INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

Comparative Analysis of Advanced Encryption Standard, Blowfish and Rivest Cipher 4 Algorithms

Adolf Fenyi
Researcher, Kwame Nkrumah University of Science and Technology, Knust, Ghana
Joseph G. Davis
Lecturer**,** Kwame Nkrumah University of Science and Technology, Knust, Ghana
Dr. Kwabena Riverson
Head of Programme CSIR Institute of Industrial Research Accra, Ghana

Abstract:
Cryptography is one of the main categories of computer security that converts information from its normal form into an unreadable form. The two main characteristics that identify and differentiate one encryption algorithm from another are its ability to secure the protected data against attacks and its speed and efficiency in doing so.Cryptography is required to transmit confidential information over the network. It is also demanding in wide range of applications which includes mobile and networking applications. Cryptographic algorithms play a vital role in providing the data security against malicious attacks. But on the other hand, they consume significant amount of computing resources like CPU time, memory, encryption time etc. Normally, symmetric key algorithms are preferred over asymmetric key algorithms as they are very fast in nature. Symmetric algorithms are classified as block cipher and stream ciphers algorithms. In this research project, I comparedthe AES and Blowfish algorithms with different modes of operation (ECB, CBC, and CFB) and RC4 algorithm (stream cipher) in terms encryption time, decryption time, memory utilization and throughput at different settings likevariable key size and variable data packet size.A stimulation program is developed using PHP and JavaScript scripting languages. The program encrypts and decrypts different file sizes ranging from 1MB to 50MB. Firstly the user input 32 characters of key and 16 characters of Initialization Vector that would be used by the algorithm to encrypt and decrypt the message. After the key and Initialization vector are input, the user then use the browse button to select a file which has a size ranging from 1MB to 50 MB on the hard-drive. A prompt is displayed if the size of the file exceeds the specified range. The submit button is used by the user to initiate the process. A notification is displayed on the screen while the process is being executed. During the encryption and decryption process, the software automatically creates a file which copies the contents of the files being encrypted and decrypted into a folder on the user's hard-drive. The stimulator analyzes and produces graphical representation of the results to the user.

Keywords: *Comparative***,** *Encryption, Algorithm***,** *Simulation*

1. Introduction

1.1. Background Study

Many times when data is exchanged electronically the privacy of the data is a requirement. The use of encryption restricts unintended recipients from viewing the data, which are deemed confidential and potentially dangerous if made known to irresponsible parties.

Today, encryption is the procedure of transforming plaintext, data that can be read by anyone, to ciphertext, data that can only be read by someone with a secret decryption key.

A message before being changed in any way is called plaintext. Plaintext messages are converted to ciphertext via some encryption method. A particular such method is called a cryptosystem.

The various encryption algorithms that this project compares are Blowfish, Advanced Encryption Algorithm (AES) and Rivest Cipher 4(RC4).

The Blowfish algorithm is a 64-bit symmetric block cipher that uses a variable-length key from 32 to 448-bits (56 bytes). The algorithm was developed to encrypt 64-bits of plaintext into 64-bits of cipher text efficiently and securely. The operations selected for the algorithm were table lookup, modulus, addition and bitwise exclusive-or to minimize the time required to encrypt and decrypt data on 32-bit processors. A conscious attempt was made in designing the algorithm to keep the operations simple and easy to code while not compromising security.

Blowfish incorporates a 16 round Feistel network for encryption and decryption. But during each round of Blowfish, the left and right 32-bits of data are modified unlike DES which only modifies the right 32-bits to become the next round's left 32-bits. Blowfish incorporated a bitwise exclusive-or operation to be performed on the left 32-bits before being modified by the F function or propagated to the right 32-bits for the next round. Blowfish also incorporated two exclusive-or operations to be performed after the 16 rounds and a swap operation. This operation is different from the permutation function performed in DES.

AES is a symmetric block cipher with a block size of 128 bits. Key lengths can be 128bits, 192 bits, or 256 bits; called AES-128, AES-192, and AES-256, respectively. AES-128 uses 10 rounds, AES-192 uses 12 rounds, and AES-256 uses 14 rounds. The first three functions of an AES round are designed to thwart cryptanalysis via the methods of "confusion" and "diffusion." The fourth function actually encrypts the data. Claude Shannon described diffusion as patterns in the plaintext that are dispersed in the ciphertext while Confusion is relationship between the plaintext and the cipher text is obscured.

The following are some of the characteristics of AES:

- Stronger –Many cryptanalysis efforts have proved futile to break AES. Assuming that one could build a machine that could recover a DES key in a second (i.e., try 2^{55} keys per second), then it would take that machine approximately 149 thousand-billion (149 trillion) years to crack a 128-bit AES key.
- Provide full specification & design details - algorithm & implementation characteristics are part of the documentation.
- Poor Performance: AES showed poor performance results compared to other algorithms since it requires more processing power and consumes more resources when block size is relatively large.

The RC4 encryption algorithm was developed by Ronald Rivest of RSA. This is a shared key stream cipher algorithm which requires a secure exchange of a shared key which is outside the specification of the RC4 algorithm. The RC4 algorithm is used identically for encryption and decryption as the data stream is simply XORed with the generated key sequence. The algorithm is serial as it requires successive exchanges of state entries based on the key sequence. This encryption algorithm is used by standards such as IEEE 802.11 within WEP (Wireless Encryption Protocol) using a 40 and 128-bit keys.

In the algorithm the keystream is completely independent of the plaintext used. An 8 * 8 S-Box (S0 S255), where each of the entries is a permutation of the numbers 0 to 255, and the permutation is a function of the variable length key. There are two counters i, and j, both initialized to 0.

The VOCAL implementation of the RC4 encryption algorithms for the MIPS is available in several forms. The forms include pure optimized software and varying levels of hardware complexity utilizing UDI instructions. The RC4 operations are supported using UDI instructions for improved performance. When special assistance hardware is not available (as is the case on most general purpose processors), the RC4 byte manipulation/exchange operations are implemented via software.

1.2. Objectives

This project deems at analyzing three encryption algorithms which are Blowfish, RC4 and AES in terms of the following criteria:

- Encryption time- The encryption time is the time that an encryption algorithm takes to produce a cipher text from a plaintext. This time does not contain file I/O time.
- Decryption time- The decryption time is the time that a decryption algorithm takes to produce a plaintext from a cipher text. This time does not contain file I/O time.
- Throughput-The throughputof an encryption scheme define the speed of encryption. The throughput is calculated as the total plaintext in Kilobytes encrypted/encryption time (KB/sec). As the throughput increases, power consumption decreases.
- Memory Utilization: The Memory Utilization defines how much memory is being consumed while doing the encryption or decryption processes.

1.3. Justification

After this research is complete, security of data in transit would be highly improved and the following institutions would benefit:

- Financial Institutions
- Security Institutions

1.4. Limitations

During the research, the challenge encounter was that differences between the performance metrics of the various algorithms were not clearly visible for files with sizes less than 100KB.

2. Literature Review

2.1. Introduction

A number of people have conducted research on the comparative analysis of Blowfish, RC4 and AES with other algorithms in terms of Key Length, Encryption Time, Decryption Time, Throughput, Memory utilization and CPU time at different settings like variable key size and variable data packet size.

In the research conducted by Jawahar Thakur and Nagesh Kumar from the Department of Computer Science in Himachal Pradesh University on the topic Algorithms Simulation Based Performance Analysis using DES,AES and Blowfish. These algorithms were analyzed under different data loads using parameters such as speed, block size and key size. A simulation program was implemented with Java.

Their presented simulation results showed that Blowfish has a better performance than other common encryption algorithms used. Since Blowfish has not any known security weak points so far, this makes it an excellent candidate to be considered as a standard encryption algorithm. AES showed poor performance results compared to other algorithms since it requires more processing power.

Nidhi Singhland, J.P and S. Raina also conducted an experiment on Comparative Analysis of AES and RC4 Algorithms for Better Utilization. In their research they compared the AES algorithm with different modes of operation (block cipher) and RC4 algorithm (stream cipher) in terms of CPU time, encryption time, memory utilization and throughput at different settings like variable key size and variable data packet size.

Their paper revealed that RC4 is fast and energy efficient for encryption and decryption. Based on the analysis done as part of this research, RC4 is better than AES.

Apoorva and Yogesh Kumar conducted research on “Comparative Study of Different Symmetric Key Cryptography Algorithms” which was AES, Twofish CAST-256 and Blowfish. The comparison took into consideration the behavior and the performance of the algorithms when different data loads are used under different settings. Their comparison was made on the basis of these parameters: speed, block size and key size.

In their research, after comparing the various results that were obtained they concluded that the Blowfish is superior to other algorithms as it takes less time to encrypt and decrypt data.

2.2. Critique of the Existing Literature Relevant to the Study

In the literature review, all the experiments conducted by cryptanalyst were based on text files of varied sizes. They however neglected image, audio and video files of varied length.

3. Methodology

3.1. Research Design

For this experiment, I use a laptop 1.1 GHz Intel CPU and 2 GB Static RAM, in which performance data is collected. In the experiment, the laptop encrypts and decrypt different file sizes ranging from 0.7MB to 50MB. In this work, I am trying to find out performance comparison between block cipher (AES and Blowfish) and stream cipher (RC4) algorithm. Based on the analysis and result, I will conclude which algorithm is better to use based on different performance metrics.

The performance metrics analyzed regarding encryption algorithms are defined below:

- Encryption time- It is the time that an encryption algorithm takes to produce a cipher text from a plain text. Encryption time is used to calculate the throughput of an encryption process. In other words, it indicates the speed of the encryption process. The encryption time is generally calculated in milliseconds. It is the time taken by an encryption algorithm to encrypt the data. Less is the encryption time; more will be performance of that algorithm.
- Decryption time- It is the time that an encryption algorithm takes to produce a plain text from a cipher text. Decryption time is used to calculate the throughput of a decryption process. In other words, it indicates the speed of the decryption process. The decryption time is generally calculated in milliseconds. It is the time taken by an encryption algorithm to decrypt the data. Less is the decryption time; more will be performance of that algorithm.
- Throughput- The throughput of the encryption scheme is calculated as the total plain text in encrypted in Kbytes divided by the encryption time in milliseconds. The unit of throughput is KB/Sec. More is the throughput; more will be the performance. As the throughput increases, power consumption decreases.
- Memory Utilization: The Memory Utilization defines how much memory is being consumed during encryption or decryption process. The memory consumption is measured in bytes.

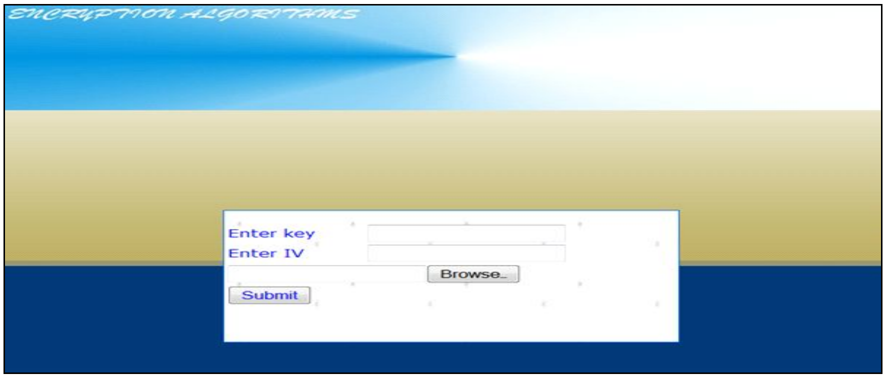


Figure 1: Graphical User Interface of the Stimulator

Figure 1 shows the screen shot of the software used for the evaluation. Firstly the user input 32 characters of key and 16 characters of Initialization Vector that would be used by the algorithm to encrypt and decrypt the message. The initialization vector becomes necessary when data needs to be encrypted in CBC and CFB since it is used to encrypt the key that would be used to encrypt the chunks of data.

After the key and Initialization vector are input, the user then use the browse button to select a file which has a size ranging from 0.5MB to 50 MB on the hard-drive. A prompt is displayed if the size of the file exceeds the specified range.

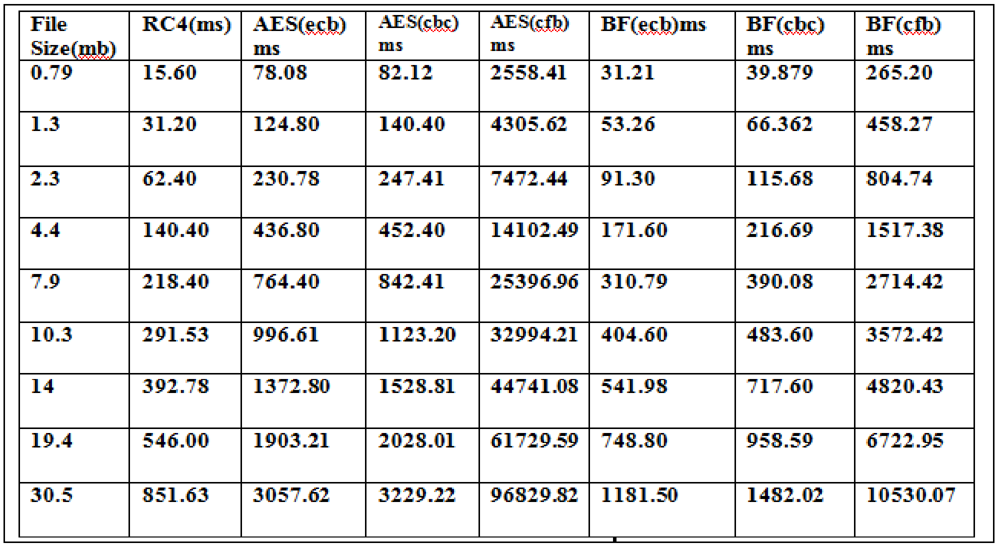
The submit button is used by the user to initiate the encryption and decryption of the file. A notification is displayed on the screen while the process is being executed.

During the encryption and decryption processes, the software automatically creates a file which copies the contents of the files being encrypted and decrypted into a folder on the user's hard-drive.

3.2. Performance Metrics of Encryption

The Encryption time of the algorithms was calculated by following steps:

- Select a file with size ranging from 0.79MB to 50MB from the hard-drive using the stimulator.
- Enter 32 characters of key and 16 characters of initialization vector which would be used to encrypt the file into the stimulator.
- Click the submit button to start the encryption process.
- Record the time that would be displayed on the graph after the stimulator as finished executing. This time is considered as the encryption time.
- Double click on a folder named encrypted on the hard-drive to view the contents of the encrypted file.
- Repeat the steps above for the encryption time of a different file size.



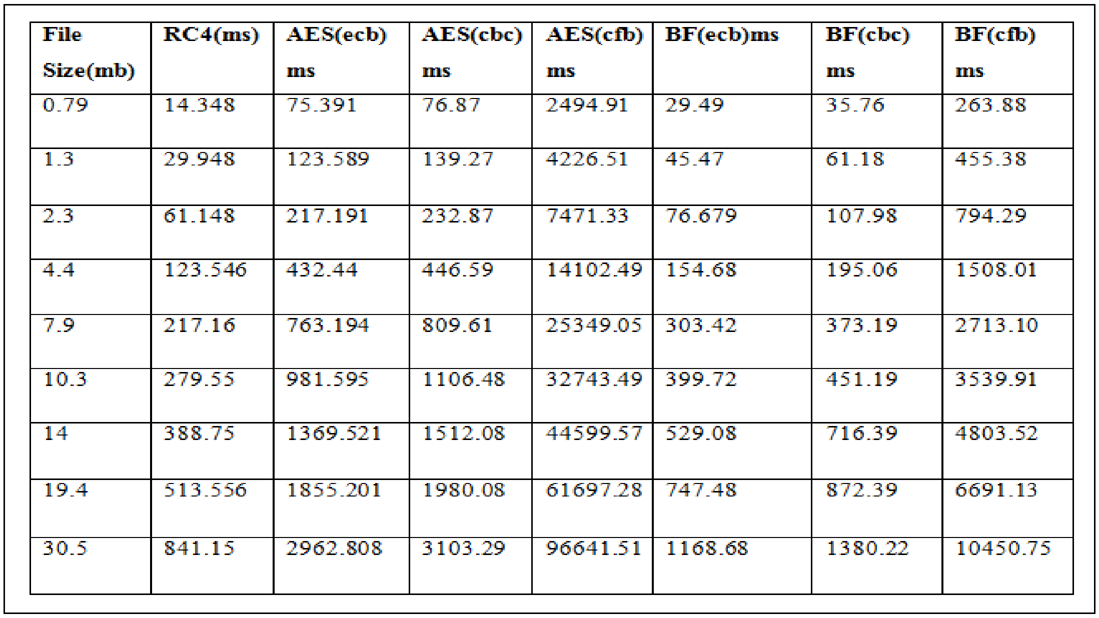
File Size(mb)	RC4(ms)	AES(ecb) ms	AES(cbc) ms	AES(cfb) ms	BF(ecb)ms	BF(cbc) ms	BF(cfb) ms
0.79	15.60	78.08	82.12	2558.41	31.21	39.879	265.20
1.3	31.20	124.80	140.40	4305.62	53.26	66.362	458.27
2.3	62.40	230.78	247.41	7472.44	91.30	115.68	804.74
4.4	140.40	436.80	452.40	14102.49	171.60	216.69	1517.38
7.9	218.40	764.40	842.41	25396.96	310.79	390.08	2714.42
10.3	291.53	996.61	1123.20	32994.21	404.60	483.60	3572.42
14	392.78	1372.80	1528.81	44741.08	541.98	717.60	4820.43
19.4	546.00	1903.21	2028.01	61729.59	748.80	958.59	6722.95
30.5	851.63	3057.62	3229.22	96829.82	1181.50	1482.02	10530.07

Table 1: Encryption time of RC4, AES and Blowfish

Table 1 shows the time that was recorded during the process of encryption. In the table it was seen that as the file size decreases, the encryption time also decreases since less bits are encrypted. The table also reveals that RC4 uses less time to perform its encryption follow by Blowfish and then Advanced Encryption Standard.

3.3. Performance Metrics of Decryption

The Decryption time of the algorithms is calculated while the stimulator is executing. Its uses the key and the initialization vector that were specified during the encryption process to decrypt the encrypted file and copy the contents of the decrypted file onto the user's hard-drive.



File Size(mb)	RC4(ms)	AES(ecb) ms	AES(cbc) ms	AES(cfb) ms	BF(ecb)ms	BF(cbc) ms	BF(cfb) ms
0.79	14.348	75.391	76.87	2494.91	29.49	35.76	263.88
1.3	29.948	123.589	139.27	4226.51	45.47	61.18	455.38
2.3	61.148	217.191	232.87	7471.33	76.679	107.98	794.29
4.4	123.546	432.44	446.59	14102.49	154.68	195.06	1508.01
7.9	217.16	763.194	809.61	25349.05	303.42	373.19	2713.10
10.3	279.55	981.595	1106.48	32743.49	399.72	451.19	3539.91
14	388.75	1369.521	1512.08	44599.57	529.08	716.39	4803.52
19.4	513.556	1855.201	1980.08	61697.28	747.48	872.39	6691.13
30.5	841.15	2962.808	3103.29	96641.51	1168.68	1380.22	10450.75

Table 2: Decryption time of RC4, AES and Blowfish

Table 2 shows the time that was recorded during the process of decryption. In the table it was seen that as the file size decreases, the decryption time also decreases since few bits are decrypted. The table also reveals that RC4 uses less time to perform its decryption follow by Blowfish and then Advanced Encryption Standard.

3.4. Performance Metrics of Memory Utilization

The type of memory that was used to perform the evaluation is SRAM (Static Random Access Memory) which is a type of memory that is faster and more reliable than the more common DRAM (dynamic RAM). The term static is derived from the fact that it doesn't need to be refreshed like dynamic RAM.

The memory utilization is evaluated by running the selected file through the stimulator. As the encryption and decryption processes are taken place, the system computes the memory consumption of the various algorithms.

File Size(MB)	AES(bytes)	Blowfish(bytes)	RC4(bytes)
0.792	2408040	2406712	1594376
1.3	4091016	4089688	2716360
2.3	7220424	7219096	4802632
4.4	13567656	13566328	9034120
7.9	24546784	24545456	16353536
10.3	31658368	31657040	21094568
14	43286272	43284944	28846504
19.4	59793680	59792352	39851448
30.5	93709672	93708344	62462104

Table 3: Memory utilization of RC4, AES and Blowfish in bytes

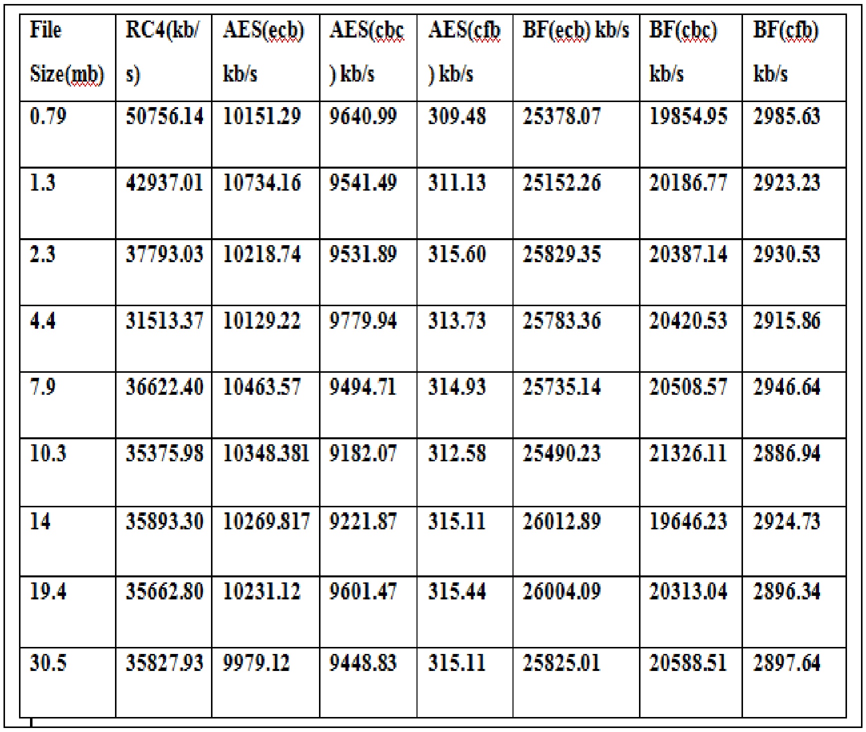
From Table 3 it can be seen that as the file sizes increases, memory consumption of the various algorithms also increases.

Advanced Encryption Standard utilized more memory followed by Blowfish and RC4 algorithms. This means that in order to use AES, you need a system with more memory before encryption and decryption can be executed.

3.5. Performance Metrics of Encryption Throughput

The Throughput of an encryption algorithm defines the efficiency of the algorithm. It is calculated as the total plain text encrypted in Kbytes divided by the encryption time in milliseconds. The unit of throughput is KB/Sec. More is the throughput; more will be the performance. As the throughput increases, power consumption decreases.

The Throughput of an encryption is evaluated by running the selected file from the user's hard-drive through the stimulator. As the encryption process is executing, the system computes the throughput for the various algorithms.



File Size(mb)	RC4(kb/s)	AES(ecb) kb/s	AES(cbc) kb/s	AES(cfb) kb/s	BF(ecb) kb/s	BF(cbc) kb/s	BF(cfb) kb/s
0.79	50756.14	10151.29	9640.99	309.48	25378.07	19854.95	2985.63
1.3	42937.01	10734.16	9541.49	311.13	25152.26	20186.77	2923.23
2.3	37793.03	10218.74	9531.89	315.60	25829.35	20387.14	2930.53
4.4	31513.37	10129.22	9779.94	313.73	25783.36	20420.53	2915.86
7.9	36622.40	10463.57	9494.71	314.93	25735.14	20508.57	2946.64
10.3	35375.98	10348.381	9182.07	312.58	25490.23	21326.11	2886.94
14	35893.30	10269.817	9221.87	315.11	26012.89	19646.23	2924.73
19.4	35662.80	10231.12	9601.47	315.44	26004.09	20313.04	2896.34
30.5	35827.93	9979.12	9448.83	315.11	25825.01	20588.51	2897.64

Table 4: Throughput for encryption of AES, Blowfish and RC4 in Kb/s

Table 4 shows summary of throughput of encryption for AES, Blowfish and RC4 algorithms. From the table, it can be seen that the larger the file size the lower the throughput since power consumption increases and more time is used in the encryption process.

4. Research Findings and Discussions

4.1. Simulation Results of Encryption

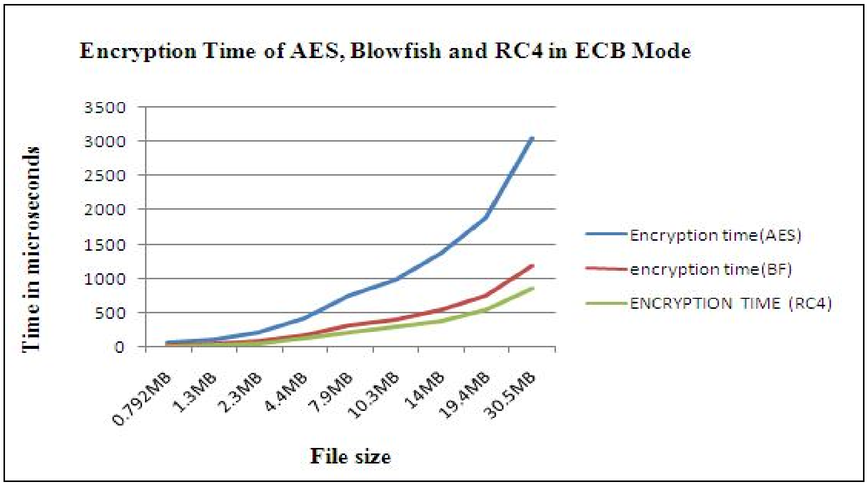


Figure 2: Encryption Times of AES, Blowfish and RC4 in ECB

In Figure 2, I show the performance of cryptographic algorithms in terms of encryption time in ECB mode. Here, I compared the encryption time of AES, Blowfish and RC4 algorithms over different packet size. RC4 takes less time to encrypt files than AES and Blowfish. This is because AES and Blowfish are block ciphers where the plain text is partitioned into large blocks and the encryption process is carried on each block separately. Encryption of each block depends on the previous block and the same key is used on each block while RC4 is a stream cipher where the different key is generated to encrypt each of the bits in the plain text and encoding of each bit depends on many of the previous bits. The data is however not partitioned into large blocks to slow the encryption process.
The same result was seen in CBC and CFB modes where RC4 showed superiority over the other algorithms.

4.2. Simulation Results of Decryption

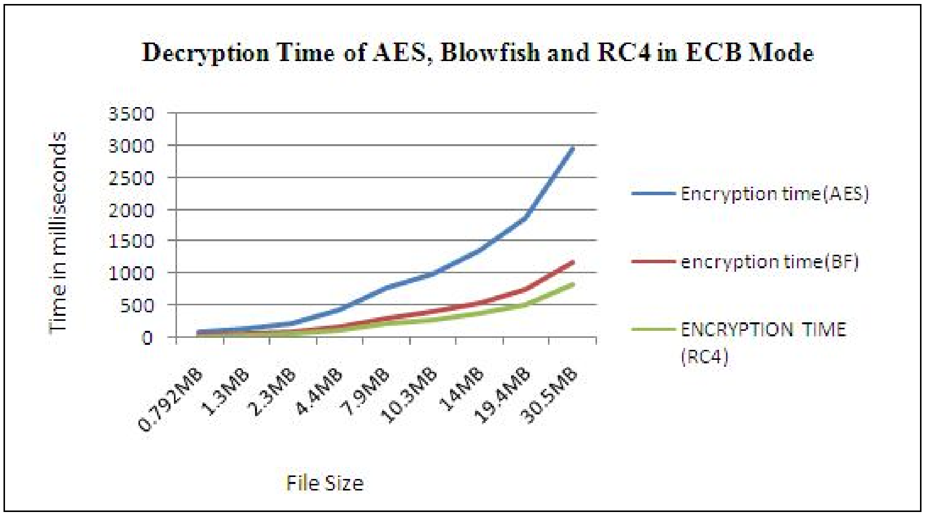


Figure 3: Decryption Time of AES, Blowfish and RC4 in ECB Mode

In Figure 3, I show the performance of cryptographic algorithms in terms of decryption time in ECB mode. Here, I compared the decryption time of AES,RC4 and Blowfish algorithms over different packet size. RC4 takes less time to decrypt files than AES and Blowfish. This is because RC4 is a stream cipher while Blowfish and AES are block ciphers which involve partition of the data into large block size before the decryption process is carried on each of the blocks.

The graph in Figure 4.2 also shows that decryption in ECB mode is faster than encryption in ECB mode as illustrated in Figure 4.2. Both encryption and decryption time also increase with the packet size. For example when the file size was 1.3 MB, the decryption time was seen to be 29.948 ms while 62.40ms was recorded for RC4 algorithm for a file of size 2.3MB.

4.3. Simulation Results of Memory Utilization

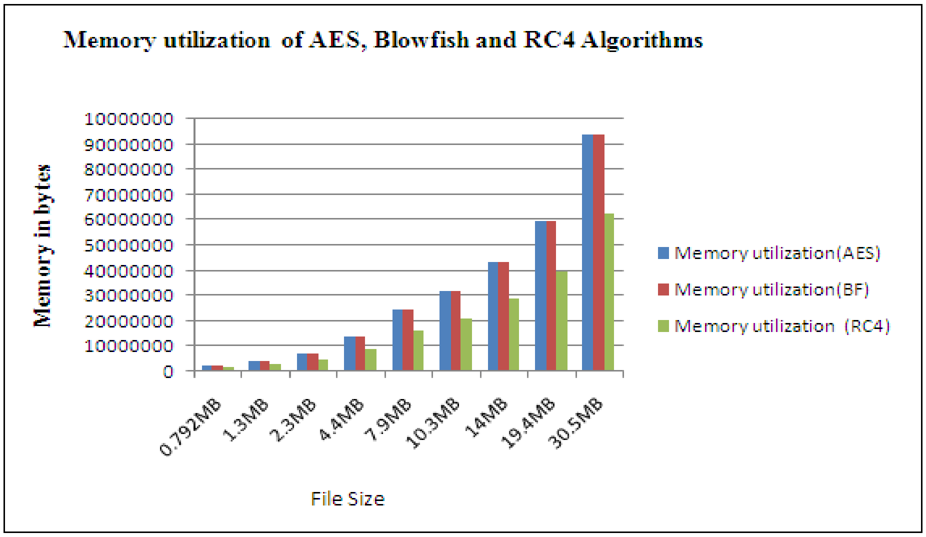


Figure 4: Memory utilizations of AES, Blowfish and RC4 algorithms

Figure 4 shows performance analysis in terms of memory utilization. As shown in the graph, RC4 consume less memory than AES and Blowfish because AES and Blowfish areblock ciphers and they work on larger chunks of data and often have "carry over" from previous blocks whereas RC4 is a stream cipher and works on only a few bits at a time. They have relatively low memory requirements and therefore cheaper to implement in limited scenarios such as embedded devices, firmware and hardware.

As the file size increases, memory sizes are drastically increased which means for extra-large files, we need a system with good memory and more CPU. For example when the file size was 0.79MB an amount of 1594376 bytes of memory was used in RC4 encryption and decryption while with 1.3MB of file size 2716360 bytes of memory used to perform encryption and decryption operations in RC4.

4.4. Simulation Results of Encryption Throughput

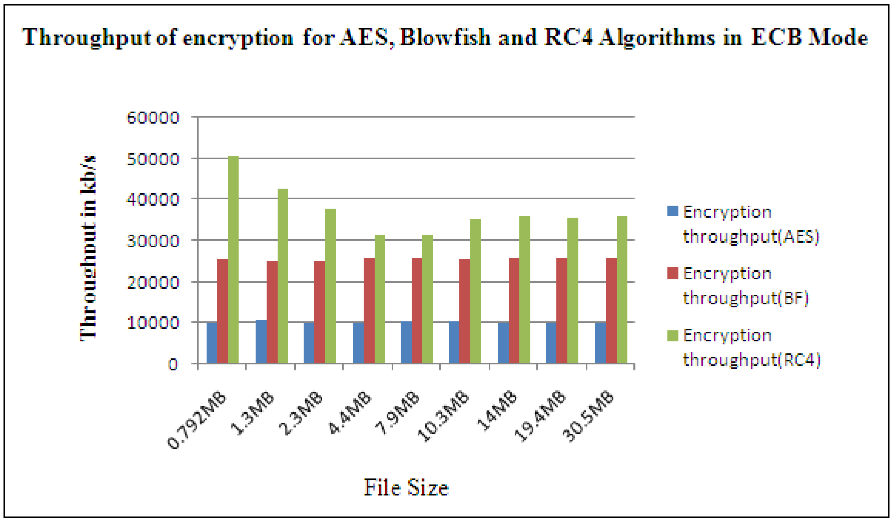


Figure 5: Throughput of encryption for AES, Blowfish and RC4 in ECB Mode

Another important performance metrics that is used to evaluate the efficiency of an encryption algorithm is the Throughput. In Figure 4.8, I show the Throughput of encryption for the various algorithms in ECB mode.Here, I compared the Throughput of AES, Blowfish and RC4 algorithms over different packet size in ECB mode. RC4 was seen to have a higher Throughput followed by Blowfish and AES. This is because RC4 is a stream cipher so it takes less time to encrypt files than AES and Blowfish which are block ciphers.

The throughput of encryption also decreases with increasing file size. This implies that the larger the file size, the lower the Throughput. For example in RC4 algorithm, when the file size was 0.79 MB the throughput of encryption was 50756.14 Kb/s while 42937.01 Kb/s was recorded for a file of size 1.3MB.

5. Conclusion and Recommendations

5.1. Conclusion

This work entitled “Comparative Analysis of AES, RC4 and Blowfish Algorithms for Better Utilization” presents a performance evaluation of RC4, AES and Blowfish algorithms. The performance metrics were throughput, CPU process time, memory utilization, and encryption and decryption time. Experiments show that the RC4 is fast and energy efficient for encryption and decryption. Based on the analysis done as part of this research, RC4 is better followed by Blowfish. AES is however slow and consumes more memory than both RC4 and Blowfish algorithms.

It was also found out that ECB mode of encryption is the fastest followed by CBC. CFB was found to be the slowest. This explains why throughputs of encryption in ECB mode were seen to be the highest in all the packet size chosen for encryption.

Finally the experiment also reveals that decryption is faster than encryption. However for small packet size of data this difference is hardly to be seen since is measured in milliseconds.

5.2. Recommendation

Even though RC4 is betteras compared to Blowfish and AES, PaulMaîtrediscovered a secret key by using the initial state table. They generated some equation on the bases of initial state table and they selected some of the bytes of secret key on the bases of guess and the remained secret key was found out by using their equation.

So the security of RC4 depends on the security of the secret key and the internal states of S-box, so many attacks focus on resuming the secret key of the internal states of the state-box.

This problem can be solved by dividing the main key into three sub keys. If the length of the main key is not divisible by the three then the key would be padded with zero to make it divisible by three. The encryption and the decryption processesare then taken through three rounds each round uses one of the sub keys generated.

During the encryption process, in the first stage, the plaintext XOR with the key stream generated on the basis of first key then in the second stage, the encrypted output of the of the first stage XOR with the key stream generated with the help of second sub key and then in the final stage, the second double encrypted message then again encrypted with the key stream generated on the basis of the third sub key.

The new algorithm is stronger than the previous one as it takes more time to find out the key as compared to the previous algorithm used in RC4.

This approach also requires more resources and is slower than the previous algorithm because of the three key processes. But it proves to be more secured.

6. References

1. Apoorva, Yogesh Kumar, “Comparative Study of Different Symmetric KeyCryptography Algorithms”, International Journal of Application or Innovation in Engineering & Management (IJAIEM),Volume 2, Issue 7, July 2013, pp. 10-15.
2. AllamMousa and Ahmad Hamad (2006), “Evaluation of the RC4 Algorithm for Data Encryption”, International Journal of Computer Science Applications Vol. 3, No.2, June 2006, pp. 44-56.
3. A.W.Naji, A.A.Zaidan, B.B.Zaidan, Shihab A, Othman O. Khalifa, “Novel
4. Approach of Hidden Data in the (Unused Area 2 within EXE File) Using Computation between Cryptography and Steganography”, International Journal of Computer Science and Network Security (IJCSNS), Vol.9, No.5, and ISSN: 1738-7906, pp. 294-300.
5. AnasMajed Hamid, Miss Laiha Mat Kiah, Hayan .T. Madhloom, B.B Zaidan, A.A
6. Zaidan,” Novel Approach for High Secure and High Rate Data Hidden in the Image Using Image Texture Analysis”, International Journal of Engineering and Technology (IJET), Published by: Engg Journals Publications, 2005, ISSN:0975-4042, Vol.1, NO.2, pp. 63-69.
7. A.W. Naji, Shihab A. Hameed, B.B.Zaidan, Wajdi F. Al-Khateeb, Othman O.
8. Khalifa, A.A.Zaidan and Teddy S. Gunawan, “ Novel Framework for Hidden Data in the Image Page within Executable File Using Computation between Advance Encryption Standard and Distortion Techniques”, International Journal of Computer Science and Information Security (IJCSIS), Vol. 3, No 1 ISSN: 1947-5500, pp. 73-78,3 Aug 2009, USA.
9. A.A. Noman, Dr. Roslina b. Mohd. Sidek, Dr. A.R.b. Ramli, Dr. L. Ali, “RC4
10. Stream Cipher for WLAN Security: A Hardware Approach”, 5th International Conference on Electrical and Computer Engineering, ICECE, 2008, pp. 50-63.
11. AtulKahate,“Cryptography and Network Security”, 2008 pp. 123-125.
12. Bruce Schneier, “Applied Cryptography “, John Wiley and Sons, New York, 1994pp. 15-22.
13. ChallaNarasimham , JayaramPradhan (2008), “Evaluation of PerformanceCharacteristics of Cryptosystem Using Text Files”, Journal of Theoretical and Applied Information Technology, pp. 254-259.
14. DiaaSalama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie
15. Mohamed Hadhoud (2008), “Performance Evaluation of Symmetric Encryption Algorithms”, IJCSNS, VOL.8 No.12, December 2008, pp. 280-286.
16. Jawahar Thakur, Nagesh Kumar, “Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis”, International Journal of Emerging Technology and Advanced Engineering Volume 1, Issue 2, December 2011)pp. 1-20.
17. JianXie, Xiaozhong Pan, “An Improved RC4 Stream Cipher”, International Conference on Computer Application and System Modeling (ICCASM), 2010 pp. 120-123.
18. Lavanya P and M. RajashekharaBabu (2011), “Performance Analysis of
19. Montgomery Multiplication Algorithm for Multi-core Systems Using Concurrent Java”, Journal of Advances in Applied Science Research, 2011, pp. 567-573.
20. Mingyan Wang, YanwenQue (2009),“The Design and Implementation of Passwords Management System Based on Blowfish Cryptographic Algorithm”, International Forum on Computer Science-Technology and Applications, 2009. Pp. 24-28.
21. M. Abomhara, Omar Zakaria, Othman O. Khalifa,A.A.Zaidan, B.B.Zaidan,
22. “Enhancing Selective Encryption for H.264/AVC Using Advance Encryption Standard “, International Journal of Computer and Electrical Engineering (IJCEE), ISSN: 1793-8198, Vol.2, NO.2, April 2010, Singapore, pp.190-240
23. NidhiSinghal, J.P. andS.Raina, “Comparative Analysis of AES and RC4 Algorithms forBetter Utilization “,International Journal of Computer Trends and Technology- July to Aug Issue 2011, pp. 20-26.