Cryptochat Encryption Messaging Application

Shubhankar Chaudhary[1], Shivam Dabas[2], Vishvjeet Singh [3], Mr. Sundeep Raj[4]

[1,2,3]*Student, Dept. of Information Technology, Inderprastha Engineering College, Uttar Pradesh, India*
[4] *Asst. Professor, Dept. of Information Technology, Inderprastha Engineering College, Uttar Pradesh, India*

---***---

Abstract - *RSA cryptosystem is the most ordinarily utilized open key cryptosystem. It is the main open key cryptosystem. The quality of this cryptosystem depends on the bigger key size. There are numerous calculations and variations of RSA. In this paper, the endeavor is to make a web application for secure transmission of messages starting with one client then onto the next. We utilized RSA calculation for encryption and decoding of the messages. The utilization of the RSA calculation has been done from the earliest starting point and is the base of a considerable lot of the cutting edge encryption calculations. We played out the transmission of the messages by the utilization of 1024 bits encryption.*

Key Words: **RSA, cryptosystem, secure, bits, encryption.**

1. INTRODUCTION

In this time of all inclusive electronic network, the electronic misrepresentation involves concern. There is to be sure need to store the data safely. This has prompted an elevated attention to shield information and assets from divulgence, to guarantee the validness of information and messages, and furthermore to shield frameworks from arrange based assaults. Cryptography is the study of encryption. Cryptography assumes a focal job in cell phone interchanges, electronic trade, sending or accepting private messages, exchange handling, giving security to ATM cards, making sure about PC from unapproved get to, computerized signature and furthermore addresses numerous parts of our day by day lives. Cryptography comprises of the considerable number of standards and strategies for changing a comprehensible message called plaintext into one that is muddled called figure content and afterward retransforming that message back to its unique Form. In current time, the cryptography is viewed as a part of both arithmetic and software engineering. It is additionally associated intimately with data and correspondence hypothesis. In spite of the fact that previously, the job of cryptography alluded uniquely to the encryption and unscrambling of message utilizing mystery keys. Be that as it may, these days, the cryptography is utilized in numerous zones; it is a result of the digitization. It is commonly arranged into two classifications, the symmetric and awry. The information moved starting with one framework then onto the next over open system can be secured by the strategy for encryption. On encryption the information is encoded or mixed by any encryption calculation utilizing the key. The client having the entrance to a similar key can decode the scrambled information. Such a cryptosystem is known as private key or symmetric key cryptography. There are numerous standard symmetric key calculations accessible. Some mainstream ones are as: AES propelled encryption standard, 3DES triple information encryption standard and so forth. All these standard symmetric calculations characterized are demonstrated to be exceptionally made sure about and dependable. The primary issue identified with these calculations is the key trade. All the imparting parties require a common mystery key. This key is required to trade between them to set up a made sure about correspondence. Thusly the security of the symmetric key calculation relies upon the security of the mystery key. The Key size is ordinarily many bits long. The key size likewise relies upon the calculation utilized. The key can't be shared on the web. Additionally when an enormous number of conveying parties are there, at that point all things considered the key trade is infeasible and troublesome as well. Every single such issue are countered by the open key cryptography. Out in the open key calculation a mutual mystery can be set up online between conveying parties with no requirement for trading any mystery information.

2. Literature Survey

The literature survey tells us about the previous study done on this topic. There has been many research on the cryptography topic.

There are different researches done where there has been modification done to the RSA algorithm, this model is based on the concept of the multiplicative homomorphism property which is OAEP. The OAEP is based on a trapdoor permutation. But the guaranteed level of security is not very high for a practical parameter choice. The authors proposed a very simple modification of the OAEP encryption in which the trapdoor permutation instance is only applied to a part of the OAEP transform. The security is tight in this updated version. OAEP can also be used to encrypt long messages without using hybrid encryption.

2.1 RSA algorithm with modified keys exchange:

Sami A. Nagar and Saad Alshamma speedup the RSA calculation through another age keys technique called RSA-Key Generations Offline to produce and spare all keys esteems in tables inside database. They proposed four security levels, in which each level has its own database and quantities of sets, these levels recognized by the e esteems and key length, before utilizing the RSA calculation between portals must prepare an Acknowledgment from RSA Handshake Database convention, this convention is answerable for creation or update the indistinguishable passages database, level determinations and foundation the calculation between doors. Nagar and Alshamma proposed another strategy for keys trade to build the trouble for any one knows the traded qualities among portals, and afterward attempt to get the n, e and d esteems, This methodology was known as Concept of Keys Exchange, where algo trades the records Nid, Eid, Did rather than n, e, d esteems.

2.2 Effect of the key size on the security:

In cryptography encryption key length plays an important role for security measures. Key length is equal to the number of bits in an encryption algorithm’s key. A short key length means poor security. However, a long key length does not necessarily mean good security. The key length determines the maximum number of combinations required to break an encryption algorithm.

If a key is n bits long, then there are two to the nth power (2^n) possible keys. For example, if the key is one bit long, and that one bit can either be a zero or a one, there are only two possible keys, 0 or 1. However, if the key length is 40 bits long, then there are 2^{40} possible keys. . A computer capable of trying a billion keys per second would take about 18 minutes to find the correct 40-bit key. A Data Encryption Standard (DES)-breaking computer called Deep Crack, which was capable of 90 billion keys per second, took 4.5 days to find a 56-bit DES key in 1999.

Whereas in our project we are using the RSA algorithm having a 1024 bits key for encryption and decryption which would be a lot harder to crack and will take a lot time.

The breaking of a 1024-bit key with a sizeable budget within months or a year. This is devasting because SSL certificates holding the public key last for 28 months. Fortunately, the complexity of the prime factorization problem grows exponentially with the key length.

Some advantages of RSA algorithm:

- Very fast and simple encryption and verification.
- Asymmetric process which uses both public and private key.
- Easier to implement than the Elliptical Curve cryptography (ECC).
- Better industry support.

3. Methodology

Basically, the proposed messaging/chat system is expected to provide a communication channel between clients via a server using encryption based on RSA in a Client/Server environment. The goal for this study is to use client/server architecture to accomplish secure chat between clients without the server being able to decrypt the message by using one layer of encryption between the clients and the server, and then a second layer of encryption between the clients in a chat room. All the used encryption processes based on RSA algorithm.

The very term customer server was at first applied to the product engineering, which depicted the circulation of the execution procedure by the standard of association of two programming forms, one of which in this model was known as the customer and the other the server. The customer procedure mentioned a few administrations, and the server procedure guaranteed their execution. It was expected that one server procedure can serve a ton of customer forms. One of the customer/server application is that "chatting". Chatting alludes to one kind of correspondence over the Internet that offers a continuous transmission of instant messages from sender to beneficiary or over a server that is control and deal with the gatherings (customers) to convey.

3.1 Client/Server:

The used client/server model describes how a server provides resources and services to one or more clients. Examples of servers including web servers, chat servers, and file servers. Each of these servers provide resources to client devices. Most servers have a one-to-many relationship with clients, meaning a single server can provide resources to m Computers. In order to meet the main requirements of businesses, networks themselves are becoming quite complex multiple clients at one time.

3.2 Chat Service:

A protected visit administration gives the capacity to have constant secure conversations among clients electronically, balanced or in bunches meeting .An open system aggregates data marginally, as opposed to on a client's individual PC that is utilized to stay in contact with individuals. A protected visiting among customer and server to make a sheltered and dependable correspondence, the benefits are:

· Allows for instant communications between users.

· Uses real time chat over the network that can eliminate costly long distance charges.

· Allows for rapid query and rapid responses.

3.3 Database Implementation:

Our project uses MySQL to manage the database, where user information and also the information about the keys of the users are stored and are linked to the application as when needed for the encryption or decryption process we can easily access the keys. This stores information in form of different tables.

3.4 Working of the RSA algorithm:

RSA involves two keys public key and private key. Public key is used for encryption and private key is used for decryption of message. The key generation takes places as follows:

STEP 1: Take any two large prime numbers P and Q.
STEP 2: Compute N by using the given formula

$$N= P * Q$$

STEP 3: Compute Eular's totient function Φ(N)

$$\Phi(N)= (P-1) * (Q-1)$$

STEP 4: Choose the public key exponent E such that
$1 < E < \Phi(N)$ and, E and Φ(N) are co-prime
Which means that GCD (E, Φ(N)) = 1
STEP 5: Determine private key exponent D through the given formula:
D *E= 1*mod (Φ(N))
This means that D is the multiplicative inverse of
E*mod ((Φ(N)).
Now, the public key consists of public key exponent E and N.
And private key consists of private key exponent D & N.
Public Key: (N, E) Private Key: (N, D)

Encryption:
For encrypting any message, the algorithm converts the given message into an integer number by using a suitable padding scheme. Then following formula is used to generate encrypted message C:

$$C = M \wedge E \bmod (N)$$

Decryption:
Following formula is used to decrypt the encrypted message:

$$M = C \wedge D \bmod (N)$$

3.5 Interface:

In this the user can register themselves by signing up or can login with the available user id and password. User can also search for the other participants available.

4. RESULT

The application is designed where we have main page having the option for logging in or signing up.

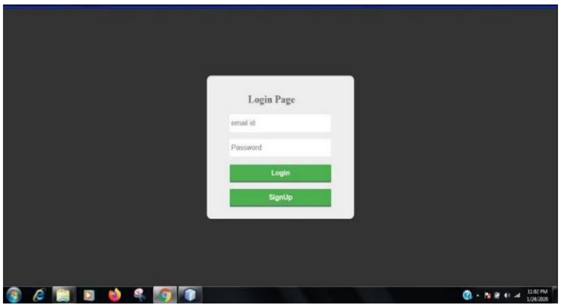
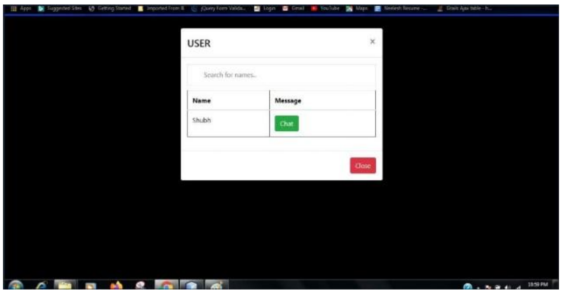


Figure 1: Login/Signup page

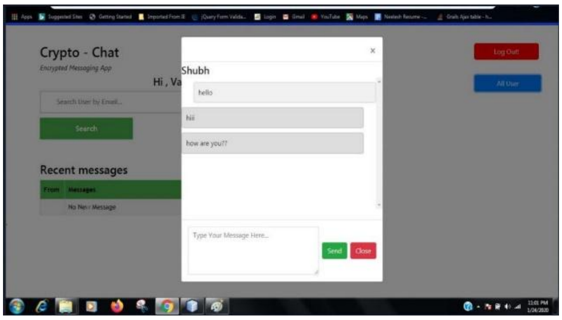
After logging in we can see we get notified about the messages received to us by some other user.



Name	Message
Shubh	Chat

Figure 2: Messages received

We can also search for other users and send messages to them through secure way.

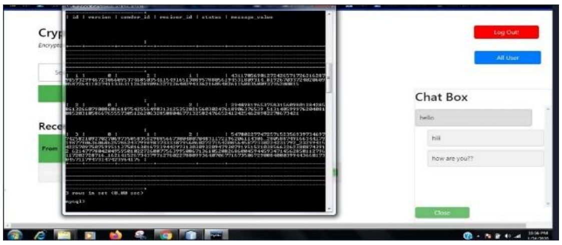


From	Messages
	No New Message

Shubh
hello
hii
how are you??

Figure 3: Exchanging messages one to another

MqSQL used to manage the database of the application stores the data of the user and information about their keys.



```
| id | version | sender_id | reciever_id | status | message_value
[illegible]
3 rows in set (0.00 sec)

mysql>
```

hello
hiii
how are you??

Figure 4: Storing of keys through MySQL

5. CONCLUSIONS

In this paper, the presentation and the use of cryptography is given. The issues identified with private keys are talked about. The open key cryptography and its utility in such a large number of regions of the life are talked about.

We additionally perceived how the size of the key influences the encryption and decoding process, which expresses that the more the size of the key the more better the security will be given.

We can say that for expanding the security of the message transmission we can utilize different calculations as well and even increment the key size that is 2048 bits RSA which when endeavored to break by a great PC would take around 300 trillion years.

There might be many algorithm or high end computers which would take comparatively less time to crack it but for a normal specs system and applying the brute force attack with one billion attempts per second the time taken would be approx.:

- 40-bit will be broken in about 9 minutes.
- 56-bit will be broken in about a year.
- 128-bit will be broken in about 5,783,128,169,837,158,197,871 years.
- 256-bit will never be broken, for all practical purposes.

So we can see using RSA algorithm with 1024 bits of key encryption for transmission of messages at a normal level would be more than sufficient.

ACKNOWLEDGEMENT

The authors would like to extend their esteemed thanks to Mr. Sundeep Raj, Asst. Professor, IT Department, IPEC. Special thanks to Dr. Pooja Tripathi, HOD, IT Department, IPEC.

REFERENCES

[1]. William Stallings, “Cryptography and Network Security”, ISBN 81-7758-011-6, Pearson Education, Third Edition.

[2]. Chouhan, K., Ravi, S. (2013). Public Key Encryption Techniques Provide Extreme Secure Chat Environment. International Journal of Scientific & Engineering Research,4(6), pp. 510-516.

[3]. Iwamoto, M., Omino, T., Komano, Y., Ohta, K. A new model of Client-Server Communications under information theoretic security. In Information Theory Workshop (ITW), pp. 511-515, 2014.

[4]. Nagar, S.A.; Alshamma, S., "High speed implementation of RSA algorithm with modified keys exchange," Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), 2012 6th International Conference on , vol., no., pp.639,642, 21-24 March 2012.

[5]. Alexandra Boldyreva, Hideki Imai, Life Fellow, IEEE,and Kazukuni Kobara, “How to Strengthen the Securityof RSA-OAEP”, IEEE TRANSACTIONS ONINFORMATION THEORY, VOL. 56, NO. 11,NOVEMBER 2010

[6]. Bidzos, Jim, "Threats to Privacy and Public Keys for Protection", COMPCON Spring '91 Digest of Papers, IEEE Computer Society Press, p. 189-94.

[7]. H. B. Pethe and S. R. Pande, "Comparative Study and Analysis of Cryptographic Algorithms," International Journal of Advance Research in Computer Science and Management Studies, vol. 5, no. 1, pp. 48-56, 1 January 2017.

[8]. Selby, A.; Mitchell, C., "Algorithms for software implementations of RSA," Computers and Digital Techniques, IEE Proceedings E , vol.136, no.3, pp.166,170, May 1989.

[9]. Desmet, L.,Johns, M.(2014). Real-time communications security on the web. IEEE Internet Computing, 18(6), pp.8-10.

[10]. Gupta, N., Saxena, A., Jain, N.(2016). Pairwise Independent Key Generation Algorithm: A Survey. International Journal of Computer Applications, 156(6),pp.12-18.

[11]. Jain, A., Kapoor, V.(2015). Secure Communication using RSA Algorithm for Network Environment. International Journal of Computer Applications, 118(7), pp.6-9.

[12]. Chaudhury, P.,Dhang, S., Roy, M., Deb, S., Saha, J., Mallik, A., Das, R. ACAFP: Asymmetric key based cryptographic algorithm using four prime numbers to secure message communication. A review on RSA algorithm. In Industrial Automation and Electromechanical Engineering Conference (IEMECON), 2017 8th Annual, pp. 332-337, 2017.