Volume 4, Issue 9, September 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Comparative Analysis of Eight Different Cryptographic Algorithms with Fourteen Factors

Priyanka Raval[*]
C.U. Shah University,
India

Jeegar Trivedi
S.P. University,
India

Abstract*— as we know that, era of today is totally based on computer. We can say that, nowadays much of the work is done by computer. Behind the wide use of computer, one important technology is used. And that technology is network. But in the current era, it is very difficult to transfer data through the internet or network securely. As per the technology developed, data could be of text or any multimedia, and any type of data should have to be transferred via network safely. As a solution, we found cryptographic algorithms. These algorithms are used to protect our data at the time of transferring it via internet. Many of the algorithms are available for cryptography. And all of them have a special importance. Here in this paper, eight different algorithms, named Blow fish, Two fish, RC2, RC6, RSA, DES, 3DES and AES are compared. This paper provide a comparative analysis of different algorithms based on Key size, Block size, Algorithm structure, Developed in, Designer, Rounds, Key used, Security, Flexibility, Scalability, Cryptanalysis resistance, Power consumption, Cipher type and Type of algorithm.

***Keywords*— Cryptography, Algorithms, Blow fish, Two fish, RC2, RC6, RSA, DES, 3DES, AES**

I. INTRODUCTION

Nowadays, most of the information is stored in the computer and it is used or shared or transferred via internet. This becomes a normal scenario. But when we talk about the internet, the first question comes in our mind is data security. As we know that day by day many more technology are developed and enhanced, solution for data security is also required which is provided through cryptography. Cryptography is a technology to transfer data in encoded form over the network. It is very effective technique to protect data from active and passive intruders. The main goal of cryptography is to keep the data secure for its intended user only.

Cryptography is the art and science of protecting information from undesirable individuals by converting it into a form non-recognizable by its attackers while stored and transmitted [1].

Terms used in cryptography:

1. Plain text: Plain texts are the original text which a sender wants to transfer over network to receiver. For example, a student wants to say "Good morning" to sir, then "Good morning" is the plain text.
2. Cipher text: cipher texts are the texts which are the converted form of plain texts, which will transfer over network, and which are not in readable form. For example, "Iqqf oqtpkpi" are the cipher texts produced for plain text "Good Morning".
3. Encryption: The process of converting plain text into cipher text is known as encryption.
4. Decryption: The process of converting cipher text to plain text is known as decryption.
5. Key: The secret word or digit or combination of both, which only sender and receiver knows and which is used in the process of conversion of cipher text to plain text and plain text to cipher text is known as key.
6. Intruder: Intruder is an unauthorized person, who wants to see the data which is transferred over network. If data is stolen and other data is placed on the network by intruder, then that intruder is active intruder. If intruder just see the data and not make any changes, then he is a passive intruder.

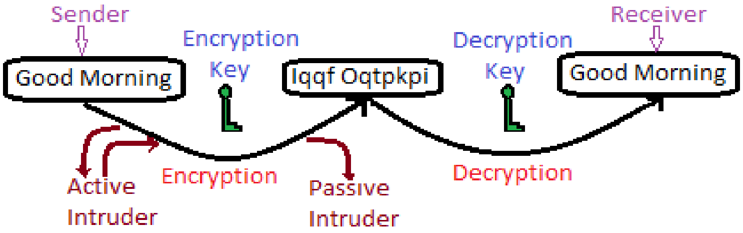

Fig. 1 Process of Cryptography

II. COMPARATIVE ANALYSIS

Here these eight algorithms are compared with each other on the basis of fourteen different factors. These factors and their meanings are listed below.

a. Developed in: This factor shows that in which year the specific algorithm is developed.
b. Designed by: This factor shows that who the designers of the specific algorithm are.
c. Security: It displays the security level of the algorithms.
d. Scalability: it shows the ability to work with the growth.
e. Flexibility: It shows that any type of modification can be possible by the algorithm or not.
f. Type of algorithm: It shows that algorithm is symmetric key algorithm or asymmetric key algorithm.
g. Key used: It shoes that the key used for encryption and decryption are same or different.
h. Cipher type: it shows that cipher texts are of stream cipher or block cipher.
i. Power consumption: It displays the power consumption of the algorithm.
j. Cryptanalysis resistance: shows the resistance of algorithm.
k. Round: It shows the digit of function used.
l. Algorithm Structure: it defines the structure used by the algorithm.
m. Key size: This factor shows key length used for algorithms.
n. Block size: This factor shows key length used for algorithms.

III. ALGORITHM COMPARISON

Here are the three tables which represent the comparison between the eight algorithms based on fourteen factors.

Table I. Basics of compared algorithm [3], [5], [6], [7], [8]

Algorithms	Developed	Designer	Type of algorithm	Key Used
Blow fish	1993	Bruce Schneier	Symmetric	Same
Two fish	1998	Bruce Schneier	Symmetric	Same
RC 2	1987	Ron Rivest	Symmetric	Same
RSA	1977	Rivest, Samir and Adleman	Asymmetric	Different
DES	1977	IBM	Symmetric	Same
3DES	1978		Symmetric	Same
RC 6	1998	Rivest, Robshaw, Sidney, lisa	Symmetric	Same
AES	2000	Rijmen, Daemen	Symmetric	Different

Table II. Work and structure related comparison [2], [3], [4], [5], [7], [8], [9]

	Key size(bits)	Block size(bits)	Round	Algorithm structure	Cipher Type	Power consumption
Blow fish	32-448	64	16	Feistel network	Symmetric block	Low
Two fish	128, 192 or 256	128	16	Feistel network	Symmetric block	Low
RC 2	8 to 128	64	18	Feistel network	Symmetric block	Low
RSA	1024 to 4096	any byte length	1	---	Asymmetric	High
DES	64	64	16	Feistel network	Symmetric block	Low
3DES	168	64	48	Feistel network	Symmetric block	More than DES & less than RSA
RC 6	128, 192 or 256	128	16	Feistel network	Symmetric block	High
AES	128, 192 or 256	128	18	Substitution-permutation network	Symmetric block	Low

Table III. Other comparative results

	Scalability	Flexibility	Security	Cryptanalysis resistance
Blow fish	No	Yes	Secure	has some classes of weak keys, 4 rounds are exposed to 2nd order differential attacks.
Two fish	No	Yes	robust and highly resistive	A related-key attack is possible requiring 2^{34}chosen plaintexts
RC 2	No	Yes	related key attack is possible	vulnerable to a related-key attack using 2^{34} chosen plaintexts
RSA	No	Yes	Timing attack is possible	768 bit key has been broken
DES	Scalable	No	Proven in adequate	vulnerable to differential and linear cryptanalysis; weak substitution table, Brute force attack is possible

3DES	Scalable	Yes	one only weak which is exit in DES	vulnerable to differential, brute force attacker could be analyse plain text using different cryptanalysis
RC 6	No	Yes	Vulnerable	single class of weak keys
AES	No	Yes	considered secure	strong against differential, truncated differential, linear, interpolation and square attacks

IV. CONCLUSIONS

As we can see from the table first, RSA and DES are the oldest algorithm among compared algorithms. RSA is the only algorithm of asymmetric type and others are symmetric algorithms. From the second table, we can see that key length of RSA is biggest. As the key size is bigger, it is harder to break the security. Power consumption by RC6 and RSA is higher compare to the other algorithms. On the basis of third table, it can be concluded that DES is the only algorithm which is not flexible. And DES and 3DES are the only algorithms which are scalable.

REFERENCES

[1] A.A.Zaidan, B.B.Zaidan, Anas Majeed, *High security cover file of hidden data using statistical technique and AES encryption algorithm*, World Academy of science Engineering and Technology (WASET), Vol.54, ISSN: 2070-3724, P.P 468-479.

[2] Md Imran Alam, Mohammad Rafeek Khan, *Performance and efficiency analysis of different block cipher algorithms of symmetric key cryptography*, International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, ISSN:2277-128X,P.P 713-720.

[3] Mohit Marwaha, Rajeev Bedi, Amritpal Singh, Tejinder Singh, *Comparative analysis of cryptographic algorithm*, International Journal of Advanced Engineering Technology, ISSN: 0976-3945, P.P 16-18.

[4] Mansoor Ebrahim, Shujaat Khan, Umer Bin Khalid, *Symmetric algorithm survey: A Comparative analysis*, International Journal of Computer Application, Vol.61, ISSN: 0975-8887, P.P 12-19.

[5] Aman Kumar, Dr. Sudesh Jakhar, Mr.Sunil Makkar, *Comparative analysis between DES and RSA Algorithm's*, International Journal of Advanced Research in Computer Science and Software Engineering,Vol.2,ISSN:2277-128X,P.P 386-391.

[6] Lalit Singh, Dr. R.K.Bharti, *Comparative performance analysis of Cryptographic algorithms*, International Journal of Advanced Research in Computer Science and Software Engineering,Vol.3,ISSN:2277-128X,P.P 563-568.

[7] B.Padmavathi, S. Ranjitha Kumari, *A survey on performance analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique*, International Journal of Science and Research(IJSR),Vol.2,ISSN: 2319-7064, P.P 170-174.

[8] Hamdan.O.Alanazi, B.B.Zaidan, Hamid A.Jalab, M. Shabbir, Y.AL-Nabhani, *New comparative study Between DES, 3DES and AES within Nine Factors*, Journal Of Computing, Vol.2, ISSN: 2151-9617, P.P 152-157.

[9] Srinivasarao D, Sushma Rani N, Ch. Panchamukesh, S.Neelima, *Analyzing the superlative symmetric cryptographic ecryption algorithm*, Journal of Global Research in Computer Science (JGRCS), Vol.2, ISSN: 2229-371X, P.P 101-105.