# COLLABORATIVE CRYPTOGRAPHIC MODEL

**A Project Report of Capstone Project - 2**

***Submitted By***

**KAMAL NAYAN**

**(1613101314/ 16SCSE101865)**

***In partial fulfillment for the award of the degree***

***of***

**BACHELOR OF TECHNOLOGY**

**IN**

**COMPUTER SCIENCE AND ENGINEERING**

**SCHOOL OF COMPUTING SCIENCE AND ENGINEERING**

**Under the Supervision of**

**Mrs. KAMAKSHI GUPTA**

**Assistant Professor**

**MAY 2020**

## *SCHOOL OF COMPUTER SCIENCE AND ENGINEERING*

## BONAFIDE CERTIFICATE

Certified that this project report "**COLLABORATIVE CRYPTOGRAPHIC MODEL**" is the bonafide work of "**KAMAL NAYAN (1613101314)**" who carried out the project work under my supervision.

**SIGNATURE OF SUPERVISOR** **SIGNATURE OF HEAD**

Mrs KAMAKSHI GUPTA, M.Tech.

**SUPERVISOR**

Mrs KAMAKSHI GUPTA, M.Tech

**Assistant Professor,**

**School of Computing Science &**
**Engineering**

Mr. MUNISH SABARBAL

**PhD (Management),PHD(CS)**

**Professor & Dean,**

**School of Computing Science&**
**Engineering**

# Abstract

It was a preliminary endeavor to gain first hand understanding of scope, problems, hurdles and challenges to be encountered in the development of collaborative cryptographic model. The study of transfer of secret messages from reciever end to sender  is called cryptography. Normally, senders and receivers are ignorant about the process of encryption and decryption. Therefore, encryption plays an important role in data communication and data security. The importance of encryption is not only to keep data confidential from useless access but also ensuring the data integrity through available way. As the ability of breaching the security is increasing rapidly, so, the process that hides information is one of the most apprehensive topic. Symmetric and asymmetric encryption are  popular, widely used and proficient encryption algorithms, which has been used since they were invented. This paper focuses on the combination of both symmetric and asymmetric encryption algorithms. Because we know that symmetric encryption algorithms are faster in reference of time as compared to asymmetric encryption algorithms.Whereas on the other hand asymmetric encryption algorithms are more secure.So we will try to get the best of both the worlds.Hence, we propose combined encryption as a sequence of different encryption algorithms with good performance, low decoding complexity, regular structure, and that can be scaled to a much bigger level.

***Keywords—SYMMETRIC encryption algorithm; ASYMMETRIC encryption algorithm; Cryptography , Integrity.***

## TABLE OF CONTENTS

# 1. INTRODUCTION

## 1.1 **BACKGROUND**

The rate at which the data is being transferred is increasing day after day. So in order to give full guarantee over secured data transmission from sender to receiver ends is of great concern.This paper tries to present a combination of some of the most efficient encryption algorithms in cryptography by combining the most common and used algorithms in the data encryption field. In this proposed method, a hybrid technique is used. In this technique, we try to use a combination of some asymmetric encryption as well as symmetric encryption to transfer data between the sender and receiver promptly and also providing better security.

Since our main concern here is the efficiency and security of the transferred data and for the performance of that, the performance of these algorithms under different settings is a big concern, the presented solutions takes into consideration the performance and the behavior of the algorithm when different data loads are used.

## 1.2 **CRYPTOGRAPHY**

Cryptography means securing information through codes so that only the intended user can read and process it. The pre-fix "crypt" means "hidden" or "vault" and the suffix "graphy" stands for "writing." Encryption is the process of converting plain text "unhidden" to a cryptic text "hidden" to secure it against data thieves. Decryption is the process where this hidden text needs to be transformed back to unhidden text to be understood on the other end. Fig.1 shows the simple flow of encryption algorithms.

### 1.2.1 **CRYPTOGRAPHY GOALS**

The goals of the security system can be listed under the following five main categories:

1. ***Authentication:*** This means that before sending and receiving data using the system, a user or system can prove their identity to another who does not have personal knowledge of their identity

2. ***Confidentiality:*** It means the assurance that only the intended recipient of a message can read it. This is the primary goal of classical cryptography.

3. ***Integrity:*** Integrity means that a piece of information has not been altered between the endpoints.

4. ***Non-Repudiation:*** It gives an assurance that neither the sender nor the receiver can falsely deny that they have sent or received a certain message.

5. ***Service Reliability and Availability:*** It happens that all security systems usually get attacked by intruders, which may affect their availability and type of service to their users. These systems should provide a way to grant their users the quality of service they expect.

## 1.3. **BLOCK AND STREAM CIPHERS**

There are two categories for encryption techniques that are based on their operation on the input data form. These two types are:

- Block Cipher
- Stream Cipher

### 1.3.1. **BLOCK CIPER**

In Block cipher the encryption and decryption of data are done in the form of blocks. The input data is first divided in the form of blocks, these blocks are then passed into the cipher system, and these cipher system then produce blocks of ciphertext. A very basic model of a block cipher is ECB (Electronic Codebook Mode).

### 1.3.2. **STREAM CIPHER**

In Stream cipher, the encryption and decryption is done by operating on bits of data. Major components of a stream cipher can be stated as, a keystream generator, and a mixing function. The main element of a stream cipher is the keystream generator whereas the mixing function can be generally seen as the XOR function.

## 2. SYMMETRIC AND ASYMMETRIC ENCRYPTIONS

Data encryption procedures are mainly categorized into two categories depending on the type of keys used to encrypt/decrypt the data involved in the transmission. These two categories are:

- Asymmetric Key Encryption
- Symmetric encryption techniques

### 2.1 SYMMETRIC ENCRYPTION

Symmetric encryption is a type of encryption where only one key (a secret key) is used to both encrypt and decrypt information. The entities communicating via symmetric encryption must exchange the key so that it can be used in the encryption and decryption for transmission of data. The Sender and Receiver first decide a mutual technique that will be used in the process. Fig. 4 shows the process of symmetric encryption. Then they come up with mutual consent on a secret key that both of them will use in this connection. After the encryption setup finishes, the sender starts sending its plain data after encrypting it with the shared (agreed) key, on the other side receiver uses the same key to decrypt the encrypted messages.

### 2.1.1 DISADVANTAGE OF SYMMETRIC ENCRYPTION

The major disadvantage of symmetric key encryption techniques is that all the communicating nodes have to share the key that was used to encrypt the data before the other nodes can decrypt it. If anyhow the key gets compromised and the intruder gets to know the key by any means, the whole system will collapse.

## 2.2 ASYMMMETRIC ENCRYPTION

Asymmetric encryption is a type of encryption where two keys are used for encryption and decryption for the data transmission. For instance, when data is encrypted using Key1 then it can only be decrypted using Key2, and vice versa. It is also called Public Key Cryptography (PKC), because of the use of two keys: a public key, which is known to the all, and private key which is known only to the specific user. Figure 5 below shows the use of the two keys between the sender and receiver. After coming up on a mutual technique that will be used in encryption and decryption for transmission of data, the receiver sends its public key to the sender. Sender uses the received public key to encrypt the data to be transmitted. Then when the encrypted data arrives at the receiver’s end, the receiver uses its private key to decrypt the data.

### 2.2.1 ADVANTAGE OF ASYMMETRIC ENCRYPTION

The capability of using two keys for encryption surmounts the problems of symmetric encryption techniques of managing secret keys. However, at the same time, this unique feature of this asymmetric encryption makes it more prone to attacks. And at the same time, the asymmetric encryption algorithms are significantly slower than symmetric encryption algorithms, due to the requirement of more computational processing power.

## 3. COMPARED ALGORITHMS

This segment plans to give the requisite background understanding to the readers to differentiate the compared algorithms.

**3.1 DES**: The Data Encryption Standard is a symmetric key encryption algorithm. It uses a short key of length 56 bits which makes it not recommendable for modern-day applications. DES became a standard in 1974 [3]. Hence that time onwards, many attacks and methods have been observed that surface the weaknesses of DES, thus making the DES encryption insecure block cipher technique.

**3.2 3DES:** Triple-DES (3DES or TDES), which now officially known as the Triple Data Encryption Algorithm (TDEA or Triple DEA), is a symmetric key encryption technique, which includes the application of the DES encryption algorithm three times to each data block in the transmitted data. Triple DES (3DES), uses the same DES algorithm to produce a more secure encryption for the same data which can be considered more adequate. However, it can also be inferred from its implementation that 3DES is slower than other block cipher methods.

**3.3 AES:** Advanced Encryption Standard, can also be stated as Rijndael. It is a technique for the encryption of data. The AES was established by the NIST in 2001, to replace DES. The Rijndael algorithm is vulnerable only to the Brute force attacks as known till now, i.e. the attacker must try all the possible combinations of characters to decrypt the encrypted data. The AES are block cipher techniques.

**3.4 Blowfish:** Blowfish is a symmetric key encryption technique, provided by Bruce Schneier in 1993. The Blowfish algorithm is also a part of many products available for encryption in the market. Blowfish also proves to be a good encryption algorithm by resulting in a good encryption rate when used in various software. The key length on the Blowfish cipher technique is variable as well. Generally, a 64-bit length key is used for block cipher in Blowfish. The Blowfish algorithm also suffers from weak key problem, however, no successful attack is known against this algorithm.

**3.5 RSA:RSA** is a asymmetric algorithm used in mordern days by mordern computers to encrypt and decrypt messages.It is an assymetric cryptographic algorithm i.e. it uses both public and private keys for crtptography.It is also called public key cryptography because one of the keys can be given to anyone.

## 4. RELATED WORKS AND STUDIES

In the specified paper, the symmetric key algorithms like Blowfish, AES (Rijndael), DES and 3DES were compared for their performance by encrypting input files having different contents and different sizes. These algorithms were carried out in a basic programming language, using specifications as per standards, and tests were carried out on two different platforms as well, to have a better comparison for their performance. The tables Table 1 shows the results of the carried-out comparisons, in which they have performed the experiments on two machines that are having processors: P-II 266 MHz and P-4 2.4 GHz.

## 4.1 OBSERVATION IN WORKS AND STUDIES

It can be easily observed from the results that the Blowfish encryption algorithm has an advantage over other encryption algorithms in terms of production rate. The results showed that Blowfish has a better performance when compared to other encryption algorithms. Moreover, it can be inferred that the AES encryption algorithm has a better performance than the 3DES and DES algorithms. From the above results it can also be inferred that the 3DES encryption algorithm has almost 1/3 production rate of the DES algorithm, or we can also say that it requires 3 times the time than DES to process equal amounts of data.

Dhawan has also performed some experiments in his paper for a comparison of the performances of the different types of encryption algorithms that were implemented using the .NET framework. However, their results are very much closer to the ones that were shown before .

The experiment was carried out on these algorithms: AES (Rijndael), DES, Triple DES (3DES) and RC2. These results show that AES performed better than other encryption algorithms in all the tested cases like the requests processing rate over different user loads, as well as in response time.

## 5. CONCLUSION

Cryptography is a very robust and wide area of study.The proposed model here tries to emphasize the advantages of combining different systems into one. In current state of cryptography, the keys are the most crucial tools in keeping the data secure and large enough to make it very difficult to crack this encryption system by any type of active or passive attackers.

## 6. REFERENCES

[1] [Edney2003] ”Real 802.11 Security: Wi-Fi Protected Access and 802.11i", . Addison Wesley 2003

[2] [ Hardjono2005] "Security In Wireless LANS And MANS,". Artech House Publishers 2005

[3] [TropSoft] "DES Overview", [Explains how DES works in details, features and weaknesses]

[4] [BRUCE1996] BRUCE SCHNEIER, "Applied Cryptography", John Wiley & Sons, Inc 1996

[5] [Nadeem2005] “Aamer Nadeem et al, "A Performance Comparison of Data Encryption Algorithms", IEEE 2005

[6] [Dhawan2002] Priya Dhawan., "Performance Comparison:

Security Design Choices," Microsoft Developer Network

October 2002. http://msdn2.microsoft.com/en-us/library/ms978415.aspx

[7] [BlowFish.NET] "Coder's Lagoon",http://www.hotpixel.net/software.html [List of

resources to be used under GNU]

[8] Encrypting data with the blowfish algorithm https://www.embedded.com/encrypting-data-with-the-blowfish-algorithm/

[9] Advanced Encryption Standards https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[10] Cryptography and Techniques https://en.wikipedia.org/wiki/Cryptography

[11] Data Encryption Standard https://en.wikipedia.org/wiki/Data_Encryption_Standard

[12] Triple DES https://en.wikipedia.org/wiki/Triple_DES

[13] Public Key Cryptography https://en.wikipedia.org/wiki/Public-key_cryptography

[14] Blowfish (Cipher) https://en.wikipedia.org/wiki/Blowfish_(cipher).