Performance Analysis Of Blow Fish, Idea and AES Encription Algorithms

M. Anand kumar[1] and K. Appathurai [2]

ABSTRACT

NETWORK AND INTERNET APPLICATIONS ARE GROWING RAPIDLY IN THE RECENT PAST. THESE APPLICATIONS ARE USED BY THOUSAND OF USERS AND CONTROLLED BY DIFFERENT ADMINISTRATIVE ENTITIES. IT IS MAINLY USED AS AN EFFICIENT MEANS FOR COMMUNICATION, ENTERTAINMENT AND EDUCATION. WITH THE RAPID GROWTH OF INTERNET, THERE IS A NEED FOR PROTECTING CONFIDENTIAL DATA. THE INTERNET WAS HOWEVER ORIGINALLY DESIGNED FOR RESEARCH AND EDUCATIONAL PURPOSE, NOT FOR COMMERCIAL APPLICATIONS. SO INTERNET WAS NOT DESIGNED WITH SECURITY IN MIND. AS THE INTERNET GROWS THE EXISTING SECURITY FRAMEWORK WAS NOT ADEQUATE FOR MODERN DAY APPLICATIONS. . CRYPTOGRAPHY PLAYS A VITAL ROLE IN THE FIELD OF NETWORK SECURITY. CURRENTLY MANY ENCRYPTION ALGORITHMS ARE AVAILABLE TO SECURE THE DATA BUT THESE ALGORITHMS CONSUME LOT OF COMPUTING RESOURCES SUCH AS BATTERY AND CPU TIME. THIS PAPER MAINLY FOCUSES ON THREE COMMONLY USED SYMMETRIC ENCRYPTION ALGORITHMS SUCH AS BLOWFISH, IDEA AND AES. THESE ALGORITHMS ARE COMPARED AND PERFORMANCE IS EVALUATED

[1] Associate Professor, Dept. of Information Technology Karpagam University, Coimbatore – 21.

[2] Associate Professor and Head, Dept. of Information Technology Karpagam University, Coimbatore – 21.

KEYWORDS—BLOWFISH, CRYPTOGRAPHY, ENCRYPTION, INTERNET, IDEA, SECURITY, SYMMETRIC ALGORITHMS

I. INTRODUCTION

THE INTERNET IS A GLOBAL SYSTEM OF INTERCONNECTED COMPUTER NETWORKS THAT USE THE STANDARD INTERNET PROTOCOL SUITE (TCP/IP) TO SERVE BILLIONS OF USERS WORLDWIDE [1]. IT IS A NETWORK OF NETWORKS THAT CONSISTS OF MILLIONS OF PRIVATE, PUBLIC, ACADEMIC, BUSINESS, AND GOVERNMENT NETWORKS, OF LOCAL TO GLOBAL SCOPE, THAT ARE LINKED BY A BROAD ARRAY OF ELECTRONIC, WIRELESS AND OPTICAL NETWORKING TECHNOLOGIES WITH THE RAPID GROWTH OF INTERNET, THERE IS NEED TO PROTECT THE SENSITIVE DATA FROM UNAUTHORIZED ACCESS. WITH THE INCREASING USE OF INTERNET FOR BUSINESS APPLICATIONS, THERE IS A GREAT DEMAND FOR QUALITY OF SERVICE. THE APPLICATION THAT IS INCREASING DAY-BY-DAY NEEDS A CONSISTENT CONTROL PROTOCOLS FOR PROVIDING QUALITY OF SERVICE (QOS). BECAUSE OF THESE REASONS THE NEED FOR SECURITY IN THE INTERNET IS STRONGER THAN EVER.

CRYPTOGRAPHY IS THE SCIENCE THAT IS WIDELY USED FOR THE NETWORK SECURITY. KEY ASPECTS OF CRYPTOGRAPHY ARE PRIVACY, AUTHENTICATION, IDENTIFICATION, TRUST AND VERIFICATION [2]. THERE ARE SEVERAL WAYS OF CLASSIFYING CRYPTOGRAPHIC ALGORITHMS. THEY CAN BE CLASSIFIED BASED

ON THE NUMBER OF KEYS THAT ARE EMPLOYED FOR ENCRYPTION AND DECRYPTION, AND FURTHER DEFINED BY THEIR APPLICATION AND USE THE CRYPTOGRAPHIC ALGORITHMS CAN BE BROADLY DIVIDED INTO THREE TYPES NAMELY SECRET KEY CRYPTOGRAPHY (SKC), PUBLIC KEY CRYPTOGRAPHY (PKC) AND HASH FUNCTIONS SOME OF THE SECRET KEY ALGORITHMS ARE DATA ENCRYPTION STANDARD (DES), ADVANCED ENCRYPTION STANDARD (AES), CAST, INTERNATIONAL DATA ENCRYPTION ALGORITHM(IDEA), BLOWFISH, TWOFISH, AND SECURE AND FAST ENCRYPTION ROUTINE(SAFER). IN THESE ALGORITHMS AES AND BLOWFISH ARE THE TWO ALGORITHMS PROVED TO BE STRONG IN THE MODERN WORLD. RSA, DIFFIE-HELLMAN, DIGITAL SIGNATURE ALGORITHM (DSA), ELGAMAL AND ELLIPTIC CURVE CRYPTOGRAPHY ARE SOME OF THE PUBLIC KEY CRYPTOGRAPHIC ALGORITHMS [3].

THE REST OF THE PAPER IS ORGANIZED AS FOLLOWS. BLOWFISH, IDEA AND AES ALGORITHMS ARE DESCRIBED IN SECTION II THAT IS FOLLOWED BY PERFORMANCE METHODOLOGY IN SECTION III. IN SECTION IV THE RESULTS ARE GIVEN AND FINALLY WE CONCLUDE IN SECTION V.

II CRYPTOGRAPHIC ALGORITHMS

THIS WORK MAINLY FOCUSES ON SYMMETRIC ALGORITHMS THAT ARE COMMONLY USED IN DATA COMMUNICATION NETWORKS. SYMMETRIC CRYPTOGRAPHIC ALGORITHMS [4] ARE ALSO REFERRED TO AS SECRET-KEY ALGORITHMS, SINGLE KEY ALGORITHMS, CONVENTIONAL ALGORITHMS, SHARED ALGORITHMS, PRIVATE-KEY ALGORITHMS OR ONE-KEY ALGORITHMS. THESE ARE THE ALGORITHMS WHERE THE ENCRYPTION KEY CAN BE CALCULATED FROM THE DECRYPTION KEY AND VICE VERSA. IN MOST SYMMETRIC ALGORITHMS, THE ENCRYPTION KEY AND THE DECRYPTION KEY ARE TRIVIALLY RELATED, OFTEN IDENTICAL. ENCRYPTION AND DECRYPTION WITH A SYMMETRIC ALGORITHM ARE DENOTED BY

$$EK(M) = C \qquad (1)$$

$$DK(C) = M$$

These algorithms require that the sender and receiver agree on a key before they can communicate securely. The security of a symmetric algorithm rests in the key; divulging the key means that anyone could encrypt and decrypt messages. As long as the communication needs to remain secret, the key must remain secret. Some examples of popular and well-respected symmetric algorithms include Twofish, Serpent, AES (Rijndael), Blowfish, CAST5, Camellia, 3DES, and IDEA. This work only focuses on Blowfish, IDEA and AES symmetric algorithms.

A. Blowfish: Blowfish: Blowfish [5] is a 64-bit symmetric block cipher with variable length key. The algorithm operates with two parts: a key expansion part and a data- encryption part. The role of key expansion part is to converts a key of at most 448 bits into several sub key arrays totaling 4168 bytes. The data encryption occurs via a 16-round Feistel network. Each round consists of a key dependent permutation, a key and data-dependent substitution. All operations are EX-ORs and additions on 32-bit words Blowfish is successor to Twofish

B. IDEA : The IDEA[6] is a 64-bit block cryptographic algorithm which uses a 128-bit key. This key is the same for both encryption and decryption. The algorithm consists of nine phases: eight identical phases and a final transformation phase. The encryption takes place when the 64-bit block is propagated through each of the first eight phases in a serial way where the block divided into four 16-bit sub-blocks is modified using the six sub-keys corresponding to each phase six sub-keys per phase and four sub-keys for the last phase). When the output of the eighth phase is obtained the block goes through a last phase the transformation one, which uses the last four sub-keys. . In terms of energy of key setup and encryption, IDEA is on par with AES. IDEA is supposed to have very good cryptanalytic properties, thereby combining efficiency with acceptable security (Potlapally, 2006)

C. AES: AES [7] is a block cipher .It has variable key length of 128, 192, or 256 bits; default 256.It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Also, AES has been carefully tested for many security applications [16].

III Performance Methodology

Performance is one of the vital components of any encryption algorithm. This section gives detailed description about the simulation environment which is used to evaluate the performance of encryption algorithms. It also describes the system components that are used in the experiment. Advanced Encryption Standard algorithm, IDEA and Blowfish algorithm was implemented in MATLAB and .Net Framework

A. System Parameters

The setup for the experiment is designed as two architectures such as wired architecture and wireless architecture. For wired architecture, Local Area Network (LAN) with eight Pentium IV systems is used. For wireless architecture two laptops are used in the experiment. The two laptops (sender and receiver) had windows XP professional installed on it. The first laptop (sender) is connected to access point. In the experiments, the first laptop encrypts a different file size for different data types ranges from 321 Kilobytes to 7.139Megabytes for text data (.DOC files), from 33 Kbytes to 8,262 Kbytes for audio data (.WAV files), from 28 Kbytes to 131 Kbytes for pictures and Images (.GIF and GPG files) using .NET environment, two commonly used encryption algorithm such as IDEA with different key sizes and Blowfish are selected and implemented.

B. Experimental criteria

Performance is evaluated for the proposed algorithm based on the several metrics which are best suited for the cryptographic algorithms. The performance is evaluated separately for text data encryption and voice data encryption. The metrics [8] that are selected for the evaluation are encryption time, decryption time, throughput of encryption, throughput of decryption,

diffusion analysis, CPU process time, and CPU clock cycles, power consumption and memory utilization.

Encryption time: The encryption time [8] is the total time taken to produce a cipher-text from plain-text. The calculated encryption time is then used to calculate the throughput of the encrypted algorithm. It gives the rate of encryption.

Decryption time: Decryption time [9] is the total time taken to produce the plain-text from Cipher-text. The calculated decryption time is then used to calculate the throughput of the decrypted algorithm. It gives the rate of decryption.

Throughput of Encryption: The throughput[10] of the encryption scheme defines the speed of encryption. When there is an increase in the throughput of the encryption algorithm, there is a decrease in the power consumption algorithm.

Throughput of Decryption: The throughput [11] of the decryption scheme defines the speed of decryption. When there is an increase in the throughput of the decryption algorithm, there is a decrease in the power consumption algorithm.

Diffusion analysis: Diffusion analysis is one of the important factors of cryptographic algorithms. This analysis is mainly used to exhibit the avalanche effect. Some of the cases of avalanche effect of the encryption algorithms are

- Changing one bit at a time in a plain-text, keeping key as constant.
- Changing one bit at a time in a key, keeping plain-text as constant.
- Changing many bits at a time in a plain-text, keeping key as constant.
- Changing many bits at a time in a key, keeping plain-text as constant.

CPU process time: The CPU process time is the time that a CPU is dedicated only to the particular process for calculations. It reflects the load of the CPU. More the CPU time used in the encryption process, the higher is the CPU load.

CPU Clock: The CPU clock cycles are a metric, reflecting the energy consumption of the CPU while performing on encryption operations. Each cycle of CPU will consume a minute amount of energy.

Power Consumption: It is the total power that required by the encryption and the decryption algorithm [12]. It was estimated based on the throughput of the encryption and decryption algorithms. When there is an increase in the throughput of the encryption/decryption algorithm, there is a decrease in the power consumption algorithm.

Memory utilization: The memory requirement for the encryption and decryption.

C. Experimental Procedure

Several experimental procedures are used such as different encoding techniques for encryption, Encryption time analysis, Decryption time analysis and Throughput analysis for encryption and decryption. Different data types such as text or document and images are used for each selected algorithms. Different key sizes are employed to trace the performance of the selected algorithms specifically power consumption. The formula to calculate the average encryption time [10] is given in the equation (2).

$$AvgTime = \frac{1}{Nb}\sum_{i=1}^{Nb}\frac{M_i}{t_i}(Kb/s) \quad (2)$$

Where

AvgTime = Average Data Rate (Kb/s)

Nb = Number of Messages

M_i=Message Size (Kb)

T_i=Time taken to Encrypt Message M_i

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 as in equation (3).

$$Throughput = \frac{Tp}{Et} \quad (3)$$

Energy consumption [13] for encryption and decryption can be measured in several ways. The first method used to measure energy consumption is to assume that an average amount of energy is consumed by normal operations and to test the extra energy consumed by an encryption algorithms. This method simply monitors the level of the percentage of remaining battery that can computed by equations. The battery life is consumed in percentage for one run.

$$OneRun = \frac{Change\_in\_Batterylife}{No\_of\_Runs} \quad (4)$$

Average battery Consumed per iteration =

$$\text{iteration} = \sum_{1}^{N}\frac{Battery\_consumed/Iteration}{No\_of\_Runs} \quad (5)$$

The second method of security primitives can also be measured by counting the amount of computing cycles which are used in computations related to cryptographic operations [14,15]. For computation of the energy cost of encryption, the equation as shown below was used.

$$B\_cost\_Encryption(ampere-cycle) = \tau * I \quad (6)$$

$$Total\_Energy\_Cost = \frac{B\_cost\_encryption}{F(Cycles/Sec)} \quad (7)$$

$$Energy\_cost = Total\_Energy\_cost * V \quad (8)$$

Where

Bcost_Encryption: = basic cost of encryption

Ô = The total number of clock cycles.

I = The average current drawn by each CPU clock cycle.

Total_Energy_Cost= The total energy cost (amp seconds).

F: clock frequency (cycles/sec).

Energy_cost = The energy cost (consumed).

So the amount of energy consumed [18, 19] by program P to achieve its goal (encryption or decryption) is given by

$$E = VCC * I * N * \tau \qquad (9)$$

Where N = The number of clock cycles.

ô = The clock period.

VCC = The supply voltage of the system

I = The average current in amperes drawn from the power source for T seconds.

IV RESULTS

This section describes the series of results based on the experimental procedures that are described in the previous sections such as encoding techniques, packet size, data types and keys. The experiments are performed several times to assure the results are constant and are valid to compare the different algorithms. Different system configurations are used o get better comparison results. Laptop , standalone PC and Networked PCs are also used to track the performance of the algorithms.

A. Results based on encoding techniques

Encoding techniques [12] plays a vital role in cryptography. It is very necessary to use these techniques in evaluating the performance of cryptographic algorithms. The following table and figure shows the data for encoding techniques. The graph shows there is no major changes in terms of encoding techniques.

TABLE I: Time consumption Encoding Techniques

S.No	Packet Size (KB)	Time Consumption(Base64 Encoding)		
		Blowfish	IDEA	AES
1	1024.00	508 ms	692 ms	503 ms
2	1500.00	621 ms	801 ms	629 ms
3	2100.02	701 ms	856 ms	681 ms
4	2512.12	767 ms	989 ms	759 ms
5	3121.07	841 ms	1045 ms	841 ms
6	3923.08	898 ms	1121 ms	878 ms
7	4120.00	956 ms	1972 ms	958 ms
8	4780.12	998 ms	2114 ms	1012 ms
9	6342.12	1420 ms	2934 ms	1298 ms
10	7231.45	1930 ms	3521 ms	1890 ms

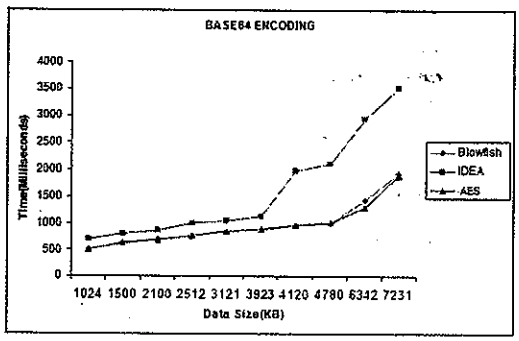


Figure 1: Time consumption (Encoding)

B Result based on Encryption Process

The encryption time was calculated for the three algorithms namely IDEA, Blowfish and AES Block cipher.

It is the total time taken to produce a cipher-text from plain-text. The calculated encryption time is then used to calculate the throughput of the encrypted algorithm. Different file sizes ranging from 40 Kb to 8000 kb is used for the evaluation. It gives the rate of encryption. From the analysis it was identified that AES have good performance when compared to other algorithms.

TABLE 2: Time consumption (Encryption)

S.No	Packet Size (KB)	Time Consumption(Encryption)		
		Blowfish	IDEA	AES
1	49.00	59.0	79.2	56.0
2	59.10	39.0	53.9	38.0
3	100.09	94.0	112.0	90.0
4	247.12	121.0	145.0	112.0
5	321.24	167.0	185.0	164.0
6	694.45	234.0	276.0	210.0
7	899.12	254.0	291.2	258.0
8	963.09	413.0	521.0	408.0
9	5345.15	1324.0	1876.0	1237.0
10	7310.39	1432.0	2143.0	1366.0

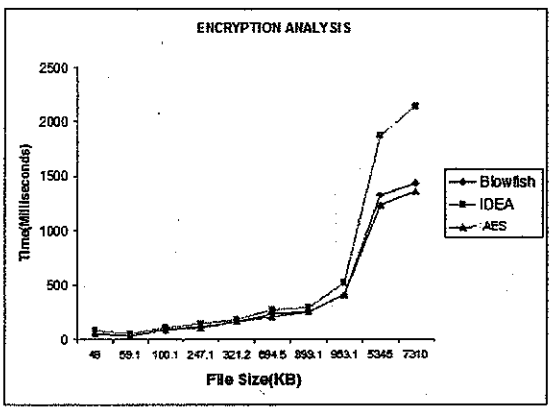


Figure 2: Time consumption (Encryption)

C. Results Based on Decryption Process

The Decryption time was calculated for the three algorithms namely IDEA, Blowfish and AES Block cipher. It is the total time taken to produce a plain-text from cipher-text. The calculated decryption time is then used to calculate the throughput of the decryption algorithm. Different file sizes ranging from 40 Kb to 8000 kb is used for the evaluation. It gives the rate of decryption. From the analysis it was identified that AES have good performance when compared to other algorithms.

TABLE 3. Time consumption (Decryption)

S.No	Packet Size (KB)	Time Consumption(Decryption)		
		Blowfish	IDEA	AES
1	49.00	65.00	78.1	61.00
2	59.10	45.00	56.7	43.00
3	100.09	89.00	110.2	79.00
4	247.12	120.00	139.0	112.00
5	321.24	167.00	176.2	168.00
6	694.45	243.00	269.0	212.00
7	899.12	223.00	287.1	259.00
8	963.09	243.00	527.6	206.00
9	5345.15	1224.00	1872.3	1216.00
10	7310.39	1435.00	2141.7	1363.00

Figure 3: Time consumption (Decryption)

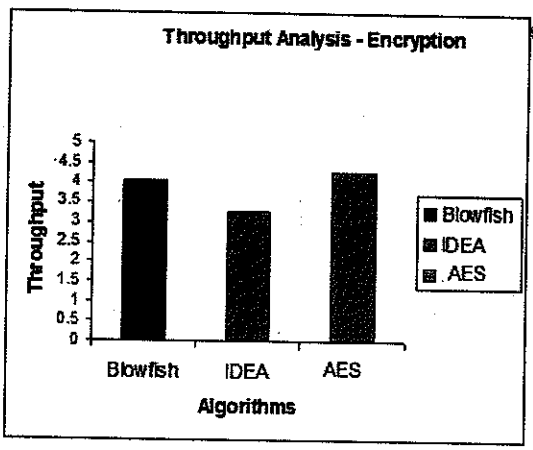


Figure 4: Throughput Analysis

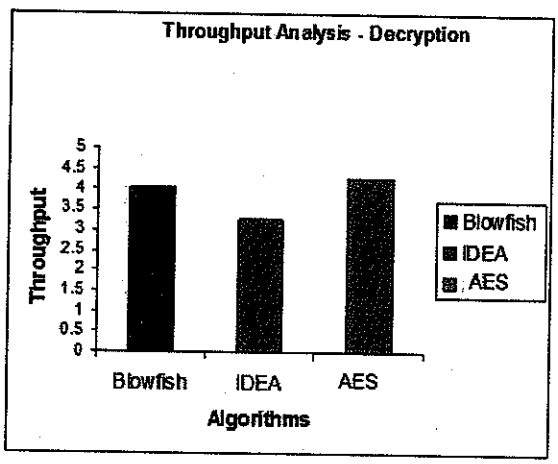


Figure 5: Throughput Analysis (Decryption)

Figure 4 and 5 shows the result based on the throughput of the encryption and decryption with different packet size. It shows that the throughput is high for AES when compared to that of Blowfish. As the throughput value is increased, the power consumption of the encryption technique is decreased. So from the experiment it proves that AES encryption algorithm consumes less power for encrypting the text than that of Blowfish.

VI.CONCLUSION

This paper presented the performance evaluation of three commonly known symmetric cryptographic algorithms. These algorithms are tested with different performance metrics. The simulation results shows that AES has better performance than Blowfish in almost all the test cases. There is no significant difference in the result for encoding techniques. It is found that AES is good for text based encryption as well as for image. It is also identified that there is change in performance when there is a change in key size of AES algorithm. Overall it is identified that AES can be used in circumstances where there is need for high security. In the case of performance aspects, Blowfish can be used

References

[1] Caicedo, C. E., J. B. Joshi, and D. Tuladhar, 2009. IPv6 Security Challenges, IEEE Computers, 42(2): 36-42.

[2] Delgosha, F., and F. Fekri, 2006. Public-key cryptography using Para unitary matrices, IEEE Transactions on Signal Processing, 54(9): 3489-3504.

[3] Diaa Salama Abdul, Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, 2008. Performance Evaluation of Symmetric Encryption Algorithms, International Journal of Computer Science and Network Security, 8(12): 78-85.

[4] Elminaam, D. S. Abd., H. Kader, M. Abdual and Hadhoud., M. Mohamed, 2010. Evaluating the Performance of Symmetric Encryption Algorithms,

International Journal of Network Security, 10(3): 216-222.

[5] Gurjeevan Singh, K. Ashwani Kumar, and S. Sandha , 2011. A Study of New Trends in Blowfish Algorithm, International Journal of Engineering Research and Applications, 1(2): 321-326.

[6] Sandipan Basu., 2011. International Data Encryption Algorithm (Idea) – A Typical Illustration, Journal of Global Research in Computer Science, 2(7): 116-118.

[7] Hua li, and Jianzhou li, 2008. A new compact dual-core architecture for AES encryption and decryption, Canadian Journal of Electrical and Computer Engineering, 33(3): 209-213.

[8] Nidhi Singhal, and J. P. S. Raina, 2011. Comparative Analysis of AES and RC4 Algorithms for Better Utilization, International Journal of Computer Trends and Technology, 1(3): 177-181

[9] Diaa Salama Abdul, Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, 2008. Performance Evaluation of Symmetric Encryption Algorithms, International Journal of Computer Science and Network Security, 8(12): 78-85.

[10] Lu, J.; Wei, Y.; Fouque, P.A.; Kim, J., "Cryptanalysis of reduced versions of the Camellia block cipher," Information Security, IET , vol.6, no.3, pp.228,238, Sept. 2012

[11] Diaa Salama Abdul, Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, 2008. Performance Evaluation of Symmetric Encryption Algorithms, International Journal of Computer Science and Network Security, 8(12): 78-85.

[12] Afaf, M. Ali Al-Neaimi, and Rehab F. Hassan, 2011. New Approach for Modifying Blowfish Algorithm by Using Multiple Keys, International Journal of Computer Science and Network Security, 11(3): 21-26.

[13] Palaniswamy, N., M. Dipesh Dugar, N. Dinesh Kumar Jain, and G. Raaja Sarabhoje, 2010. Enhanced Blowfish algorithm using bitmap image pixel plotting for security improvisation, Education Technology and Computer, (1): 533-538.

[14] Daemen, J., and V. Rijmen, 2010. The First 10 Years of Advanced Encryption, IEEE Security and Privacy, 8(6): 72-74.

[15] Jingmei Liu., Baodian Wei, Xiangguo Cheng, and Xinmei Wang, 2005. An AES S-box to Increase Complexity and Cryptographic Analysis, Proceedings of IEEE International Conference on Advanced Information Networking and Applications, 1-5.

[16] Li, Xiang., Chen, Junli, Liu, Weixiao, and Wan, Wanggen 2009. An improved AES encryption algorithm, Wireless Mobile and Computing 1(1): 694-698.

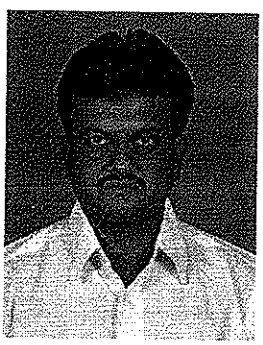
[17] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, 2007.A Modified AES Based Algorithm for Image Encryption, World Academy of Science, Engineering and Technology, 3(1): 526-531

[18] Mohan H. S., and Raji Reddy, A. , 2011. Performance Analysis of AES and MARSEncryption Algorithms, International Journal of Computer Science Issues, 8(4): 363-368.

[19] Monika Agrawal, and Pradeep Mishra, 2012. A Comparative Survey on Symmetric Key Encryption Techniques, International Journal on Computer Science and Engineering, 4(5): 877-882.

Authors Biography

Dr. M. Anand Kumar has completed M.Sc and M.Phil in computer science from Bharathiar University. He has Completed Ph.D in Karpagam University and currently working as an Associate Professor in karpagam University having ten years experience in teaching.. His area of research includes network security and information security. He has presented twenty papers in national conferences and four papers in international conferences. He has published twelve papers in international journals.



Dr. K.Appathurai working as Associate professor and Head department of Information Technology in Karpagam University, Coimbatore, Tamil Nadu, India. His area of interest is Spatial database. He published 10 papers in the reputed journals.