International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

Comparative Analysis of Encryption Algorithms Against Text Files

Nidhi Girish[1*], Pranav B[1], Prof Swetha S[2], Dr.Chethana Murthy[2]

[1]*Student, Dept. of Information Science and Engineering, RV College of Engineering, Bengaluru, India*
[2]*Professor, Dept. of Information Science and Engineering, RV College of Engineering, Bengaluru, India*

Abstract – *The proliferation of technology and vast amount of data transferred every day has made it imperative to practice security measures to protect people and their information. This issue has been handled by the implementation of cryptography in exchange of data. However, there exist many algorithms that can be used to encrypt and decrypt information and choosing the right one for a specific task is crucial. This paper focuses on effectively comparing four popular encryption ciphers, namely RSA, DES, Triple DES and Blowfish, through a web application that allows for measuring various factors of encryption, to provide a graphical result of the best algorithm to use for encrypting text files.*

***Key Words*: Cryptography, Encryption, Symmetric, Asymmetric, DES, Triple DES, RSA, Blowfish, Key**

1. INTRODUCTION

Information Security is a transient field that relies on the use of cryptography to secure data during transfer. Encryption is the process applying varied functions to a given message in order to change its appearance, such that anyone other than the person to whom the message is intended will not understand it. The process of using unique keys with specific methods to retrieve information from encrypted test is known as Decryption. The strength of an algorithm is its ability to resist attacks, and it is correlated with the type and number of keys used, as well as the core function being implemented. Repeated application of aspects of an algorithm on the data tends to make the end result more secure. These algorithms are classified broadly as Symmetric and Asymmetric encryption, which are discussed ahead.

This project revolves around comparing four popular symmetric and asymmetric ciphers according to theoretical and practical analysis showcasing the strength of these algorithms. A Django – based Web application was developed to measure the time taken to encrypt ten text files of different sizes as one of the main and practical criteria for analysis.

The paper is arranged as follows. In section 2 the overview of cryptography is described. In section 3 the methodology of comparative analysis is given. In section 4 the results and the discussions area is detailed. Section 5 of the paper is the conclusion of the Research Project.

1.1 Basic Terms

Plaintext: Plaintext is a phrase used in information security (cryptography) that indicates to a message before the process of encryption or decryption. That is, it is a message in an arrangement that is straightforwardly understood by humans.

Encryption: is the course of obscuring the given messages to make them incomprehensible in the deficiency of some special knowledge. It is commonly done for security purpose, and largely done for very confidential communications. It is also designed for authentication (that is, the course of authorizing the identity of a particular individual). The decryption process is the exact opposite of the encryption process, that is, the translation of encrypted data into plaintext or the original text.

Plaintext: should never be misunderstood with plain text. Plain text refers to the text consisting completely of characters that are mainly used in most of the written human language. The Plaintext is written with sequences of multiple bits that do not symbolize human readable characters. Plaintext is mostly written in plain text.

Cipher text: Ciphertext is the encrypted text modified from the plaintext using various encryption algorithms. Ciphertext cannot be read without a key until it's been converted back into plaintext (decrypted). The decryption cipher is an algorithm that alters the ciphertext into plaintext.

Key: A cryptographic key is a set of string of bits utilized by a cryptographic algorithm to remodel plain text into cipher text or the other way around. This key remains confidential and ensures a very secure communication.

A cryptographic key is the heart of any cryptographic operations. Many of the cryptographic systems include a set of various operations, like encryption and decryption. A key is a component of the variable data that's provided as one of the input to a cryptographic algorithm to execute this kind of operation. In an efficiently designed cryptographic scheme, the protection of the scheme depends on the protection of the keys used.

2. OVERVIEW OF CRYPTOGRAPHY

2.1 Symmetric Encryption

This is the simplest and the easiest kind of encryption. Symmetric encryption is a cryptographic process where an individual key is responsible for all encryptions and decryptions. The involved parties, that is the receiver and sender, share a unique key, password, or passphrase, to decrypt or encrypt the messages they prefer. Some of the most popular and famous algorithms that are in use even today, have been categorized as symmetric cryptography, including DES (Data Encryption Standard), Triple DES and AES (Advanced Encryption Standard). The former two have been considered for the purpose of this project and they are very close in functioning.

2.2 Asymmetric Encryption

This uses pair of keys. The Asymmetric encryption is also a type of crypto-system where in the encryption and decryption processes are achieved using a pair of unique keys, namely, a public key and a private key. Therefore, this method is otherwise known as public-key encryption. Asymmetric encryption focuses on the conversion of plaintext into cipher-text utilizing either one of the 2 keys that are available (that maybe public or private key) along with an encryption algorithm. Using the other key (public or private key) along with a decryption algorithm, the original plaintext is regained from the encoded cipher text. The most popularly asymmetric encryption crypto-system is RSA which is widely used and popular.

2.3 Encryption Algorithms Implemented

DES: It is the most popular choice of encryption algorithm and it was formulated on Data Encryption Standard (DES) which was developed in 1977 by the National Bureau of Standards. The DES algorithm in itself is called as the Data Encryption Algorithm (DEA). In this algorithm, the plaintext is encrypted in a series of 64-bit blocks with the help of a 56-bit key. It takes a series of 64-bit input data and transforms it into blocks of a 64-bit output. The steps that are followed in the encryption process with the same key of that of the receiver, are implemented to reverse the encryption on the encryption side. The DES algorithm relishes a large and a wide spread use all over. DES has also been the victim of many controversies regarding the security the DES provides.

It is a symmetric block cipher that encrypts and decrypts the data using a 56-bit key. DES takes a 64-bit block of plaintext as the input and it results in 64-bit block cipher text as output. [4] This cipher text is produced by repeating the main algorithm 16 times, which includes permutation and substitution in each round. It is known that the more the number of rounds, there is an increase in amount of effort needed to find the key using Brute Force method. This makes DES a strong cipher in this aspect.

As mentioned above, the DES algorithm uses a 56-bit key for encryption. In reality, initially is when the key is generated. The key comprises of 64 bits and even before the algorithm's procedure begins, the key size is reduced to 56 bits by discarding every 8^{th} bit of the key to make it a 56 bit key. To achieve this, the subsequent bit positions in the key 8, 16, 24, 32, 40, 48, 56 and 64 are removed and hence, the 56-bit key is created.

The DES algorithm is predicated on 2 basic and important features of cryptography: the first feature being substitution (also called confusion) and the second, transposition (also called diffusion). It involves a series of 16 similar steps, every step in the process is titled as a round. Each of the rounds execute the above steps of substitution and transposition.

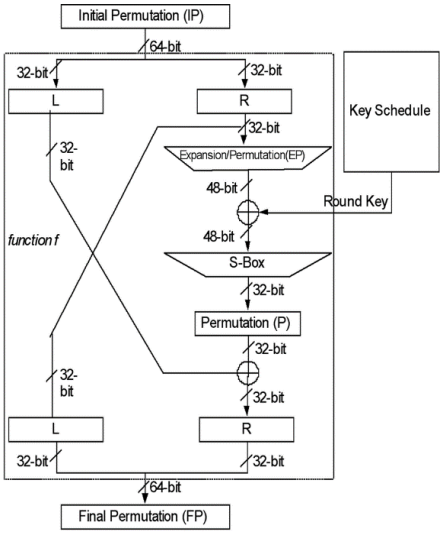

Fig-1: DES Procedure

• Triple DES: As mentioned above, DES algorithm uses a series of 56 bit keys to encrypt each block of plain text. The drawback is that DES can easily be deciphered with the help of modern technologies. To prevent hackers from cracking into systems the double DES and triple DES were developed which are much more secure than that of the original single DES. This is because of the fact that the double and triple DES uses 112 and 168 bit keys respectively.

While using triple DES, the user first has to generate and issue a triple DES key K, which comprises of three various DES keys K1, K2 and K3. By doing so the triple TDES key has length of 3×56 = 168 bits. To achieve the following the plaintext block has to encrypted with the key k1, then the output of the previous has to be decrypted with k2,and that output has to be encrypted with k3, by following the above procedure it gives rise to the cipher text. For the decryption process the exact opposite has to be followed of that of the encryption process that is decrypt with k3, encrypt with k2 and then finally decrypt with k1 this results back to the plaintext.

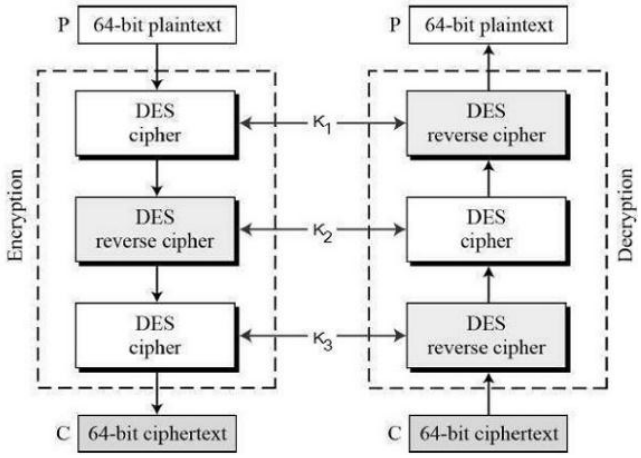

Fig-2: Triple DES Procedure

• RSA: The RSA algorithm was initially developed and defined in the year 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of (MIT). [2] It is an algorithm that is used by many modern computers for encryption and decryption of the messages. RSA is categorized as an asymmetric cryptography algorithm. The RSA algorithm is presently used in as many as 100's of different software products and this algorithm can be used for various things such as digital signatures, key exchange, or encryption of small data. In the RSA algorithm, either the private or the public key can be used for the encryption of a message, for the decryption process the other key from the one chosen to encrypt a message should be used to decrypt the message. The RSA algorithm gets all of its security value from factorization of very large integers that are obtained by the product of the 2 extremely large prime numbers. Many popular protocols such as SSL/TLS, S/MIME, OpenPGP, and Secure Shell operate and solely depend on the RSA for digital signature functions and encryption.

The primary security of RSA is determined by on the two strong suits of separate functions. The RSA algorithm is the most prevalent in public-key cryptosystem strength of which is grounded on the practical struggle of factoring the very huge numbers.

Encryption Function – it's considered as a 1-way function of translating of the plaintext into ciphertext and it may be translated back only with the knowledge of personal key or also known as the private key.

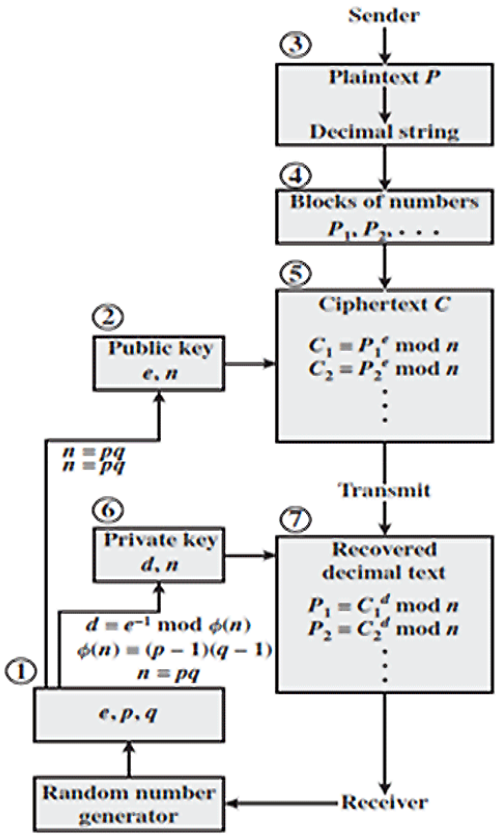

Fig -3: RSA Procedure

Key Generation – the issue of determining the private key from an RSA public key is alike to factoring the various modulus. A hacker thus cannot use his knowledge of an RSA public key to work out an RSA private key unless he can factor. It's also a 1-way function, from p & q values to modulus n is straightforward but the reverse isn't possible.

If either one of those two functions are shown non one-way, then RSA are broken. In fact, if a method for factoring efficiently is developed then RSA will not be safe.

• Blowfish: Designed by Bruce Schneier in 1933, this algorithm uses keys ranging from 32 to 448 bits. Its main purpose was to serve as an alternative to DES. [3] It has the well-known 16 round Feistel Structure, and operates on S-boxes which depend on large keys. It's large key size and range makes the cipher increase its strength and opportunities of use. [3]

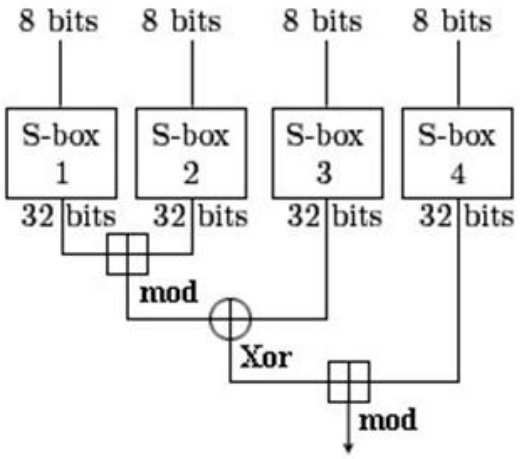

Fig -4: Blowfish F Function

3. METHODOLOGY OF COMPARATIVE ANALYSIS

The idea behind this project is to find the best encryption algorithm to encrypt text files taking into account four of the most popular software and hardware cryptographic algorithms, namely DES, Triple DES, RSA and Blowfish.

Primarily, the analysis was classified into two categories, as discussed below.

3.1 Theoretical Analysis

Cryptographic algorithms are preferred based on their strength. This is defined and is according to various factors that determine the amount of effort needed to break the cipher and retrieve plaintext form encrypted text. As a part of theoretical comparative Analysis, we looked into 8 different parameters that help differentiate between the four Encryption and Decryption ciphers. The parameters are:

•Development: Who developed the algorithm and when did it become public.[6]

•Key length: The length of key used by the cipher in each round.

•Rounds: The number of times the main function was repeated.

•Block Size: Size of the input block of text in bits [1].

•Encryption Ratio: Ratio of the Size of the encrypted part to the whole data size.

•Security Level: How impenetrable is this cipher determines its security level with adequate to high being the range.

•Attacks Found: Attacks that are successful against the respective cipher. [6]

3.2 Practical Analysis

•The Encryption algorithms were implemented in python and incorporated to a Django-based Web Application.

•It allows for the user to upload a text file and run the four encryption algorithms against it separately, retrieving the time taken to encrypt the text in the given text file.

•The times for encryption for each of the ciphers against text files of ten different sizes was noted and compared.

4. RESULTS AND DISCUSSION

The project efficiently differentiated between DES, Triple-DES, RSA and Blowfish. The Theoretical analysis yielded results as described in Table 1.

With respect to the Development methods, both DES and Triple DES found their start at IBM while the other two algorithms were not developed by an organization. Uniquely, Blowfish is credited to a single individual whereas RSA was founded by a team of three.

Key length of each cipher is a deciding factor to its strength and usability. In this project, all four algorithms being considered have different key lengths. RSA and Blowfish has variable wavelengths depending on the size of plaintext or cipher text given as input, while DES has a fixed 56 bit key. In the case of Triple DES, depending on whether the user wants to repeat keys, 112 bit keys or 168 bit keys can be used.

The speed of the ciphers that is expected is, DES and Triple DES are the slowest among the four algorithms. RSA is seen to be faster than the previous two, but Blowfish has been observed to be the fastest among the four, with a higher throughput capacity.

The basic idea behind rounds is that it is a complete unit of encryption or decryption operations applied on plaintext or cipher text respectively. This unit is repeated a given set of times to improve the strength of the function being applied on text. Out of the four, RSA does not follow this procedure, as it is involves executing a series of mathematical functions at once. This make it valid to count the number of rounds of encryption in RSA as one. However, DES and Blowfish employ sixteen rounds, while Triple DES has the highest number, leading at 48 rounds.

Three of the ciphers have a fixed 64 bit block size, but RSA allows for variable length of text as input for the algorithm. This allows for RSA to be more convenient to use, without requiring the plaintext or cipher text to be modified before applying the algorithm.

Encryption Ratio proves as an important parameter as it defines the speed at which the data can be transmitted after encryption, compared to the speed of the original data transmission. In this case, only Triple DES has a decent balance between the length of cipher text for the length of plaintext encrypted. The other three algorithms usually result in a larger cipher text compared to the plaintext.

Security Level, expressed in "bits", usually defines the exponential value with base 2 operations necessary to crack the cipher using brute force. Blowfish succeeds in this regard, with a very high ‘n’ bit value, followed by RSA and with Triple DES, DES coming in third.

The attacks that have been successful against the four ciphers respectively have been listed in Table 1.

The Practical Analysis was conducted in a series against files of ten different sizes. In an ascending order, the ciphers were run against each file, with their execution times noted down. Finally the throughput was calculated in MB/second to derive the following results, described in table 2.

5. CONCLUSION

It can be inferred from the practical analysis that among the symmetric ciphers, Blowfish has the highest speed. Given the understandable number of rounds in 3-DES, it is the slowest cipher. However, by paying attention to the theoretical analysis, it is confirmed that 3-DES is least easy to crack, making it very safe for communication, if compromise of time efficiency is acceptable.

Table -1: Theoretical Analysis of DES, Triple- DES, RSA and Blowfish

Parameters	Algorithms			
	DES	Triple DES	RSA	Blowfish
Development	1970 by the company IBM and was Published in 1977	IBM in the year 1978	By 3 people Ron Rivest, Shamir & Leonard Adleman in 1978	Bruce Schneier in 1993
Key length	56 bit key	112,168 bit key	variable key length, depends on the no. of bits in the module	Variable key length
Speed	Very Slow	Slow	Moderate	Very Fast
Rounds	16	48	1	16
Block Size	64	64	variable size	64
Encryption Ratio	High	Moderate	High	High
Security Level	Adequate	Adequate	Good	High Security
Attacks found	Differenti-al analysis, Linear cryptanaly sis	Related key attacks	Timing attack	No attacks are found to be effective

Table -2: Practical Analysis of DES, RSA, 3-DES and Blowfish

Input Size(KB)	Time taken to encrypt (s)			
	RSA	3-DES	DES	Blowfish
9 KB	0.026	0.059	0.023	0.089
28 KB	1.88	4.36	0.785	0.5
50 KB	2.49	7.43	1.29	1.01
83 KB	4.1	12.08	2.24	1.96
154 KB	9.73	21.7	4.66	3.15
279 KB	16.87	38.29	8.96	5.84
558 KB	31.42	59.07	17.01	10.76
837 KB	52.44	84.85	33.63	15.89
1022 KB	67.03	104.3	59.25	23.09
1952 KB	134.58	199.65	116.36	46.34
Throughput	1.43 MB/s	0.87 MB/s	1.92 MB/s	4.26 MB/s

REFERENCES

[1] Mohit Marwaha, Rajeev Bedi, Amritpal Singh, Tejinder Singh "COMPARATIVE ANALYSIS OF CRYPTOGRAPHIC ALGORITHMS" (2013).

[2] Rajdeep Bhanot and Rahul Hans, "Review and Comparative Analysis of Various Encryption Algorithms" (2015).

[3] Monika Agarwal, Pradeep Mishra ".A Comparative Survey on Symmetric Key Encryption Techniques" (2012).

[4] Sunil Kumar Sahu, Aja Kushwaha "Performance Analysis of Symmetric Encryption Algorithms for Mobile ad hoc Network" (2014).

[5] Amritpal Singh, Mohit Marwaha, Baljinder Singh, Sandeep Singh "Comparative Study of DES, 3DES, AES and RSA" (2013)

[6] Hemangi Zope, Prof. Savita Sangam, "Comparative Analysis of Various Encryption Algorithms and Techniques", IJRASET (2017).

[7] Text book By William Stallings "Cryptography and Network Security Principles and Practices" Fourth Edition (2005)

[8] Atul Kahate "cryptography and network security", Tata McGraw-Hill publishing company, New Delhi, 2008.

[9] D. Asir Antontony Gnana Singh, R.Priyadharshini, "Performance Analysis of Data Encryption Algorithms for Secure Data Transmission" (2016).

[10] W. Diffie, E Hellman" New Directions in Cryptography", 1976.