Comparative Study on Cryptographic Algorithms

Pooja Mudgil [#], Parikshit Sehgal, Mohit Garg, Vaibhav Chhabra

Department of Information & Technology,
Bhagwan Parshuram Institute of Technology, Delhi
[#] Corresponding Author, Email: *engineer.pooja90@gmail.com*

***Abstract* – Cryptography is formed from the combination of two Greek words Krypto "secret" and Graphene which means "To write". The encryption techniques can be classified into two types as asymmetric key encryption and symmetric key encryption. In symmetric key encryption, the key with which the sender carries out encryption is the same as the one with which the receiver carries out decryption whereas in asymmetric key encryption there are two keys one is called public key while the other is called private key, public key is used for encryption while private key is used for decryption. In this paper, we carry out a performance analysis of the following algorithms. DES, AES, Onetime pad Cipher are symmetric key algorithms and RSA is an asymmetric key algorithm. The performance measure in terms of String length v/s Total Time Consumed by Algorithm was conducted to analyze which is the fastest algorithm and which one is the most secure.**

***Keywords* – AES, DES, Onetime Pad Cipher, RSA.**

1. INTRODUCTION

In this period of ever-growing access electronic connectivity and continuously increasing the risk of cyber-attacks and eavesdropping by elements with ill motives and hence the importance of network security can never be undermined. The tremendous growth in access of computer systems and their interconnections via networks has increased the dependence of individuals and groups on the information stored and communicated using these systems. There is a need to protect data and resources from unauthorized access or possibility of a leak and to protect systems from network-based attacks. Cryptography is a standard method of securing data and resources from network-based attacks. It is an attempt at providing secure information in presence of adversaries to maintain information security such as data confidentiality, data integrity, authentication, and non-repudiation. The procedure of converting ordinary text in the Cipher text is called encryption. The ordinary text is one which is human readable form and the ciphertext is machine-readable form. The reverse process of converting a ciphertext into human-readable form is called decryption. Encryption and decryption related keywords are explained in this paper and there is also detailed information about how the algorithm works [1],[9].

To determine the security provided by an encryption algorithm we have to see the size of the key space. The larger the key size the greater the security but this may lead to a decrease in encryption and decryption speed and this may consume more hardware resources and processing power. The larger is the size of the key the more computation resources an attacker has to put in terms of the exhaustive search of key space and thus the higher is the level of the security provided.

Key is a piece of information which decides how the conversion of plaintext to cipher text and vice versa will be done. The larger the key space the more possible keys can be constructed. The strength of the encryption process of the algorithm relies on the length of the key, secrecy of the key, the initialization vector and how they all work together [2],[10].

2. LITERARTURE REVIEW

During the course of our research we came across several papers that studied only one algorithm studied several different algorithms from the view of storing data in encrypted form in cloud or from the point of view of network security. There were few research papers that did a comparative analysis of several algorithms based on their efficiency in encrypting strings. However, we could come across only two research papers where the comparison was done on basis of execution time of algorithms. Our research paper encrypts a message which can contain number alphabets and special characters and sends it over a network in client server application and then decrypts it. We calculate the total running time of the algorithms for strings of different lengths and plot it on a graph.

3. BASIC TERMS USED IN CRYPTOGRAPHY

3.1. Plain Text

In cryptography, the plaintext is a piece of text which is in the form which can be read by humans. This is a piece of message or information sent from the sender to the receiver. It is also referred to as clear text and is given as an input to the encryption algorithm for the encryption process.

3.2. Cipher Text

The text produced as a result of the encryption process is cipher text. It is a machine-readable text that cannot be understood by humans. Plaintext is converted to cipher text before it sent by the sender over the network to the receiver.

3.3. Encryption

Encryption is a technique that allows the user to hide information from others. Encryption requires two basic things such as key and possible encryption algorithms. It is used to send the confidential message to the user. It is a process in which the given original text is converted into a cipher text or unreadable form.

3.4. Decryption

Decryption is basically reverse process of encryption. It is a process of converting a cipher text back into a plain text that the user can read. It happens at the receiver end so that they can read the message that was sent by the sender. It also needs a key and algorithm for decrypting the text.

3.5. Key

Key operates on the plain text and converts it into cipher text. The real strength of cryptography is in the key. It is used for both decryption and encryption process. Key, could be any of the following number ,function or an algorithm. Key performs the transformation.

3.6. Cryptosystem

The system which is used to implement cryptography is known as a cryptosystem [3].

4. ALGORITHMS USED

4.1. Data Encryption Standard

This algorithm was developed by IBM in 1977 and is symmetric key block cipher algorithm. It uses a block size of 64 bits and a key size of 56 bits (where 8 bits are parity bits) to encrypt plain text which is 64 bits in size. It consists of fiestal network which divides a block into two equal's halves and both the halves pass through a function.DES has a series of S-boxes and P-boxes. DES works on two fundamental attributes of cryptography Diffusion (Substitution) and Confusion (Permutation) consisting of 16 rounds. In each round data bits and key are shifted, then permuted, followed by XOR and sent through, 8 s-box. In the first round, 64-bit plaintext is handed to initial permutation (IP). Then IP generates two halves left plaintext (LPT) and right plaintext (RPT). Both the halves go through 16 rounds. At the last both halves are rejoined. Decryption is the same process perform rounds in reverse order [4],[6].

Algorithm: -

[1] DES works on an input plaintext of 64-bit length and 56-bit key (8 bits of parity) generating an output of 64-bit block.

[2] The plaintext block is subject to a shift the bits around.

[3] By subjecting the key to its permutation the eight parity bits are removed.

[4] The plaintext and key are processed in 16 rounds consisting of:

a. The key is divided into two 28 bit halves

b. Each half of the key is shifted (rotated) by one /two bits, in accordance with the round.

c. Upon recombining the two parts they are subjected to compression permutation to reduce bit size from 56 to 48. This key which is now compressed is used to encrypt the round's plaintext block.

d. The key halves which were rotated in step 2 are used in the next round.

e. The total data block is divided into two 32-bit halves.

f. Now size of one of two halves is increases to 48 bits by subjecting it to Expansion Permutation.

g. The 48 bit compressed key is XORed with output from step 6.

h. The output of step 7 is given as input into an S-box, which reduced the 48 bit block back into 32 bits by substituting the keys.

i. The output of step 8 is subject to a P-box to permute the bits.

j. The output from the P-box is exclusive-OR'ed with another half of the data block.

k. The two data halves are interchanged and become the next rounds input [1].

4.2. Advanced Encryption Standard

DES has been the encryption standard since 23 Nov 1976, however as computational power of computers increased it became vulnerable to attacks. Hence NIST started a competition in 1997 for new encryption standard. In 1998 the cryptanalysis of the algorithm was carried out. The DES encryption process which was done in 16 rounds was cracked in less than three days by a specially made computer called DES cracker. The DES cracker was created by the electronic frontier foundation for less than $250,000 and won the RSA DES challenge-II.

The alternatives to a new encryption standard were triple DES and International Data Encryption Algorithm (IDEA). The problem in this was IDEA and 3DES were too slow and IDEA was not free to implement due to patents. NIST wanted free and easy to implement an algorithm that would provide good security. Additionally, they wanted the algorithm to be more efficient and flexible.

The contest to find the new algorithm was started in 1997 and went on for three years and an algorithm proposed by two Belgium scientists Vincent Rijmen and Joan Daemen. They named the algorithm Rijndael. On November 26, 2001, a standard version of Rijndael algorithm was accepted this was called the Advanced Encryption Standard. AES defined a cipher in which the block length can be independently specified to be 128,192 and 256 bits. Unlike DES, AES is a substitution-permutation network and not a fiestal network. AES is comparatively easy to implement and also requires little memory [2], [4].

In AES, there are four transformations for one round.

1) Sub bytes: It adds confusion by processing each byte through an S-Box. An S-Box is a substitution table in which one byte is substituted for another.

2) Shift rows: It provides simple permutation of data, whereas other steps involve substitution. It performs a circular rotation on each row. When decrypting, it performs the circular shift in the opposite direction for each row.

3) Mix columns: Each byte of the column is used in this substitution. Each byte is mapped into a new value that is a function of all four bytes in that column. The inverse used for decryption involves a very different set of constants.

4) Add round key: In this the current block is XORed with the expanded along with the

expanded key. It is the only step which makes use of the key and obscures the result, hence must be used at the start and end of each round [3].

4.3. Vernam Cipher (One Time Pad)

Vernam Cipher was invented by Gilbert Sandford Vernam at the end of 19th century. He was also the inventor of Stream Cipher. It is known as the strongest possible method of encryption. Vernam Cipher also known as "One Time Pad" is implemented using a random set of non-repeating characters as the input cipher text. The length of cipher text and plain text is equal. The most powerful point in this algorithm is that the key which is used once is never used again and so is discarded after one use.

Imagine Alice wants to encrypt a message and sent it to Bob and Eve wants to access the encrypted message. Alice will roll a 26 sided dice to generate a long list of random shifts and will share this with Bob. The two powerful points here are: -

Shifts will never fall into a repetitive pattern.

There will be no frequency distribution, therefore any leakage of information. It will be impossible for Eve to break this encryption. In this encryption technique, each letter is shifted by a different number between 1-26.so, it will be impossible to apply brute force here. Example: -

A L I C E
26 * 26 * 26 * 26 * 26 nearly 12Million

One Time Pad encryption algorithm can be generalized by using the equation: $C_i = E(P_i, K_i)$ for I =1,2,3,…,n where E is the encryption operation, Pi is the i^{th} character of the plaintext k_i is the i^{th} byte of the key used, C_i is the i^{th} character of the cipher text which will for formed. Both the keystream K and the encryption operation E must be kept secret. OTP is the perfect secrecy in action [5].

Algorithm:

1. Write each plain text as a number (A=0, B=1,….., Z=25).

2. Write One Time Pad (key used) as a number (A=0, B=1,….,Z=25).

3. Add plain text alphabet number to one-time pad alphabet number.

4. If sum>=26, subtract 26 from it.

5. At last, convert each number of the sum to the alphabet, the cipher text is formed now.

For example: -

```
Plain text - F   E   L   L   O W      OTP-  X   M   C   K
L   T

           5  4  11 11 14 22           23 12  2  10  11
19


     5    4     11    11    14  22

   +23   12     2     10    11  19

    -------------------------------------

    28   16     13    21    25  41

   -26                          -26

  -----------------------------------------

     2   16     13    21    25  25

     C    Q      N     V     Z   Z
```

FELLOW is encrypted to CQNVZZ using OTP-XMCKLU [6].

4.4 Rivest-Shamir-Adleman Algorithm (RSA algorithm)

RSA is an asymmetric cryptography algorithm developed by Ron Rivert, Adi Shamir and Len Adlemen in 1977. RSA is mostly implemented public key cryptographic, as well as digital signature. RSA is a public key cryptography algorithm because one of the public or private key is given to anyone. RSA uses prime no. to generate keys (i.e. public and private key).[1]

ALGORITHM

Step 1: Choose two large prime no's P and Q such that P~=Q

Step 2: Now calculate n as n = P*Q

Step 3: Compute φ (n) = (P-1)*(Q-1)

Step 4: Choose e (public key) such that e must be:
An integer
Not a factor of n
E lies between 1 < e < φ (n)
Step 5: Now calculate private key, d as
d*e modφ (n) = 1
Step 6: For encryption:
C=M^e Mod n, where M=input data for encryption
Step 7: For decryption
M=C^d mod n [3],[7],[8].

5. COMPARISON OF ALGORITHMS

Based on the research done over the four encryption algorithms, the Table 1 is the brief outcome of the study. The main goal of this paper is accomplished here. All the four algorithms are compared well on various important parameters that helps to find us that which algorithm will prove the best for particular application that is under observation like Vernam Cipher is used for defence applications all around the world and where speed is required with moderate security, we have Advanced encryption standard (AES). Consider the Table II; this table consists of values which were computed from java programs implemented on Netbeans IDE. Fig.1 is the graphical view of the Table 2.

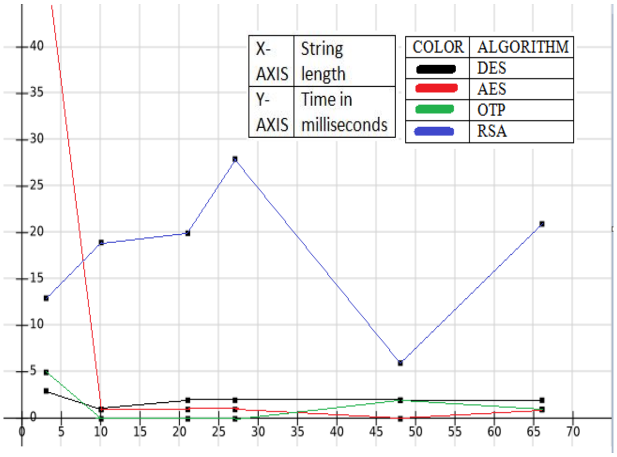

Fig.1: String length v/s Total Time Consumed by Algorithm.

Table 1: Difference between Algorithms. [1], [4]

Parameters	DES	AES	RSA	OTP
Abbreviat--ions of	Data Encryption Standard	Advanced Encryption Standard	Rivest-Shamir-Adleman	One Time Pad
Developed by	IBM	Vincent Rijmen, John Daemen	Ron Rivest, Adi Shamir, Leonard Adleman	Gilbert Vernam
Year	1970	1998	1978	1918
Type	Symmetric	Symmetric	Asymmetric	Symmetric
Key size	56 bits	128,192, or 256 bits	Variable	Variable
Security	Proven insecure	secure	Highly secure	Perfectly secure
Execution speed	Slower than AES	faster	slower	Comparable to AES
Block size	64-bits	128,192,	variable	------

Table 2: Values computed from java Programs.

String length	DES (E+D)	AES (E+D)	OTP (E+D)	RSA (E+D)
3	3	662	5	13
10	1	1	0	19
21	2	1	0	20
27	2	1	0	28
48	2	0	2	6
66	2	1	1	21

6. CONCLUSION

Cryptography is used for secure communication. It is about constructing and analyzing protocols that prevent third parties or public from reading private messages. This paper presents a comparative analysis of cryptographic algorithms like AES, DES, RSA, and OTP.

Each algorithm has been compared on the basis of various parameters (Table 1). A graph (String length v/s Runtime) has been made which shows the comparison between the running times of the algorithm by giving the same input to all the algorithms. From the above graph what we observe that AES give very high time for encryption and decryption process for the first string following which there is drastic fall in the encryption and decryption time even for the longest string the time taken by AES is less than RSA and DES and is at par with OTP however it is not useful for applications where more we want to use it more than one time. AES is the fastest and RSA is the most secure for regular applications. OTP is useful for sending extremely secret classified information only once.

References

[1] Mohit Marwaha, Rajeev Bedi, Amritpal Singh, Tejinder Singh "Comparative Analysis of Cryptographic Algorithm", Singh et al., International Journal of Advanced Engineering Technology E-ISSN 0976-3945.

[2] ManzoorHussain Dar, Pardeep Mittal, Vinod Kumar,"Comparative Study of Cryptographic Algorithms", IJCSN International Journal of Computer Science and Network, Volume 3, Issue 3, June 2014.

[3] M. Harini, K. Pushpa Gowri, Pavithra, M. Pradhiba Selvarani, "Comparative Study and Analysis of Various Cryptographic Algorithm", International Journal of Scientific & Engineering Research Volume 8, Issue 5, May-2017.

[4] Ankita Verma, Paramita Guha, Sunita Mishra, "Comparative Study of Different Cryptographic Algorithms", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 5, Issue 2, March - April 2016.

[5] K.V.O. Rabah, "Implementation of One Time Pad Cryptography", Information Technology Journal 4(1) 87-95 ,2005 ISSN 1882 -5638.

[6] Yogesh Kumar, Rajiv Munjal, "Comparison of symmetric and asymmetric cryptography with existing vulnerabilities", IJCMS-Oct.2011.

[7] Eli Biham and Adli Shamir, "Differential Cryptanalysis of full DES".

[8] Dan Boneh and Glenn Durfee "Cryptanalysis of low exponent RSA"

[9] Piper F "Encryption", Security and Detection, Ecos 97. European Conference

[10] Schweighofer E (1997) Downloading information Info I & Common Technology.