Performance Analysis of Cryptographic Algorithms in the Information Security

U. Thirupalu[1]
Research Scholar
Dept. of Computer Science
S V U CM&CS-Tirupati
India-517502

Dr. E. Kesavulu Reddy[2] Ph. D, FCSRC (USA)
Assistant Professor
Dept. of Computer Science
S V U CM&CS-Tirupati-A.P
India-517502

Abstract: **Information security is the process of protecting information. It protects its availability, privacy and integrity. The two main characteristics that identify and differentiate one encryption algorithm from another are its ability to secure the protected data against attacks, speed and efficiency. security is the most challenging issue in the world and the various security threats in the cyber security has to be avoided and to give more confidentiality to the users and to enable high integrity and availability of the data. The encryption of the data by using the various data encryption algorithms will provide the additional security to the data being transmitted. This paper mainly focuses on comparative analysis of (AES, DES, 3DES, BLOWFISH, RC4), Asymmetric (RSA, DSA, Diffie-Hellman, EI-Gamal, Pailier), Hashing (MD5, MD6, SHA, SHA256) algorithms.**

Keywords: Encryption. Decryption, Data Security, Key size, information security, Symmetric algorithms, Asymmetric Algorithms.

I. INTRODUCTION

The cryptosystems are processing with different types of cryptographic algorithms. These cryptographic algorithms are used for encryption of data and decryption of data using of shared keys or single key.These are fall into two categories i.e. 1. Public key cryptosystem or Asymmetric key cryptosystem.2. Secret key cryptosystem or Symmetric key cryptosystem.

II. LITERATURE SURVEY

Encryption algorithm plays a vital role, to provide secure communication over the network. Encryption is the fundamental tool for protecting the data. Encryption algorithm converts the data into scrambled form by using "the key" and only user have the key to decrypt the data The techniques in Security algorithms are Symmetric Algorithms and asymmetric Algorithms.

A. Symmetric Algorithms

- D E S
- 3 D E S
- BLOWFISH
- RC5
- RC6
- A E S
- IDEA
- Homomorphic Encryption
- *DES*

DES is first block symmetric encryption algorithm published by NIST designed by IBM on 1974. The same key is used for both encryption and decryption; DES uses 64-bit key in terms of 8-bits for error correction and 56-bits as a key but in every byte 1 bit in has been selected as a 'parity' bit, and is not used for encryption mechanism. The 56 bit is permuted into 16 sub- keys each of 48- bit length. It also contains 8 S- boxes and same algorithm is used in reversed for decryption [1]. The implementations of the DES (data encryption standard) algorithm based on hardware are low cost, flexible and efficient encryption solutions.

Algorithm:

DES_ Encrypt (X, Y) where E = (L, R)

X ← IP (M)

\For round ←1 to 16 do

Yi ←SY (Y, round)

L ←L xor F(R, Ki)

swap (L, R)

End

swap (L, R)

X←IP^{-1}(X)

return X.

End

- *Triple-DES*

TDES is an enhanced version of DES is based on Feistel structure. The CPU power consumed by TDES is three times more than DES. The 3DES uses a 64 bit plain text with 48 rounds and a Key Length of 168-bits permuted into 16 sub- keys each of 48- bit length. It also contains 8 S-boxes and same algorithm is used in reversed for decryption [2]. Triple DES the algorithm is considered to be practically secure, in spite of having theoretical attacks.

Algorithm

For j = 1 to 3
{
C**j,0** = IV**j**
For i = 1 to n**j**

{

C**j,i** = E**K3** (D**K2** (E**K1** (P**j,i** C**j,i-1**)))

Output C**j,i**
}
}

❖ *Blowfish*

Blowfish algorithm was first introduced in 1993.The Blowfish is highly rated secure variable length key encryption algorithm with different structure and functionality than all other algorithms. Blowfish is a block cipher that uses a 64 bit plain text with 16 rounds, allowing a variable key length, up to 448 bits, permuted into 18 sub-keys each of 32- bit length and can be implemented on 32- or 64-bit processors. It also contains 4 S- boxes and same algorithm is used in reversed for decryption [3].

Algorithm

Divide x into two 32-bit lengths : x**L**, xM

For i = 1to 16:

X**L**= X**L** XOR P**i**

x**M** = F (X**L**) XOR x**M**

Swap X**L** and x**M**

Next i

Swap X**L** and x**M** (Undo the last swap.)

x**M** = x**M** XOR P**17**

x**L** = x**L** XOR P**18 then**

Combine XL and x**M.**

❖ *RC5*

RC5 was developed in 1994. The key length if RC5 is MAX2040 bit with a block size of 32, 64 or 128. The use of this algorithm shows that it is Secure. The speed of this algorithm is slow. [3]

Algorithm

A = A + S[0];

B = B + S[1];

for i = 1 to r do

A = ((A Xor B) <<< B) + S[2 * i]

B = ((B Xor A) <<< A) + S[2 * i + 1]
Next

❖ *AES*

AES is a block cipher that uses a 128 bit plain text with variable 10, 12, or 14 rounds and a variable Key Length of 128, 192, 256 bit permuted into 10 sub- keys each of 128, 192, 256 bit length respectively[5].. It only contains a single S- box and same algorithm is used in reversed for decryption. Rijndael's default number of Rounds is dependent on key size i.e. Rounds = key length/32 + 6. Rijndael AES provides great flexibility for implementing based on parallel structure with effective resistance against attacks [3] [4].

Algorithm

Cipher (byte [] input, byte [] output)
{
byte[4,4] State;

copy input[] into State[] Add Round Key

for (round = 1; round < Nr-1; ++round)

{

SubBytes ShiftRowsMixColumns AddRoundKey

}
SubBytes ShiftRows AddRoundKey

copy State[] to output []
}

B .Asymmetric Key cryptographic Algorithms

❖ RSA
❖ DSA
❖ Diffie-Hellman
❖ ELGAMMAL

❖ *RSA algorithm*

Rivest-Shamir-Adleman (RSA) is a special type of public key cryptography which over the years has reigned supreme as the most widely accepted and implemented general-purpose approach public-key encryption techniques [2]. The RSA algorithm follows a block cipher encryption technique, in which the plaintext and the cipher are integers between 0 and n – 1 for some n. A typical size for n is 1024 bits, or 309 decimal digits. That is, n is less than to1024.RSA algorithm has three major steps.

1. Key generation
2. Encryption

3. Decryption

Algorithm

1. Key Generation; KeyGen (p,q)
Input : Select two prime integers p ,q.
2. Compute n = p q , Φ (n) = (p-1)(q-1)
3. Choose e as exponent then gcd (e, p-1) = 1
4. gcd (e, q-1) = 1
5. gcd (e, (p-1) (q-1)) = 1
6. Compute d such that ed =1(mod Φ (n))
7. Compute d = e^{-1} (mod Φ (n))
Find a unique value d such that
Φ (n) divides 5d-1 value ---- pi Key
Public Key = (n, e).
Private Key = (n, d).
Encryption
$C \equiv M^{E} \pmod N$
8. Encrypt the message M
$C \equiv M^{E} \pmod N$
Decryption
9. To decrypt the cipher text we have
$M = C^{d} \pmod n$
M = Plain Text.
MD5 (Message Digest5)
The Message Digest5 (MD5) was developed by Ronald Rivest in 1992 by taking the block sizes as 512 bit and the digest size as 128 bit. The hash function producing the 128 bit hash value. The MD5 can be used as the best solution to impose the brute force attack to act against the extensive vulnerabilities and to provide excessive security.
SHA (Secure Hash Algorithm)
The Secure Hash Algorithm (SHA) is the most prominent hash algorithm used in the cryptographic systems. It uses 160- bit which is also a resemblance of the MD5 algorithm. The SHA-1 was originally developed by the National Security Agency (NSA) to be part of the Digital Signature Algorithm.

❖ *DSA*

The Digital Signature Algorithm (DSA) was proposed by the National Institute of Standards and Technology (NIST) in August 1991. DSA, the entropy, secrecy, and uniqueness of the random signature value *k* is critical [6]. It is so critical that violating any one of those three requirements can reveal the entire private key to an attacker. Using the same value twice (even while keeping *k* secret), using a predictable value, or leaking even a few bits of *k* in each of several signatures, is enough to break DSA. [5]

❖ *Diffie-Hellman Key Exchange (D-H)*

Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

❖ ***EIGamel***

In cryptography, the EI Gammel encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange. It was described by Taher EI Gammel in 1984. EI Gammel encryption is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems. The Digital Signature Algorithm is a variant of the EIGamel signature scheme, which should not be confused with EI Gammel encryption. EIGamel encryption can be defined over any cyclic group .Its security depends upon the difficulty of a certain problem in related to computing discrete logarithms.

❖ *TWOFISH*

Bruce Schneier is the person who composed Blowfish and its successor Twofish. The Keys used in this algorithm may be up to 256 bits in length .Twofish is regarded as one of the fastest of its kind, and ideal for use in both hardware and software environments. Twofish is also freely available to anyone who wants to use it. As a result, we'll find it bundled in encryption programs such as Photo Encrypt, GPG, and the popular open source software [6].

❖ *IDEA*

IDEA stands for International Data Encryption Algorithm which was proposed by James Massey and Xuejia Lai in 1991. IDEA is considered as best symmetric key algorithm. It accepts 64 bits plain text. The key size is 128 bits. IDEA consists of 8.5 rounds. In IDEA the 64 bits of data is divided into 4 blocks each having size 16 bits. The basic operations are modular, addition, multiplication, and bitwise exclusive OR (XOR) are applied on sub blocks. There are eight and half rounds in IDEA each round consist of different sub keys. Maximum number of keys used for performing different rounds is 52 [7].

❖ Homomorphic Encryption

Homomorphic encryption was a one of encryption technique which allows specific types of computations to be carried out on cipher text. It gives an encrypted result which when decrypted matches the result of operations performed on the plaintext. When the data is transferred to the cloud we use standard encryption methods to secure this data, but when we want to do the calculations on data located on a remote server, it is necessary that the cloud provider has access to the raw data, and then it will decrypt them [8].

III. RELATIVE WORK

Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures gives us theoretical comparison of symmetric and asymmetric cryptography algorithms [9].compares symmetric and asymmetric cryptography algorithms using parameters key length ,speed , encryption ratio and security attacks[10]. Comparisons 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[11] . Comparative study of symmetric and asymmetric cryptography techniques using throughput, key length, tunability, speed, encryption ratio and security attacks [12]. Evaluation of blowfish algorithm based on avalanche effect gives a new performance measuring metric avalanche effect [13].

IV.COMPARISON OF SYMMETRIC AND ASYMMETRIC ALGORITHMS

S.NO	CHARACTERISTICS ALGORITHM	BSIZE BITS	KEY LENGTH	SECURITY	SPEED
1	DES	64	56	Inadequate	Very slow
2	Blow Fish	64	448	Secure	Fast
3	RC2	64	128	High secure	Very fast
4	RC5	32,64 or 128	2040	Secure	Slow
5	RC6	128	128 or 256	Secure	Fast
6	3DES	64	112,168	InSecure	Slow
7	AES	128, 192 or 256	128,192 or 256	High secure	Very fast
8	RSA	128	1024-4096	Secure	Very slow
9	DSA	256	192	Secure	Fast
10	DIffe-Hellman	---	--	In secure	Slow
11	Two Fish	128	128,192or 56	Secure	Very Fast
12	IDEA	64	128	Inadequate	Slow
13	Elgammel	--	--	Not secure	Fast
14	Homomorphic Encryption	--	--	Secure	Fast
15	SHA	512	160	Secure	Slow
16	MD5	512	128	Secure	Slow
17	RC4	40-124		Secure	Very fast

Table. I.. Comparison of Symmetric key and asymmetric key Cryptographic Algorithms

Blowfish is the better than other algorithms in throughput and power consumption [14]. Blowfish encryption algorithm is leading with the security level that they provide and faster encryption speed. Blowfish was replaced by Two fish.RC6 might be observed as interweaving two parallel RC5 encryption Techniques. The RC6 can use an extra multiplication operation but not present in RC5 in order to make the rotation dependent on each bit, and not the least significant few bits [15]. Triple DES has slow performance in terms of power consumption and throughput when compared with DES [14] [16]. AES encryption is fast and flexible, it can be implemented on various platforms especially in small devices. AES has been carefully tested for many security applications [16][17].

RSA is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys are used in encryption and decryption process [16]. The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factorization of large integers. The main disadvantage of RSA is that it consumes more time to encrypt data. Actually this is disadvantage of asymmetric key algorithms because the use of two asymmetric keys. It provides good level of security but it is slow for encrypting files. The strength of the each encryption algorithm depends upon the key management, type of cryptography, number of keys, number of bits used in a key. Longer the key length and data length more will be the power consumption that will lead to more heat dissipation. So, it is not advisable to use short data sequence and key lengths.

The DSA is a variant of the EIGamal signature scheme, which should not be confused with EIGamal encryption.

Table. 2.Experimental results using Crypto ++

S.NO	Algorithm	Megabytes(2^20 bytes) Processed	Time Taken	MB/Second
1	**Blowfish**	256	3.976	64.386
2	**Rijndael (128-bit key)**	256	4.196	61.010
3	**Rijndael (192-bit key)**	256	4.817	53.145
4	**Rijndael (256-bit key)**	256	5.308	48.229
5	**Rijndael (128) CTR**	256	4.436	57.710
6	**Rijndael (128) OFB**	256	4.837	52.925
7	**Rijndael (128) CFB**	256	5.378	47.601
8	**Rijndael (128) CBC**	256	4.617	55.447
9	**DES**	128	5.998	21.340
10	**(3DES)DES-XEX3**	128	6.159	20.783
11	**(3DES)DES-EDE3**	64	6.499	9.848

The security of EIGamal depends on the difficulty of a particular problem in related to computing discrete logarithms [18]. Homomorphic encryption was a one of encryption technique which allows specific types of computations to be carried out on cipher text.
AES algorithm is most efficient in terms of speed, time, and throughput. DES algorithm consumes least encryption time and AES algorithm has least memory usage while

encryption time difference is very minor in case of AES and DES algorithm. RSA encryption time and memory usage is also very high but output byte is least in case of RSA algorithm.

The experiment result shows that the memory required for implementation is smallest in blowfish whereas it is largest in RSA. DES and AES require medium size of memory. So the Blowfish is best option smaller size of memory. AES is the more confident, integrity and highest priority for any application. Blowfish consumes the least time amongst all. Blowfish is efficient in software, at least on some software platforms. AES is the best suitable for better cryptographic strength. DES is the best suitable for network bandwidth.

V. V.EXPERIMENTAL RESULTS

A. Experimental results using Crypto ++

The experiment are conducted on commonly used cryptographic algorithms based on system parameters Pentium 4 and 2.1 GHZ processor on windows XP compiled C++ code with Microsoft Visual C++.NET 2003to evaluate the execution time for encryption and speed benchmarks [19].

The result shows that Blowfish and AES have the best performance among others. Compare to both AES the best secure and efficient algorithm with limited key size among the all above algorithms. Finally AES performs highly secure encryption algorithm and accepted with higher key size. The popular secret key algorithms including DES, 3DES, AES (Rijndael), Blowfish, were implemented, and their performance was compared by encrypting input files of varying contents and sizes. The algorithms were implemented in a uniform language (Java), using their standard specifications, and were tested on two different hardware platforms, to compare their performance.

The performance of the Secret key or Symmetric key algorithms comparing by the encrypting input files with various contents and sizes using Java as common language in two different platforms. The first experiment on P-II 266 MHZ and P-4 2.4 GHZ

B. Show the results of their experiments conducted on P-II 266 MHz with Java.

File Size KB	DES	3DES	AES	BF
20,527	24	72	39	19
36,002	48	123	74	35
45,911	57	158	94	46
59,852	74	202	125	58
69,545	83	243	143	67
137,325	160	461	285	136
158,959	190	543	324	158
166,364	198	569	355	162
191,383	227	655	378	176
232,398	276	799	460	219
Average Time	134	383	228	108
B/Sec	835	292	491	1,036

Table 3. The experiment shows the Comparative execution times (in seconds) of encryption algorithms in ECB mode on a P-II 266 MHz machine.

File Size Bytes	DES	3DES	AES	BF
20,527	2	7	4	2
36,002	4	13	6	3
45,911	5	17	8	4
59,852	7	23	11	6
69,545	9	26	13	7
137,325	17	51	26	14
158,959	20	60	30	16
166,364	21	62	31	17
191,383	24	72	36	19
232,398	30	87	44	24
Average Time	14	42	21	11
B/Sec	7,988	2,663	5,320	10,167

Table.4.Performance comparison on Symmetric key algorithms

The observations based on the results shows that Blowfish has a very good performance compared to other algorithms. AES has better performance than 3DES and DES. AES is considered among best secure and efficient algorithm in the above all algorithms [20].

VI. CONCLUSION

We discuss the weakness and strength of asymmetric key algorithms and symmetric key algorithms. Based on survey RC5 and RC4 security is questionable but RC4 faster than RC5. These encryption algorithms AES is more secure, efficient and faster than to all algorithms with allowing 256-bit key sizes and protect against future attacks. Blowfish was replaced by Twofish.

RSA is best Asymmetric key algorithm but it consumes more time for encryption and factorization problem for large Integers in the decryption process.

AUTHORS INFORMATION

I am U.Thirupalu joined as a Research Scholar (PT) in the department of computer science ,S V U CM&CS , Tirupati. I am pursuing PhD under the guidance of Dr.E.kesavulu Reddy in the Dept. of Computer Science, S v u CM&CS, Tirupati.

REFERENCES

[1] Cong Wang, Qian Wang, Kui Ren and Wenjing Lou "Ensuring Data Storage Security in Cloud Computing." IEEE 200 9.

[2] Yogesh Kumar, Rajiv Munjal andn Harsh Sharma Comparison of Symmetric and Asymmetric Cryptography With Existing Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and anagement Studies, Vol. 11, Issue 03, Oct 2011.

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

[4] Gurpreet Singh, Supriya Kinger"Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security" International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.

[5] Uma Somani, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

[6] Mr. Mukta Sharma and Mr. Moradabad R. "Comparative Analysis of Block Key Encryption Algorithms "International Journal of Computer Applications (0975 – 8887) Volume 145 – No.7, July 2016.
[7] AshimaPansotra and SimarPreet Singh "Cloud Security Algorithms" International Journal of Security and Its Applications Vol.9, No.10 (2015), pp.353-360.
[8] Iram Ahmad and Archana Khandekar "Homomorphic Encryption Method Applied to Cloud Computing" International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 15 (2014), pp. 1519-1530.
[9] Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures by Yogesh Kumar, Rajiv Munjal, and Harsh ,(IJAFRC) Volume 1, Issue 6, June 2014. ISSN 2348 – 4853.
[10] Comparative analysis of performance efficiency andsecurity measures of some encryption algorithms y AL.Jeeva, Dr.V.Palanisamy, K.Kanagaram compares symmetric and asymmetric cryptography algorithms ISSN: 2248-9622.
[11] 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.
[12] Comparative Study of Symmetric and Asymmetric Cryptography Techniques by Ritu Tripathi, SanjayAgrawal compares Symmetric and AsymmetricCryptographyTechniques 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
[13] Evaluation of Blowfish Algorithm based on Avalanche Effect by Manisha Mahindrakar gives a new performance measuring metricavalanche effect. International Journal of Innovations in Engineering and Technology (IJIET) 2014.
[14] Mr. Gurjeevan Singh, Mr.Ashwani Singla And Mr. K S Sandha "Cryptography Algorithm Compassion for Security Enhancement In Wireless Intrusion Detection System" International Journal of Multidisciplinary Research Vol.1 Issue 4, August 2011.
[15] Mr.Milind Mathur and Mr. Ayush Kesarwani "Comparison between DES, 3DES, RC2, RC6, Blowfish and AES" Proceedings of National Conference on New Horizons in IT - NCNHIT 2013.
[16] urpreet Singh, SupriyaKinger "Integrating AES, DES, and 3-DES Encryption Algorithm for Enhanced Data Security" International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.
[17] Uma Somani, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", 2010 First International Conference On parallel, Distributed and Grid Computing (PDGC-2010).
[18] AnnapoornaShetty , ShravyaShetty K , Krithika K "A Review on Asymmetric Cryptography – RSA and ElGamal Algorithm" International Journal of Innovative Research in Computer and Communication Engineering Vol.2, Special Issue 5, October 2014
[19] RFC2828],"Internet Security http://www.faqs.org/ rfcs/rfc2828.html.
[20] Aamer Nadeem et al, "A rformance Comparison of Data Encryption Algorithms", IEEE 2005.