Performance Evaluation of Hybrid Cryptography System

Er. Parvin Shaikh[#1], Dr. SonaliPatil[*2]

[#]*Student,* [*]*Professor, Department of Information Technology (Information Security), K.J. Somaiya College of Engineering (Aff. To Mumbai University), Vidyavihar East, Mumbai, India*

Abstract- *The spectacular growth of the Internet has make an increased awareness of an interest in security issues. Although Security is measure concern over internet, many applications have been developed and designed without considering main objectives of information security that is confidentiality, authentication, and privacy. As our daily activities become more and more reliant upon data networks, the importance of an understanding of Such security issues will also increase. Cryptography plays important role in secure data communication. First Phase of this paper presents the development of Hybrid Cryptography system which contains Chaffing & Winnowing Algorithm, Diffie-Hellman Key Exchange Algorithm and Advanced Encryption Standard (AES)algorithm and second phase of the paper shows the performance evaluation of AES, Chaffing &Winnowing, Diffie Hellman Key Exchange Algorithm and Hybrid Cryptographic Algorithms. Cryptography algorithms provide a secure data communication over the internet and play key role in any security system. In this paper, different experiments have been conducted to compare these algorithms in term of encryption time, decryption time and throughput over variable concurrency for fixed time and BruteForce attack resistance capability among all algorithm.*

Keywords—*Encryption, Decryption, Hybrid Cryptography, Diffie Hellman Key Exchange, AES, Chaffing and Winnowing.*

I. INTRODUCTION

For security of data communication over public network, various cryptographic methods and algorithms are used. The cryptographic methods are divided as symmetric cryptography and asymmetric cryptography method. Same key is used for encryption as well as for decryption in symmetric cryptography methods unlike asymmetric cryptography method. The problem with symmetric cryptography method is that participants should share a secret key among each other in a secure way which is difficult. Asymmetric cryptography method overcome the issue of key sharing by using 2 keys.This paper presents the implementation and comparison of AES, Chaffing &Winnowing, Diffie Hellman Key Exchange Algorithm and Hybrid Cryptographic Algorithmsfor variable concurrency for fixed time. Our Aim is to compare the cryptography algorithm to calculate the performance evaluation among selected algorithm by calculating encryption time, decryption time and throughput for each algorithm to identify which algorithms outperforms others in term ofparameters decided for comparison. This paper is organized as follows: Section 2 of this paper describes ProposedArchitecture Section 3 highlights parameters used for the comparison evaluation. Section 4 describes experimental setting and data required for the Evaluation, results are shown in section 5 and Section 6 presents conclusion of the research work.

II. PROPOSED ARCHITECTURE

Considering the anomalies in the existing system computerization of the whole activity is being suggested after initial understanding and analysis of both symmetric and asymmetric key cryptography algorithms and by studying the security provided by Symmetric and Asymmetric cryptography separately and by comparing it with hybrid cryptography algorithm. Various test cases and experiments have been used to determine the performance of the selected symmetric and asymmetric cryptography with hybridcryptography algorithms. The Hybrid Cryptography system is developed using Visual Studio with C# .Net as programming language for securely data transformation.

A. System Feasibility

Using hybrid cryptography strategy and existing Encryption and decryption algorithm methods, this proposed architecture will be in great demand. It will provide various potential applications related to Secure Communication mainly for secure data communication and transformation over internet: ATM systems, Image encryption and Secure Storage Confidential Cooperate Documents, Government Documents,FBI Files, Personal Storage Devices Person Information Protection and hence, this system is quite feasible in the current situation where data security is so much important and less supply of secure data transfer system.

B. Merits

Following are the merits of Hybrid Cryptography System

1. System with high performance.

2. Very efficient at encrypting large amount of bulk data.
3. Provide Authenticity by solving key distribution issue.
4. Confidential information will be sent to legitimate user only. Secret key cannot be sent to attacker ID.
5. Email functionality is provided. All secret data or key can be received via Emails
6. Multiple level of security such as
   - Padding Character should be matched at decryption site
   - Private or Public Key should be matched at decryption site
   - To trick hacker, no error is shown if user provide wrong key or padding Character.
   - To make plain text into cipher text, data is passed through 3 different algorithms named as Diffie Hellman key exchange algorithm, Chaffing and winnowing algorithm, AES and paddingcharacter.
7. Diffie Hellman shared key is used for AES Encryption.

C. *Demerits*

Following is the main disadvantage of Hybrid Cryptography System

1. System response time is average.

D. *Modules*

Following modulesis implemented in developed Hybrid Cryptography System.

1. *Hybrid Cryptography Encryption*

Following process is followed in Hybrid Cryptography Encryption

- Plain text is replaced using Chaffing and Winnowing algorithm and generates new text.
- Shared key is generated using Diffie-Hellman algorithm.
- Shared secret key is used to encrypt the replaced text using Advance Encryption Standard (AES) algorithm.
- Finally padding Characters are added to left or right of encrypted text generated after AES Encryption Process and creates more complex cipher text which is difficult to break.
- Final Cipher Text is sent to Receiver via Email along with Padding Character and Padding Position (LEFT/RIGHT).

Figure 1 shows Hybrid Cryptography Encryption process

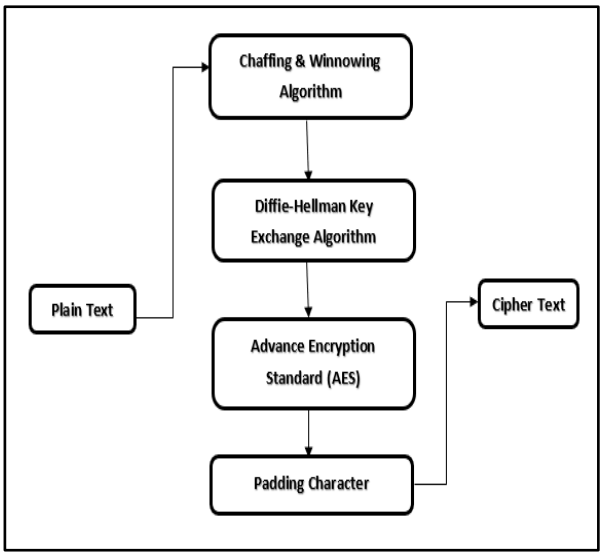

Figure 1: Hybrid Cryptography Encryption Process

2. *Hybrid Cryptography Decryption*

- Padding characters are removed from Cipher text choosing correct padding place (Left or Right).
- Shared secret key is generated using Diffie-Hellman algorithm.
- Cipher text is decrypted using AES with shared secret key.
- Finally, text is replaced using Chaffing and Winnowing algorithm and generate plain text.

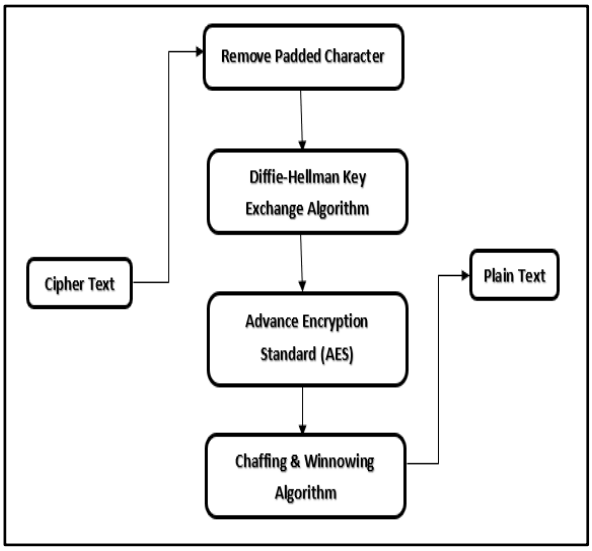

Figure 2 : Hybridcryptography Decryption Process

3. *Chaffing and Winnowing*

Thisis separate module which replaced plain text and generate new text.

4. *Key Generation*

This is separate module which generate key using Diffie Hellman key exchange algorithm which uses

two prime numbers , public key and user's private information.

5. AES Encryption & Decryption

There is separate module provided for AES Encryption and Decryption in which Plain text is encrypted using AES algorithm. User is asked to provide the key and text will be encrypted and decrypted.

E. Algorithm Used

For building "encryption and decryption using hybrid cryptography" system following algorithm are used

1. Chaffing and Winnowing

Chaffing and winnowing is a cryptographic technique to achieve confidentiality without using encryption when sending data over an insecure channel. The name is derived from agriculture: after grain has been harvested and threshed, it remains mixed together with inedible fibrous chaff. The chaff and grain are then separated by winnowing, and the chaff is discarded. The technique was conceived by Ron Rivestand published in an on-line article on 18 March 1998. Although it bears similarities to both traditional encryption and steganography, it cannot be classified under either category[1].

This technique allows the sender to deny responsibility for encrypting their message. When using chaffing and winnowing, the sender transmits the message unencrypted, in clear text. Although the sender and the receiver share a secretkey, they use it only for authentication. However, a third party can make their communication confidential by simultaneously sending specially crafted messages through the same channel[2].

2. Diffie Hellman Key Exchange Algorithm

Diffie-Hellman key exchange offers the best of both worlds -- it uses public key techniques to allow the exchange of a private encryption key. Let's look at how the protocol works, from the perspective of Alice and Bob, two users who wish to establish secure communications [3]. We can assume that Alice and Bob know nothing abouteach other but are in contact.

Here are the eight steps of the process:

1. Communicating in the clear, Alice and Bob agree on two large positive integers, n and g, with the stipulation that n is a prime number and g is a generator of n.
2. Alice randomly chooses another large positive integer, XA, which is smaller than n. XA will serve as Alice's private key.
3. Bob similarly chooses his own private key, XB.
4. Alice computes her public key, YA, using the formula YA = (g^XA) mod n.
5. Bob similarly computes his public key, YB, using the formula YB = (g^XB) mod n.
6. Alice and Bob exchange public keys over the insecure circuit.
7. Alice computes the shared secret key, k, using the formula k = (YB ^XA) mod n.
8. Bob computes the same shared secret key, k, using the formula k = (YA ^XB) mod n.

Alice and Bob communicate using the symmetric algorithm of their choice and the shared secret key, k, which was never transmitted over the insecure circuit.

3. Advance Encryption Standard (AES)

AES is a symmetric key block cipher encryption algorithm designed by Vincent Rijmen and Joan Daemen in 1998. It is based on Feistel network and support 128 bit block size and key length 128, 192 and 256 bits. AES performs 10, 12 or 14 round and the number of rounds depends on the key. It means for 128 bit key length AES performs 10 rounds, for192 bit key it performs 12 rounds and for 256 bit key it performs 14 rounds. In AES each round performs some steps. Key-expansion, Initial-round, Rounds and Final-rounds. In Rounds step, Sub-byte generation, Shift-rows, Mix-columns and Add-round_key are performed whereas in Final-rounds step, same functions are performed except Mix-columns function [4].

There is separate module provided for AES Encryption and Decryption in which Plain text is encrypted using AES algorithm. User is asked to provide the key and text will be encrypted and decrypted.

III. EVALUATION PARAMETERS

Following parameters were selected for comparing performance of AES, Chaffing &Winnowing, Diffie Hellman Key Exchange Algorithm and Hybrid Cryptographic Algorithms.

1. Encryption/Decryption time (Computation Time/ Response Time)

The encryption time can be calculated as the time that algorithm require to make a encrypted text (cipher text) from plain text.The decryption time can be calculated as the time that an algorithm takes to regeneratea original plain text from a cipher text.

2. Throughput

Throughput can be calculated as total encrypted plaintext (bytes) divided by the encryption time. Higher the throughput is considered as high performance.

3. *Brute Force Attack*

Brute force attack is a trial-and-error method used to obtain information by generating many consecutive guesses and combination as to the value of the desired data.

IVEXPERIMENTAL SETTING AND DATA

This Experiment was performed on Intel(R) Pentium(R) 2 Dual CPU E2140 @1.60 GHz processor with 4 GB of RAM on Windows 7 operating system. Tool used for experiments is JMeter. Experiments were carried out on variable concurrency like 50 users, 200 users, 400 users and 600 users for fixed period i.e. for 10 Minutes.

V.RESULTS

A. Performance Evaluation based on response time

Table 1 and Figure 3 show Performance among all algorithms for 50, 200, 400 and 600 concurrenciesfor period of 10 minutes. AES (Advance Encryption Standard) showed better performance over Diffie Hellman Algorithm, Chaffing &Winnowing and Hybrid Cryptography Encryption and Decryption algorithm in term of speed.

Algorithm\ concurrency	**50 users**	**200 users**	**400 users**	**600 users**
AES	11.332	39.223	56.431	64.814
Diffie Hellman	14.469	47.359	60.588	67.978
Chaffing & Winnowing	14.409	42.508	55.799	59.546
Hybrid Cryptography Encryption	18.506	58.171	88.385	91.819
Hybrid Cryptography Decryption	21.429	63.092	78.703	87.858

Table 1: Response time for all algorithms

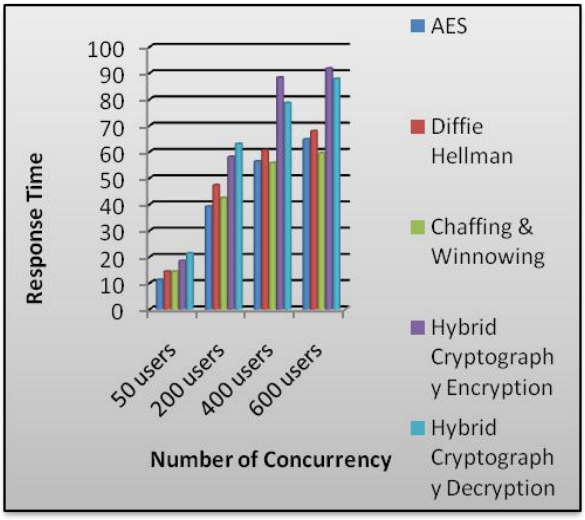

Figure 3: Response Time Graph for all algorithms

B. Performance Evaluation based on Throughput

Table 2 and Figure 4 shows Performance Evaluation among all algorithms based on throughput for 50, 200, 400 and 600 concurrency (users) for period of 10 minutes.

Hybrid Cryptography Encryption and Decryption algorithm showed better performance over AES (Advance Encryption Standard),Diffie Hellman Algorithm, Chaffing &Winnowing algorithm in terms of throughput.

Algorithm\concurrency	**50 users**	**200 users**	**400 users**	**600 users**
AES	0.90259	1.03937	1.19785	1.53219
Diffie Hellman	0.90533	1.06854	1.32806	1.64886
Chaffing & Winnowing	0.89191	1.11889	1.44471	1.79306
Hybrid Cryptography Encryption	0.94319	1.33268	1.82063	2.23261
Hybrid Cryptography Decryption	0.92875	1.23619	1.67738	2.06499

Table 2: Throughput for all algorithm

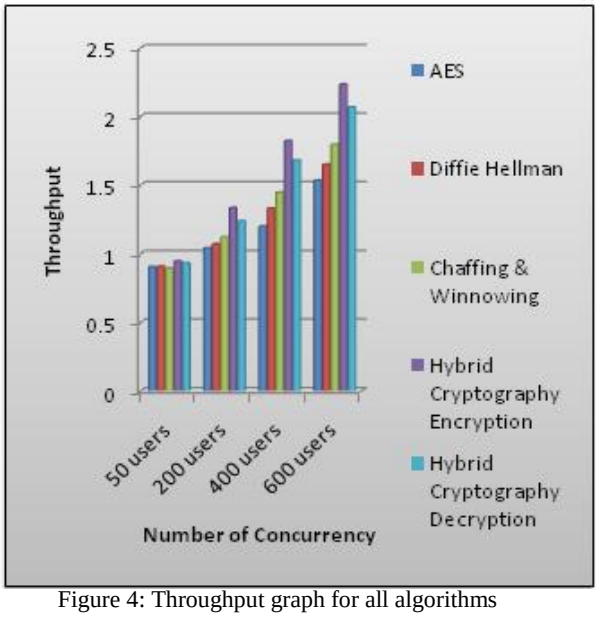

Figure 4: Throughput graph for all algorithms

C. Performance Evaluation based on Brute Force Attack Resistance Capability

To compare Brute Force attack resistance capability among all algorithms, sample easy data is chosen for each algorithm.

1. *Chaffing and Winnowing Algorithm*

To test Brute force attack on Chaffing and Winnowing algorithm sample easy plain text is chosen as follow

- Plain Text: hello
- Winnowing & Chaffing Output: c6tth

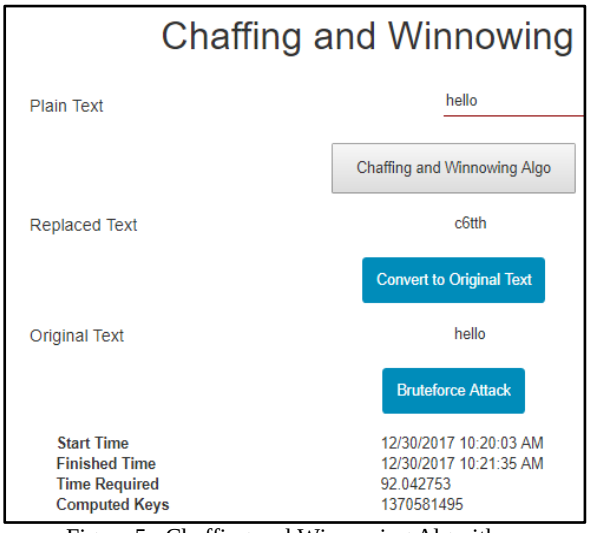

Figure 5 : Chaffing and Winnowing Algorithm

2. *Diffie Hellman Key Exchange Algorithm*

To test Brute force attack on Diffie Hellman Key Exchange Algorithm sample example is chosen as follow

i. Alice and Bob agree to use a modulus p = 23 and base g = 5 (which is a primitive root modulo 23).

ii. Alice chooses a secret integer a = 4, then sends Bob A = g^a mod p
   - A = 5^4 mod 23 = 4

iii. Bob chooses a secret integer b = 3, then sends Alice B = gb mod p
   - B = 5^3 mod 23 = 10

iv. Alice computes s = Ba mod p
   - s = 10^4 mod 23 = 18

v. Bob computes s = Ab mod p
   - s = 4^3 mod 23 = 18

vi. Alice and Bob now share a secret key (the number is 18).

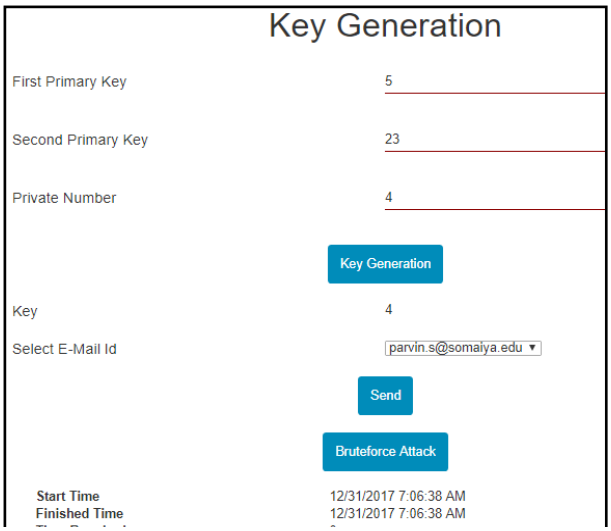

Figure 6 : Diffie Hellman Key Generation Algorithm

3. *Advance Encryption Standard (AES)*

To test Brute force attack on Advance Encryption Standard Algorithm sample example is chosen as follow

- Plain Text: c6tth
- Key: 18

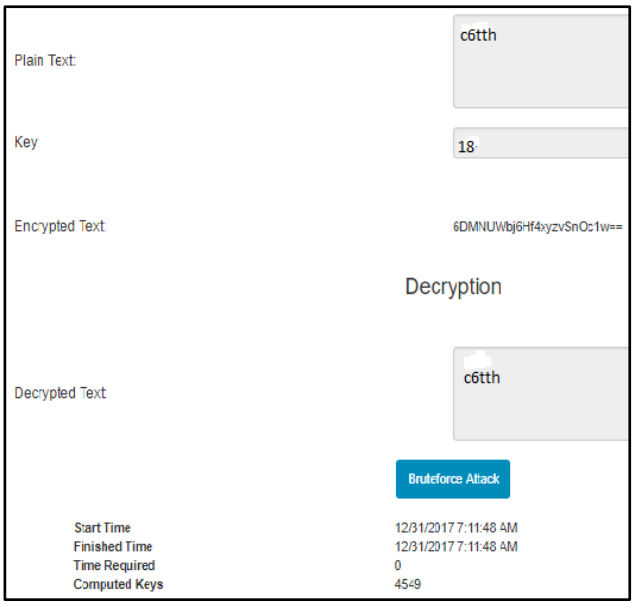

Figure 7: Advance Encryption Standard

4. *Hybrid Cryptography system*

Above mentioned sample data of each algorithm are used for Hybrid Cryptography system. Following steps to be followed

STEP 1 : Key Sharing

Sender and Receiver must exchange the key using key generation module. Please note that both Sender

and Receiver should perform key generation process at their end to exchange the key.

- Sender with email id parvin.s@somaiya.edukey using Diffie-Hellman key generation module as follow

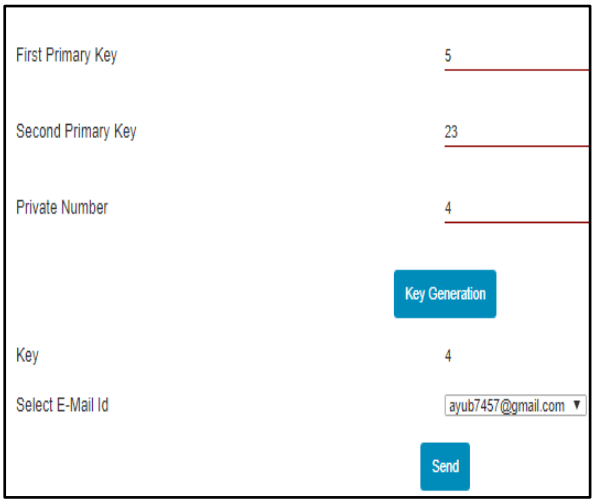

Figure 8: Sender generates Key using key generation

- Sender sent the key to receiver Email-Id.

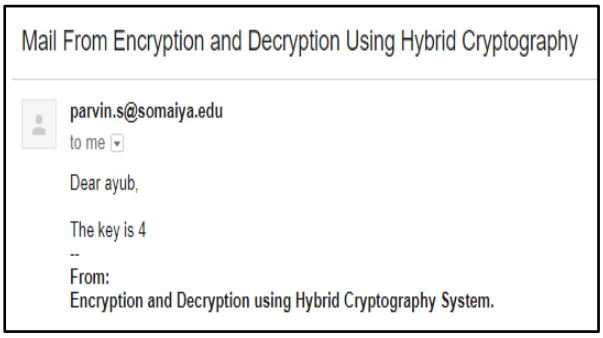

Figure 9: Key is sent to receiver Email id

- Similar way Receiver will generate key using Diffie Hellman key generation module and share it with sender via Email as follow

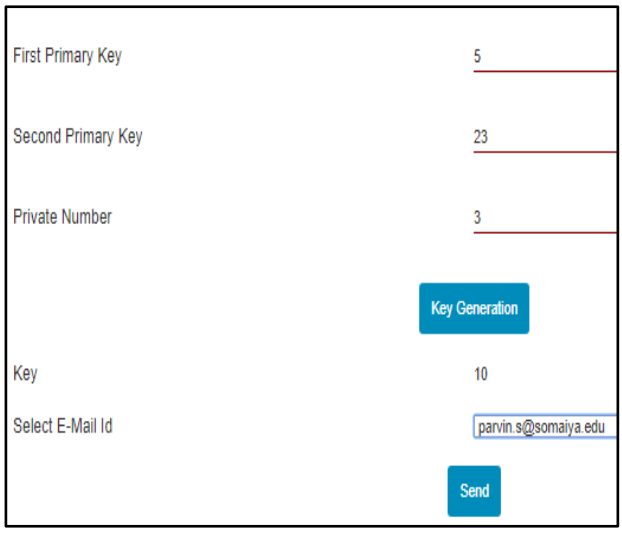

Figure10: Receiver generates Key

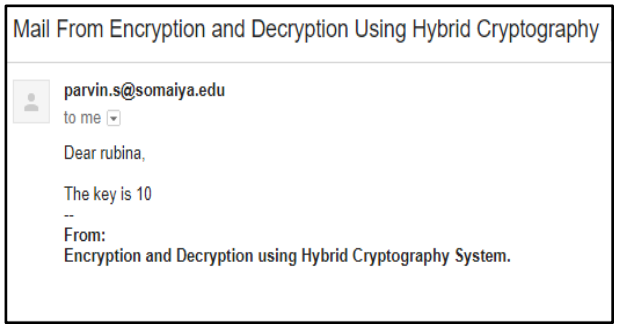

Figure 11 : Key is sent to Sender Email id

STEP 2: Encryption Process

Before sender start Encryption, he/she need tohave receiver public key generated by Diffie Hellman algorithm at receiver end.

- Plain text is replaced using Chaffing and Winnowing algorithm and generates new text.
- Shared key is used along with other required information like prime numbers. Shared secret key is used to encrypt the replaced text using Advance Encryption Standard (AES) algorithm and generates cipher text.
- Finally padding Characters are added to left or right of encrypted text generated after AES Encryption Process and creates more complex cipher text which is difficult to break.
- Final Cipher Text is sent to Receiver via Email along with Padding Character and Padding Position (LEFT/RIGHT).

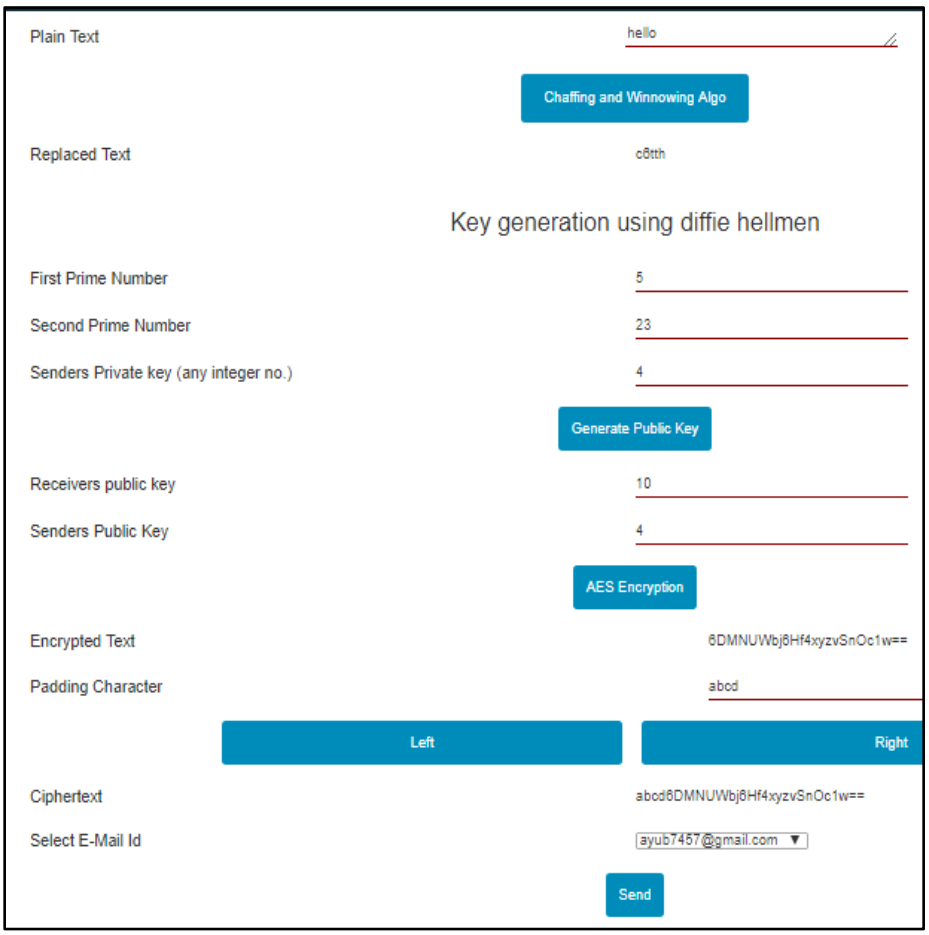

Figure 12: Hybrid Cryptography Encryption Process

- Senders sent confidential information like Cipher text, Padding character and Padding place to receiver Email Id (ayub7457@gmail.com) .

Figure 13: Confidential Information is sent to email id

- Receiver gets all required information from sender on Email id provided while registration as shown below

Figure 14: Receiver gets required information

STEP 3: Decryption Process

Before receiver start decryption, he/she need to have sender public key generated using Diffie Hellman algorithm at sender end, padding place. Using Decryption module, Receiver decrypt the ciphertext

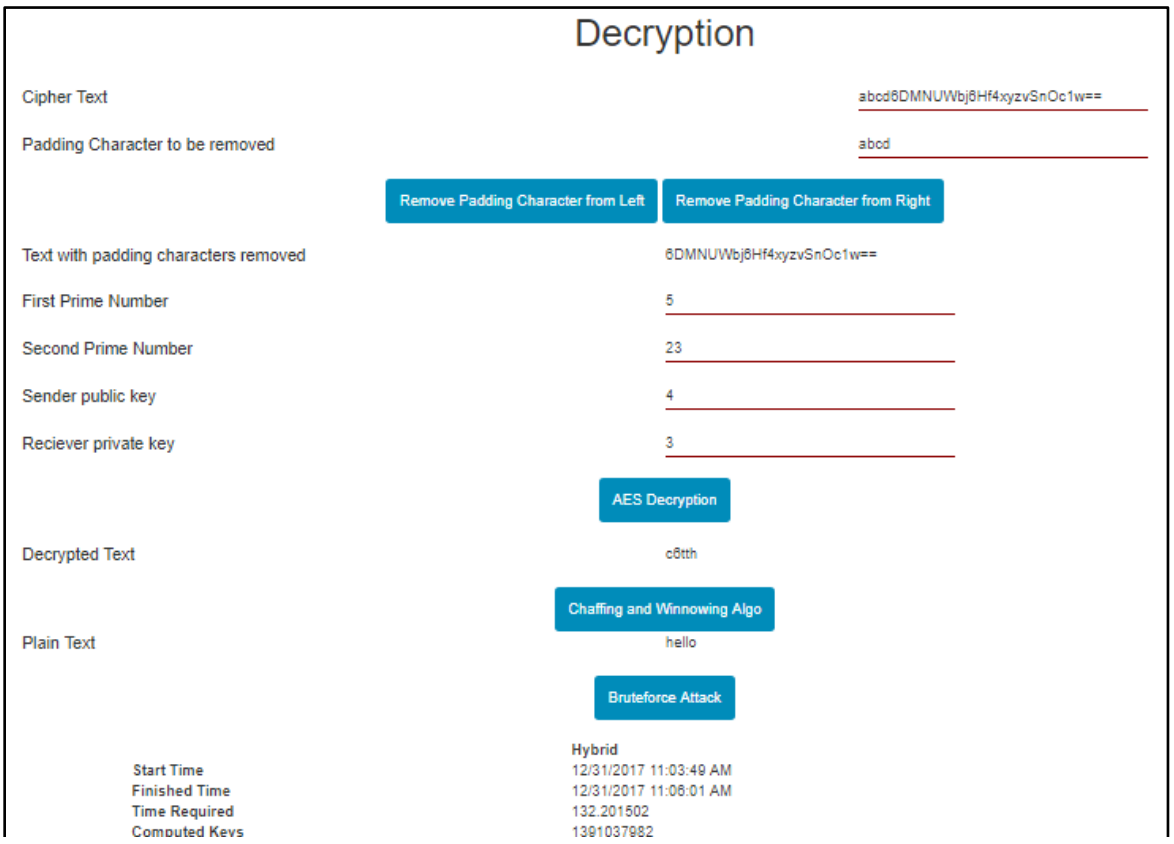

Figure 15: Hybrid Cryptography Decryption Process

Figure 15 shows the Hybrid Decryption Process in which below sequence is used to decrypt the cipher to get the plaintext.

- Padding characters are removed from Cipher text choosing correct padding place (Left or Right).
- Shared secret key is generated using Diffie-Hellman algorithm.
- Cipher text is decrypted using AES with shared secret key.
- Finally, text is replaced using Chaffing and Winnowing algorithm and generate plain text.

Table 3 show resistance capabilityamong all algorithms against Brute Force Attack. Hybrid Cryptography system showed better performance over Diffie Hellman Algorithm, Chaffing &Winnowing Algorithm and Advance Encryption Standard algorithm.

Algorithm\ BruteForce	Start Time	Finish Time	Time Required (sec)	Computed Key
AES	7:08:48 AM	7:08:48 AM	0	4549
Diffie Hellman	7:06:38 AM	7:06:38 AM	0	56
Chaffing &Winnowing	10:20:03 AM	10:21:35 AM	92.042753	1370581495
Hybrid Cryptography system	11:03:49 AM	11:06:01 AM	132.201502	1391037982

Table 3:Resistance Capabilityamong all algorithms against Brute Force Attack

VI. CONCLUSION

It is System Design about "Encryption & Decryption using Hybrid Cryptography" application based on C# i.e. Windows Application. It gives more security for Encryption & Decryption of data as system uses Hybrid cryptography algorithms. Hybrid Cryptography Algorithm is very efficient at Encrypting large amount of bulk data and it solves key distribution issue also. Though every task is never said to be perfect in security perspective even more improvement may be possible in this application to achieve more security then existing system.

An efficient algorithm should provide maximum security with operation performed in less time. The hybrid combination of above mentioned algorithms is more secured, and it also provides completion in less time as when combined with high security. We can also implement some other algorithms to improve the security of the system by improving the key length and by using efficient combination of algorithms in future to develop more secure system.

This paper also presents the comparison of AES, Diffie Hellman Key exchange algorithm, chaffing and winnowing algorithm and Hybrid Cryptography system in term of encryption time, decryption time, throughput and Brute Force attack. Different experiments were conducted for comparison of these algorithms and it is concluded that Hybrid Cryptography algorithm performed better in term of throughput, AES in term of performance time. Throughput is the most important parameter that demonstrates the performance of any algorithm. Brute Force attack resistance capability were also performed among all algorithm It is observed that Brute force attack resistance capability of Hybrid Cryptography is better than Advance Encryption Standard (AES), Diffie Hellman Key Exchange Algorithm and Chaffing and Winnowing Algorithm.

ACKNOWLEDGEMENT

I offer my profound gratitude towards all thestaff members of K. J. Somaiya College of Engineering, Vidyavihar, Mumbai for providing me all academic assistancerequired to complete this research paper.

I would like to thank my colleagues, who have contributedto ease the understanding of this project and this paper by giving their time and taking a keen interest in making this a success.

REFERENCES

[1] https://en.wikipedia.org/wiki/Chaffing_and_winnowing.
[2] Aaron D Schroeder, "Pad and Chaff: Secure Approximate String Matching in Private Record Linkage".
[3] The People's Armed Police Force Academy of China, "Research on Diffie-Hellman Key Exchange Protocol", 2nd International Conference on Computer Engineering and Technology [Volume 4] , 2010.
[4] Abdullah Al Hasib, Abul Ahsan Md. MahmudulHaque , "A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography" Third International Conference on Convergence and Hybrid Information Technology, 2008.
[5] Shahzadifarah, m. Younasjaved, Azrashamim, Tabassamnawaz "An experimental study on Performance Evaluation of Asymmetric Encryption Algorithms" WSEAS 3rd European Conference of Computer Science (WSEAS ECCS) December 2012.
[6] DepavathHarinath, M V Ramana Murthy, B Chitra, "Cryptographic Methods and Performance Analysis of Data Encryption Algorithms In Network Security" International Journal Of Advanced Research In Computer Science And Software Engineering, Volume 5, Issue 7, July 2015.
[7] Manju Rani, Dr. Sudesh Kumar, "Analysis on Different Parameters of Encryption Algorithms for Information Security" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 8, August 2015
[8] O.O. Adekanmbi, O.O. Omitola, T.R. Oyedare, S.O. Olatinwo, "Performance Evaluation of Common Encryption Algorithms for Throughput and Energy Consumption of a Wireless System" Journal of Advancement in Engineering and Technology" Voume3 /Issue1, June 2015.