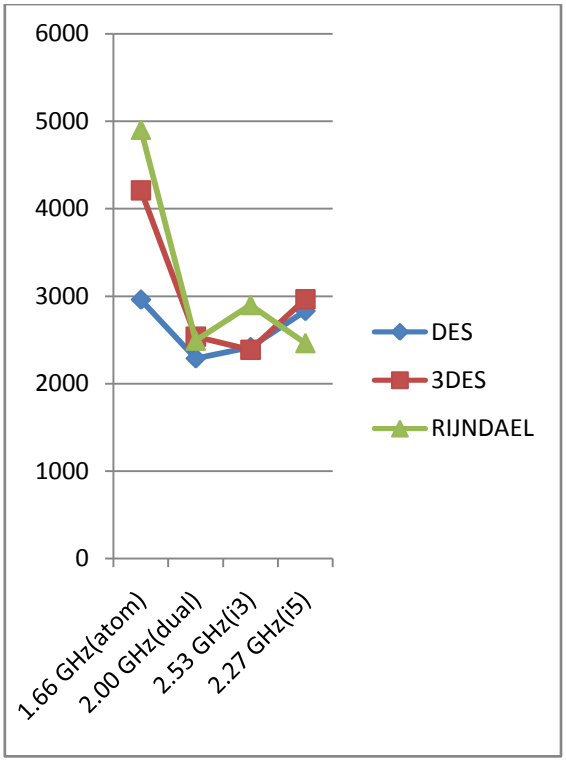

Figure 11: Processing time of decryption algorithms (base64 encoding with file 1 MB)

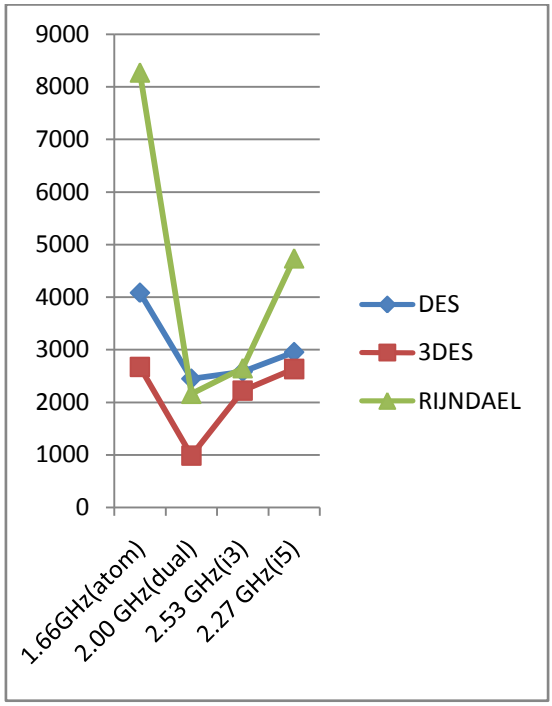

Figure 10: Processing time of decryption algorithms (hexadecimal encoding with file 1 MB)

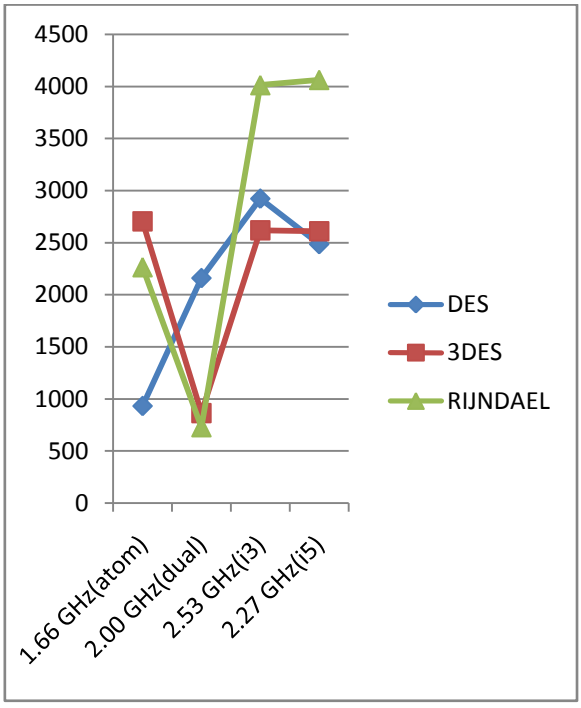

Figure 12: Processing time of decryption algorithm (hexadecimal encoding with file all zero 3 KB)

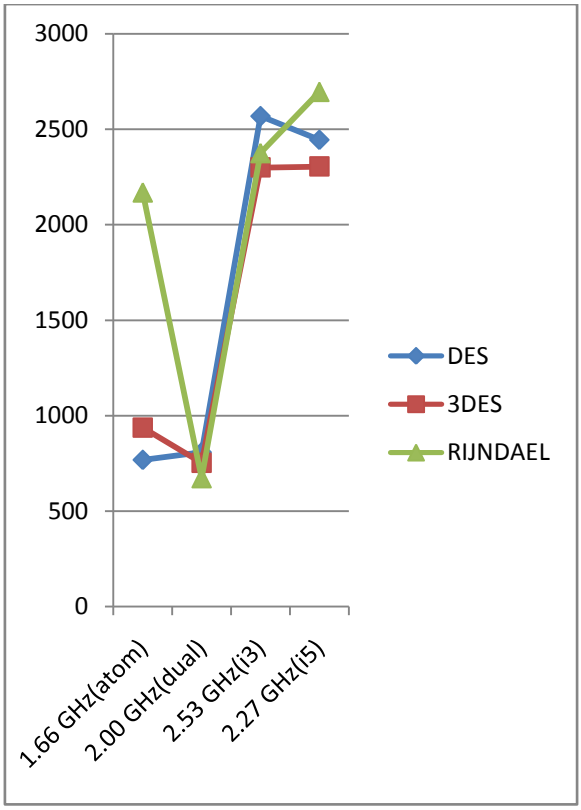

Figure 13: Processing time of decryption algorithms (base64 encoding with file all zero 3 KB)

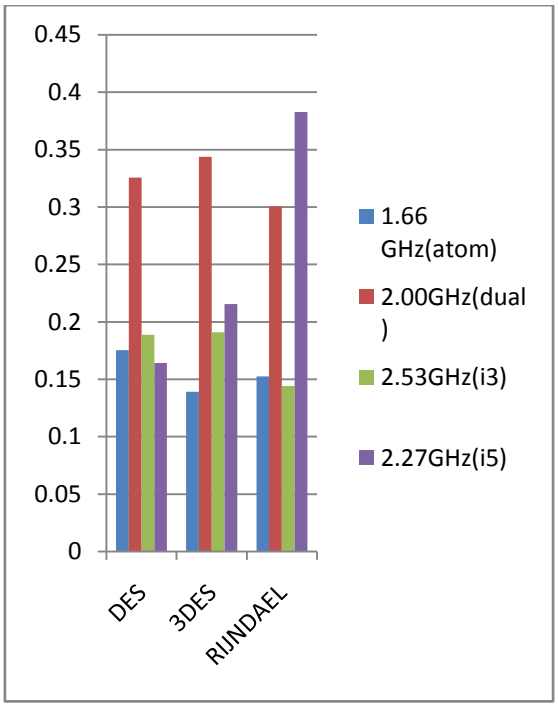

Figure 14: Throughput of encryption algorithms (hexadecimal encoding)

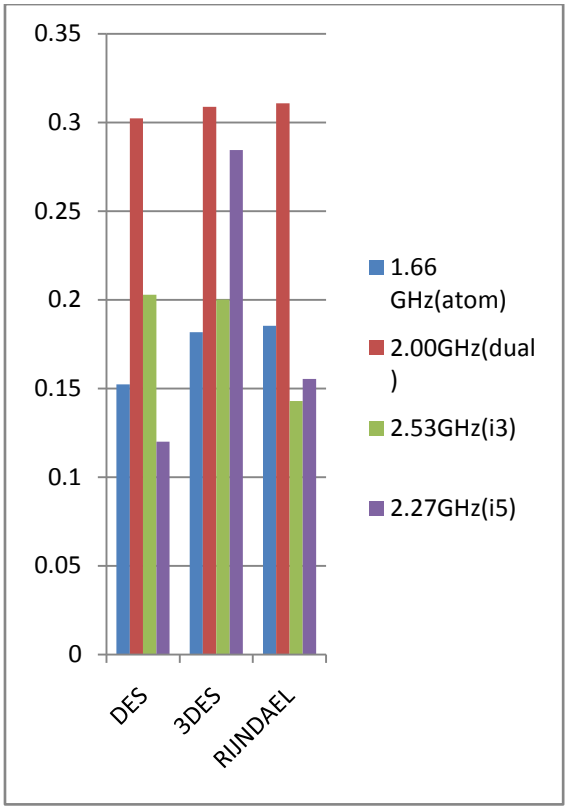

Figure 15: Throughput of encryption algorithms (base64 encoding)

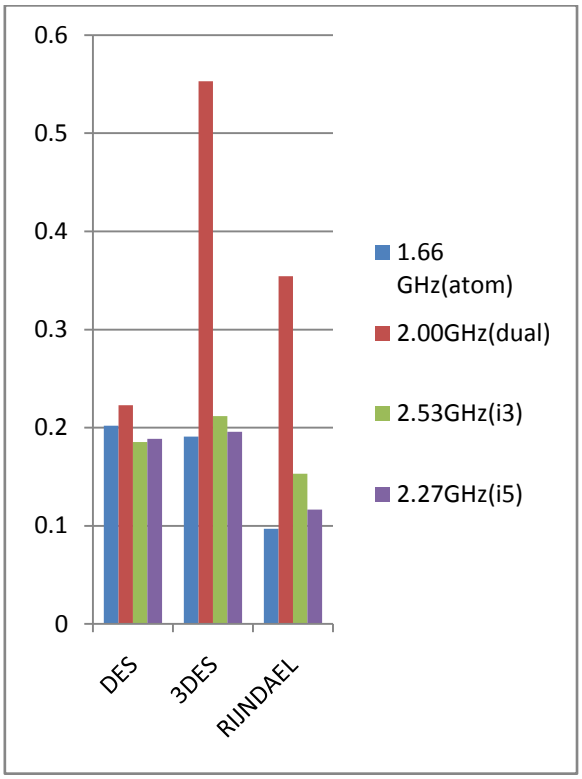

Figure 16: Throughput of decryption algorithms (hexadecimal encoding)

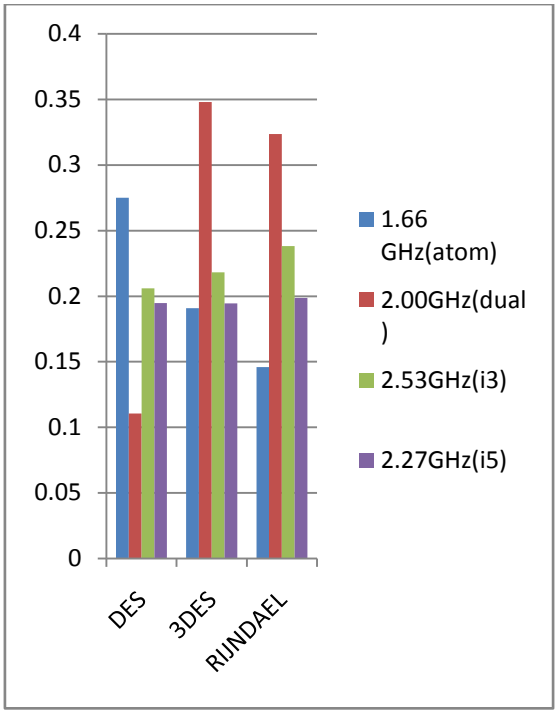

Figure 17: Throughput of decryption algorithms (base64 encoding)

6. CONCLUSION

The hardware processors are taken on which these algorithms are executed are 1.66 GHz, 2.00 GHz, 2.27 GHz, 2.53 GHz. Over this each hardware each algorithm is successfully executed by taking three different size of string which is 1 KB, 3 KB, and 1 MB. Then the processing time is calculated which is taken as parameter for performance analysis. The hardware processor 2.27 GHz (i5) and 2.00 GHz (dual) gives better performance than others. AES (Rijndael) algorithm is executed lesser processing time as compared to other algorithms. Processor 2.00 GHz (dual) gives best throughput than other hardware processors. Processor speed is inversely proportional to time calculated after encryption and decryption.

7. FUTURE SCOPE

This paper gave valuable knowledge to author about in understanding the cryptographic algorithms its basic work and which algorithm is performed well then others.. In this paper only one parameter is taken under evaluation but this can further more analyzed by taking other parameters. And it would be interesting to study how performance is affected by taking different parameters.

REFERENCES

[1] Auerbach, "An Overview of Cryptography", http://www.garykessler.net/library/crypto.html, September 1998.

[2]**"**Data encryption standard (des)", federal information processing standards publication (fips) 46-3 , 1999 October 25.

[3]Dirk Rijmenants **"**What is cryptography", http://users.telenet.be/d.rijmenants/en/cryptography.htm 2004.

[4] PGP Corporation "An Introduction to Cryptography", June 8, 2004

[5] Aamer Nadeem, Dr M. Younus Javed," A Performance Comparison of Data Encryption Algorithms", 2005 IEEE.

[6]Abdullah Al Hasib, Abul Ahsan Md. Mahmudul Haque," A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography", Third International Conference on Convergence and Hybrid Information Technology,2008.

[7] D.S. Abdul. Elminaam,H. M. Abdul Kader, M. M. Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms" Communications of the IBIMA Volume 8, 2009.

[8] Ross J. Anderson," Security Engineering: A Guide to Building Dependable Distributed Systems", 2010

[9] Neetu Settia," Cryptanalysis of Modern Cryptographic Algorithms", IJCST Vol. 1, Issue 2, December 2010

[10] O P Verma, Ritu Agarwal, Dhiraj Dafouti, Shobha Tyagi," Peformance Analysis Of Data Encryption Algorithms", 2011

[11] Srinivasarao D,Sushma Rani N, Ch.Panchamukesh ,S.Neelima, " analyzing the superlative symmetric cryptographic encryption algorithm (ascea)", Journal of Global Research in Computer Science, Volume 2,No. 7, July 2011.

[12]Gurjeevan Singh, Ashwani Kumar Singla,K.S. Sandha, "Through Put Analysis Of Various Encryption Algorithms", IJCST Vol. 2, Issue 3, September 2011.

[13] "Cryptography",crypto00.pdf

[14]"Triple DES Encryption", http://www.tropsoft.com/strongenc/des3.htm

[15] Abdel-Karim Al Tamimi," Performance Analysis of Data Encryption Algorithms "