Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 617 – 624

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish

Priyadarshini Patil[a,*], Prashant Narayankar[b],Narayan D G [c], Meena S M[d]

[a]*Priyadarshini Patil,Department of Information Science & Engineering , BVBCET , Hubli 5800031,India*
[b]*Prashant Narayankar,Department of Information Science & Engineering , BVBCET , Hubli 5800031,India*

Abstract

In today's internet era, with online transactions almost every second and terabytes of data being generated everyday on the internet, securing information is a challenge. Cryptography is an integral part of modern world information security making the virtual world a safer place. Cryptography is a process of making information unintelligible to an unauthorized person. Hence, providing confidentiality to genuine users. There are various cryptographic algorithms that can be used. Ideally, a user needs a cryptographic algorithm which is of low cost and high performance. However, in reality such algorithm which is a one stop solution does not exist. There are several algorithms with a cost performance trade off. For example, a banking application requires utmost security at high cost and a gaming application sending player pattern for analytics does not bother much about security but needs to be fast and cost effective. Thus, amongst the cryptographic algorithms existing, we choose an algorithm which best fits the user requirements. In, this process of choosing cryptographic algorithms, a study of strengths, weakness, cost and performance of each algorithm will provide valuable insights. In our paper, we have implemented and analyzed in detail cost and performance of popularly used cryptographic algorithms DES, 3DES, AES, RSA and blowfish to show an overall performance analysis, unlike only theoretical comparisons.

Peer-review under responsibility of organizing committee of the ICISP2015

Keywords:AES;Blowfish; DES;3DES;RSA;

1. Introduction

In today's world of gadget addiction, information storage, processing and retrieval are computer based. The

**E-mail address:priydarshini.patil@bvb.edu*

Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.108

government, judiciary, small to big enterprises and almost every individual is using computer and internet based services. This puts a huge responsibility on computer scientists and especially information security scientists as the bad people out there are also evolving fast with technology. With convenience and ease of use provided by technology, certain risks are posed. We all are very happy with technology at our finger tips on mobiles and computers. Various online applications like shopping apps, banking apps, social networking apps provide services round the clock. But if an attacker gets a banking password, money is stolen at the same ease. An attacker may acquire social media login credentials and use it for mischievous activities. Hence, securing information on computer, information sent via network, and information residing in applications is necessary. Cryptography is one such mechanism used in securing information and we will be analyzing cryptographic algorithms in our paper.

2. Related Work

[1]Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures by Yogesh Kumar, Rajiv Munjal, and Harsh gives us theoretical comparison of symmetric and asymmetric cryptography algorithms.[2]Comparative analysis of performance efficiency and security measures of some encryption algorithms by AL.Jeeva, V.Palanisamy, K.Kanagaram compares symmetric and asymmetric cryptography algorithms using parameters key length , tunability ,speed , encryption ratio and security attacks. [3]New comparative study between DES, 3DES and AES within nine factors by Hamdan.O.Alanazi, B.B.Zaidan, .A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani compares DES,3DES and AES algorithms with nine factors key length , cipher type, block size, developed year ,cryptanalytic resistance , possible keys, possible ascii keys and time required to check all possible keys . [4]Comparative study of symmetric and asymmetric cryptography techniques by Ritu Tripathi, Sanjay Agrawal compares symmetric and asymmetric cryptography techniques using throughput, key length, tunability, speed, encryption ratio and security attacks.[5]Evaluation of blowfish algorithm based on avalanche effect by Manisha Mahindrakar gives a new performance measuring metric avalanche effect.

Here, there are theoretical comparisons done but not supported with results and implementations. We have gone a step ahead and implemented the algorithms and measured performance of an application with respect to cryptographic strength and system performance in terms of cost and response time. The metrics encryption time and decryption time tell us the responsiveness of the application. The metrics memory used and number of bits required to encode optimally to measure cost has not been used in any experiments till now. The metrics entropy and avalanche effect to measure cryptographic strength and resistance against attacks have also been not used in any experiments till now. Hence, we have used new metrics in analyzing the performance of the algorithms.

3. Algorithms in our Experiment

3.1. DES

Data Encryption Standard (DES) is a symmetric key block cipher. The key length is 56 bits and block size is 64 bit length. It is vulnerable to key attack when a weak key is used. DES was found in 1972 by IBM using the data encryption algorithm. It was adopted by the government of USA as standard encryption algorithm. It began with a 64 bit key and then the NSA put a restriction to use of DES with a 56- bit key length, hence DES discards 8 bits of the 64 bit key and then uses the compressed 56 bit key derived from 64 bit key to encrypt data in block size of 64-bits .DES can operate in different modes - CBC, ECB, CFB and OFB, making it flexible. It is vulnerable to key attack when a weak key is used. In 1998 the supercomputer DES cracker, with the help of lakh's of distributed PCs on the Internet, cracked DES in 22h.

3.2. 3DES

[9]In cryptography, Triple DES is also called Triple Data Encryption Algorithm which is a block cipher. Triple Data Encryption Standard (3DES) was first published in 1998 which gets its name so because it applies DES cipher

three times to each block of data, Encryption – Decryption – Encryption using DES. The key length is 112 bits or 168 bits and block size is 64 bit length. Because of the increasing computational power available these days and weak of the original DES cipher, it was subject to brute force attacks and various cryptanalytic attacks; Triple DES was designed to provide a relatively simple method of increasing the key size of DES to protect against such attacks, without designing a completely new block cipher algorithm.

3.3. AES

[6]Advance Encryption Standard (AES) algorithm was developed in 1998 by Joan Daemen and Vincent Rijmen, which is a symmetric key block cipher.AES algorithm, supports any combination of data and key length of 128, 192, and 256 bits. AES allows a 128 bit data length that can be split into four basic operational blocks. These blocks are considered as array of bytes and organized as a matrix of the order of 4×4 which is also called as state and subject to rounds where various transformations are done. For full encryption, the number of rounds used is variable N = 10, 12, 14 for key length of 128,192 and 256 respectively. Each round of AES uses permutation and substitution network, and is suitable for both hardware and software implementation.

3.4. Blowfish

[7]Blowfish was first published in 1993 .It is a symmetric key block cipher with key length variable from 32 to 448 bits and block size of 64 bits. Its structure is fiestal network. Blowfish is a symmetric block cipher that can be used as a informal replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and commercial use. Blowfish was designed by Bruce Schneier as a fast, free alternative to existing encryption algorithms. From then it has been analyzed considerably, and it is slowly gaining popularity as a robust encryption algorithm. Blowfish is not patented, has free license and is freely available for all uses.

3.5. RSA

[8]RSA is founded in 1977 is a public key cryptosystem. RSA is an asymmetric cryptographic algorithm named after its founders Rivest, Shamir &Adelman. It generates two keys: public key for encryption and private key to decrypt message .RSA algorithm consist of three steps, step one is key generation which is to be used as key to encrypt and decrypt data, step two is encryption, where actual process of conversion of plaintext to cipher text is being carried out and third step is decryption, where encrypted text is converted in to plain text at other side.RSA is based on factoring problem of finding product of two large prime numbers. Key size is 1024 to 4096 bits.

4. Implementation

We have implemented and compared DES, 3DES, AES, blowfish and RSA. We have implemented the algorithms in java using Eclipse IDE .We have used packages java security and java crypto .The packages java crypto and security provides security features like encryption , decryption , key generation , key management infrastructure , authentication and authorization features. However, blowfish is not provided in java security and crypto library. We implemented blowfish in java, converted into a jar and added blowfish jar to crypto library externally. We have used files of sizes 25KB, 50KB, 1MB, 2MB, 3MB consisting of text and images as input for encryption. The encrypted output of each file is saved as a file, which in turn is input for decryption. For sake of comparison we have used the same input files for all algorithms throughout the experiment. We have used a same system for all implementations and analysis work, so that memory and processor conditions remain same for all algorithms for comparison. All block cipher algorithms are set in a same mode ECB which is default in java crypto and security.

Java crypto and security package contains the classes and interfaces that implement the Java security architecture.

These classes can be broadly divided into two categories. First, the classes that implements cryptography to perform operations for information to be transmitted. Second, there is authentication and access control classes that implement message digests and digital signatures and can authenticate users and other objects. Using the libraries of this package, we implement various cryptographic algorithms making minor changes in the calling functions. The method of implementing algorithms using functions of java.security and java.crypto package is as follows: Generate key using key generator class, create a cipher object with parameters algorithm name and mode, initialize the cipher created for encryption/decryption and perform encryption/decryption using doFinal() method

5. Evaluation Parameters

Each of the encryption techniques has its own strong and weak points. In order to apply a suitable cryptography algorithm to an application, we should have knowledge regarding performance, strength and weakness of the algorithms. Therefore, these algorithms must be analyzed based on several features. In this paper, analysis is done with following metrics under which the cryptosystems can be compared are described below:

5.1. Encryption time

The time taken to convert plaintext to ciphertext is encryption time. Encryption time depends upon key size, plaintext block size and mode. In our experiment we have measured encryption time in milliseconds. Encryption time impacts performance of the system. Encryption time must be less making the system fast and responsive.

5.2. Decryption time

The time to recover plaintext from ciphertext is called decryption time. The decryption time is desired to be less similar to encryption time to make system responsive and fast. Decryption time impacts performance of system. In our experiment, we have measured decryption time is milliseconds.

5.3. Memory used

Different encryption techniques require different memory size for implementation. This memory requirement depends on the number of operations to be done by the algorithm, key size used, initialization vectors used and type of operations. The memory used impacts cost of the system. It is desirable that the memory required should be as small as possible.

5.4. Avalanche effect

In cryptography, a property called diffusion reflects cryptographic strength of an algorithm. If there is a small change in an input the output changes significantly. This is also called avalanche effect. We have measured Avalanche effect using hamming distance. Hamming distance in information theory is measure of dissimilarity. We find hamming distance as sum of bit by bit xor considering ascii value, as it becomes easy to implement programmatically. A high degree of diffusion i.e. high avalanche effect is desired. Avalanche effect reflects performance of cryptographic algorithm.

$$\text{Avalanche effect} = (\text{hamming distance} \div \text{file size}) \quad (1)$$

5.5. Entropy

Randomness is an important property in cryptographic processes because information should not be able to be guessed by an attacker. Entropy is measure of randomness in the information. It measures uncertainty in the

information. In information security, we require security algorithms to yield high randomness in encrypted message, so that there is less or no dependency between key and ciphertext. With high randomness, the relationship between key and ciphertext becomes complex. This property is also called confusion. A high degree of confusion is desired to make it difficult to guess to an attacker. Entropy reflects performance of cryptographic algorithm. We calculate entropy using Shannon's formula.

5.6. Number of bits required for encoding optimally

The number of bits required to encode an encrypted character should be less. Since, the encrypted bit will be transmitted over a network after encoding, this metric tell us the bandwidth required for transmission. If an encrypted bit is encoded with fewer bits, it will consume lesser bandwidth and also lesser storage. Hence, this impacts cost.

6. Results and Discussions

In this section we discuss the results obtained based on six evaluation parameters.

6.1. Encryption time

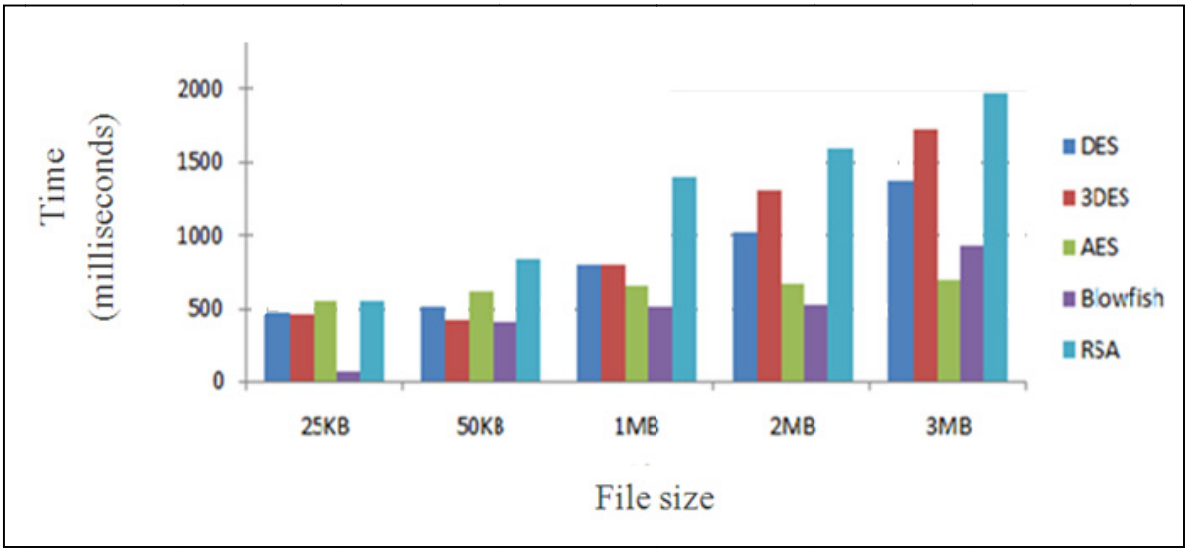

Fig. 1. Encryption time vs. File size for DES, 3DES, AES, Blowfish and RSA.

Fig. 1. Shows that RSA takes highest time for encryption, and blowfish takes least time for encryption, being fastest.3DES is a trick to reuse DES implementations by cascading three instances of DES with distinct keys. 3DES is believed to be secure up to at least "2^{112}" security was designed for efficient hardware implementation but it is less efficient in software. Blowfish consumes the least time among all. Blowfish is efficient in software, at least on some software platforms. It uses key-dependent lookup tables; hence performance depends on how the platform handles memory and caches.

6.2. Entropy

Table 1. Average entropy values.

	DES	3DES	AES	Blowfish	RSA
Average entropy per byte of encryption	2.9477	2.9477	3.84024	3.93891	3.0958

Table 1 shows that Blowfish scores highest average entropy per byte of encryption. Entropy is a measure of degree of randomness of information. Randomness is an important and desirable property of cryptographic algorithms.AES heavily uses s boxes and p boxes, whereas Blowfish also uses round function on s- array and p-array. Hence, both AES and Blowfish yield high degree of randomness in output information, making the output less susceptible to attacks.

6.3. Decryption time

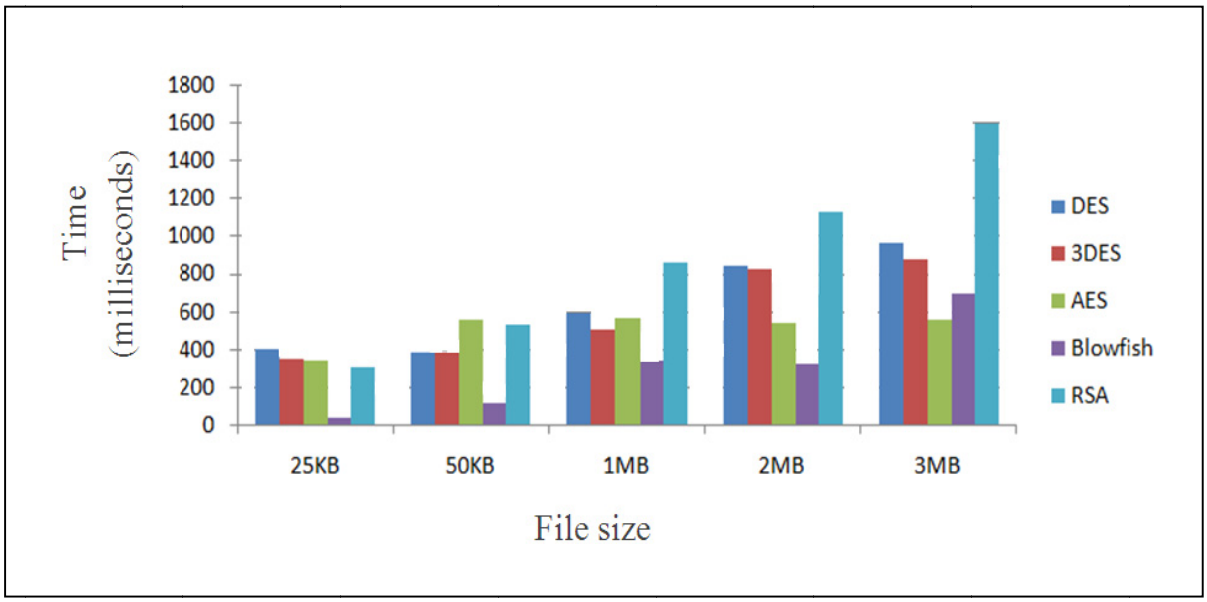

Fig. 2. Decryption time vs. File size for DES, 3DES, AES, Blowfish and RSA.

Fig. 2. shows that all algorithms take less time for decryption than encryption, RSA takes highest time for decryption, and blowfish takes least time for decryption, being fastest.RSA being public key cryptosystem uses one way function which is hard to invert using prime numbers. The use of modular exponentiation, multiplicative inverse and two keys public and private key makes RSA slow compared to symmetric key algorithms.

6.4. Memory Used

Table 2. Comparison of memory used.

Algorithm	Memory Used(KB)
DES	18.2

3DES	20.7
AES	14.7
Blowfish	9.38
RSA	31.5

Table 2 shows that memory used for unit operations for listed algorithms. Blowfish consumes least memory whereas RSA consumes highest memory per unit of operation.DES and AES require medium size of memory. Therefore, if the demand of any application is the smallest memory size the Blowfish is the best option.

6.5. Avalanche Effect

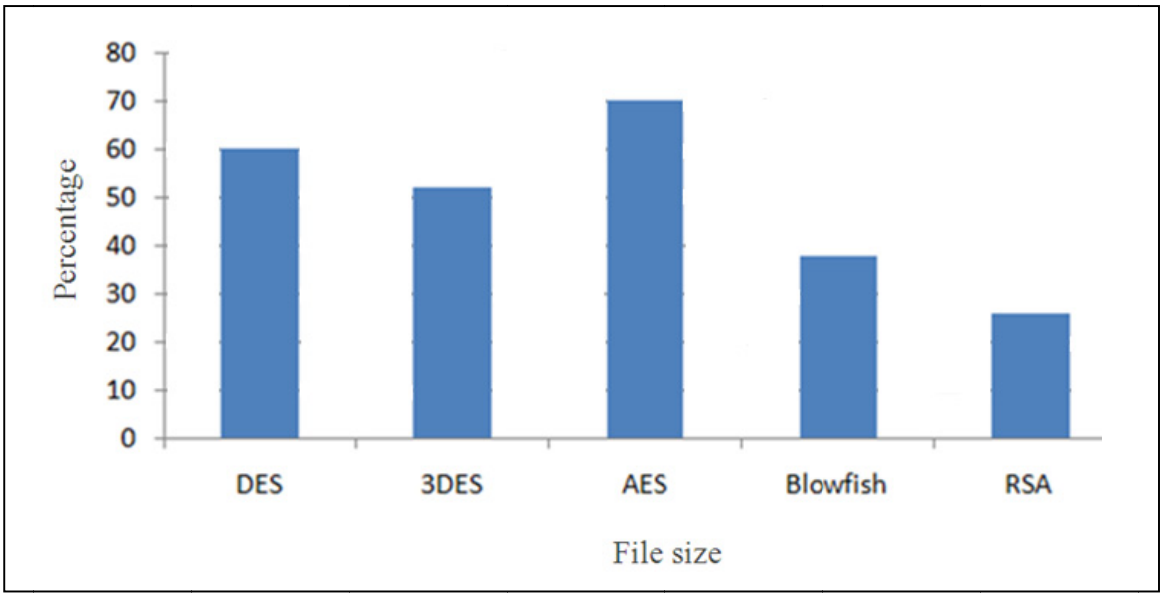

Fig. 3. Avalanche effect for DES, 3DES, AES, Blowfish and RSA.

Fig.3. Shows that AES exhibits highest Avalanche effect whereas RSA exhibits least Avalanche effect. Avalanche effect tells us the degree of diffusion of information .A change of one bit in plaintext leading to significant change in bits of output information.AES uses a substitution permutation network using multiplicative inverse and affine transformations over a galois field leading to high mixing of information leading to high diffusion in output.

6.6. Number of bits required to encode optimally

Table 3. Optimal encoding length

	DES	3DES	AES	Blowfish	RSA
Average number of bits required to optimally encode a byte of encrypted data	27	40	256	128	44

Table 3 shows that AES requires highest number of bits to be encoded optimally an encrypted data and DES requires least number of bits to be encoded optimally, indicating AES requires highest bandwidth for transmission.

7. Conclusion

Each of the encryption techniques has its own strong and weak points. In order to apply a suitable cryptography algorithm to an application, we should have knowledge regarding performance, strength and weakness of the algorithms. From the experiment results, it is evident that the memory required for implementation is smallest in blowfish whereas it is largest in RSA. DES and AES require medium size of memory. Therefore, if the demand of any application is the smallest memory size the Blowfish is the best option; Results shows that RSA consumes more time for encryption and decryption compared to others. Blowfish consumes the least time amongst all. Blowfish is efficient in software, at least on some software platforms. After evaluating algorithms based on parameter Avalanche effect AES scores highest; we can conclude that AES can be used in applications where confidentiality and integrity is of highest priority. Evaluating DES, 3DES, AES, Blowfish and RSA based on parameters entropy, Blowfish scores highest; hence we can conclude that Blowfish is strongest against guessing attacks. Results shows that AES requires highest number of bits to be encoded optimally an encrypted data and DES requires least number of bits to be encoded optimally, indicating AES requires highest bandwidth for transmission. If time and memory is a major factor in the application, Blowfish is the best suited algorithm. If cryptographic strength is a major factor in the application, AES is the best suited algorithm. If network bandwidth is a major factor in the application; DES is the best suited algorithm. We can evaluate other cryptographic techniques on similar lines considering other performance metrics and implement the best-fit algorithm for a targeted application.

References

1.Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures byYogesh Kumar, Rajiv Munjal, and Harsh ,(IJAFRC) Volume 1, Issue 6, June 2014. ISSN 2348 - 4853

2.Comparative analysis of performance efficiency and security measures of some encryption algorithms by AL.Jeeva, Dr.V.Palanisamy, K.Kanagaram compares symmetric and asymmetric cryptography algorithms ISSN: 2248-9622

3. New Comparative Study Between DES, 3DES and AES within Nine Factors Hamdan.O.Alanazi, B.B.Zaidan, . A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani JOURNAL OF COMPUTING, VOLUME 2, ISSUE 3, MARCH 2010, ISSN 2151-9617

4. Comparative Study of Symmetric and Asymmetric Cryptography Techniques by Ritu Tripathi, Sanjay Agrawal compares Symmetric and Asymmetric Cryptography Techniques using throughput, key length, tunability, speed, encryption ratio and security attacks. IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011 ISSN (Online): 2231-5268

5. Evaluation of Blowfish Algorithm based on Avalanche Effect by Manisha Mahindrakar gives a new performance measuring metric avalanche effect. International Journal of Innovations in Engineering and Technology (IJIET) 2014

6. Efficient Implementation of AES, RituPahal, Vikaskumar, Volume 3, Issue 7, July 2013 ISSN: 2277 128X, © 2013, IJARCSSE

7. Superiority of blowfish Algorithm ,Pratap Chandra Mandal , Volume 2, Issue 9, September 2012 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering

8. A study and performance of RSA algorithm, IJCSMC, Vol. 2, Issue. 6, June 2013, pg.126 – 139, ISSN 2320– 088X

9. Data encryption and decryption by using triple DES and performance analysis of crypto system, Karthik .S ,Muruganandam .A, ISSN (Online): 2347-3878 Volume 2 Issue 11, November 2014