International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 6 June 2021, pp: 433-437 www.ijaem.net ISSN: 2395-5252

Secure Chatting Application using NTRU Asymmetric Cryptography Algorithm

Mrs. SapanaKolambe, Mrs. Dipali Patil, Mr. Kalyan Bamane
Department of Information Technology
D. Y. Patil College of Engineering Akurdi, Pune

Submitted: 25-05-2021 Revised: 01-06-2021 Accepted: 05-06-2021

ABSTRACT- Information security is thebest approach deliberated to keep data secure from unauthorized access. Nowadays, people feel more convenience usinga chat applicationon a smartphone to communicate with each other than calling or short messageservices (SMS) features. Major advantages of chat application are there are no limitations of message size, no limitations of the number ofconsumers to use it; especially text as well as any document can be sent easily.

In this paper, we implement a secure chatting application using asymmetric cryptography algorithms. The proposed system allows the users to communicate via text messages, voicemessages, and photos. The proposed system usedthe NTRU algorithm to generate the key pair and exchange to produce the shared key that will be used for theencryption of data. For the text message, the voice, andimages we used the NTRU security algorithm for encryption and decryption.In review, when it comes time to analyze the actual performance, we get the same security levels; NTRU has a good performance which is better than ECC and RSA.

Index Terms- NTRU, ECDH (Elliptic Curve Diffie Hellman Key Exchange), AES (Advanced Encryption Standard), Android, Chatting Application,RSA algorithm, encryption.

I. INTRODUCTION

Information technology is an important factor in human life that has provided comfort and ease in communicating. Most common used technology for communication is smartphones, which is a mobile phone with the ability of a portable computer. Currentlyto communicate with each other, people feel more convenience using chat application in a smartphone than calling other user or short messageservices (SMS) services. Some of the advantages of chat application are there is no limitation on message size, number of customers can use it; especially younger generation, and it also works on mobile web without application download.[3]. As it is very easy and more convenient for end users to communicate with smartphones, there are also new threats to communication data which is digital data that raise issues related to security in online data exchange. This security effort is carriedout with the aim of preserving the integrity and confidentiality which are important factors of any information that stored or transmitted by oneparty to another.

Cryptography is the algorithm which is used to maintain the security of the current data transmission in the communication channel. Cryptography is a field related to two main concepts in security includes Encryption and Decryption. These techniques are called cryptographic systems or ciphers. Encryption is a process of transforming a raw data or the original message, i.e. plaintext, into a coded message calledciphertext. Decryption is the inverse process of encryption that which converts the ciphertext (coded text)back to the plaintext. Researchers developed several algorithms related to this schemas which consists of Caesarcipher, RivestShamirAdleman (RSA), data encryption standard (DES), triple data encryption standard (3DES), ellipticcurve cryptography (ECC), and advanced encryption standard (AES) and NTRU(N-th degree Truncated polynomial Ring Unit). These algorithms help to improve the security ofa system with the objective of providing Complexity level for protection to maintain theintegrity and confidentiality of the data.

Public key is used in Asymmetric algorithm. Public and private keysare used in asymmetric cryptography where public key distributed publicly across the channel and private key used on the decryption side to convert the cipher text into plain text. Asymmetric algorithms are used to secure exchange of communication on the internet. RSA algorithm is used for encryption of asymmetric key for better and secure transaction on the internet. Asymmetric is the relatively slower than symmetric due to computations on cryptography of asymmetric key.

SSL is popular example where the asymmetric key is used for safe and secure

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 6 June 2021, pp: 433-437 www.ijaem.net ISSN: 2395-5252

communication on the internet. In this article, we propose that how to maintain authentication and confidentiality of information during transportation by implementing the RSA algorithm, where it will ensure confidentiality of information. RSA algorithm commonly used inasymmetric cryptography for encryption and decryption of information. Confidentiality is a term for protection of message from observer and authentication means that the receiver needs assurance as the Identify of the sender.

Nowadays, cryptographic algorithms such as ECC and RSA are the most common algorithms used forinformation security. The RSA algorithm was first introduced by RonRivest, AdiShamir, and LeonardAdlemanin 1978. However, to obtain the bestalgorithm in information security for communication purpose, Chandrasekaet al.4 [12] have compared the ECC and RSA algorithms based on thesize of encryption results at the same level of security. The comparison results show that the ECC has smaller sizesthan RSA algorithm.

NTRU (Nth degree Truncated polynomial Ring Unit)[13] is an open source and cryptography for encryption and decryption of text. At corresponding cryptographic strength, NTRU performs costly private key operations faster than RSA does. The time of performing an RSA private patented public-key cryptosystem which uses lattice-based operation increases as the cube of the key size, whereas that of an NTRU operation increases quadratic ally. In [14], authors compared NTRU algorithm with RSA and ECC algorithm on different parameters. Authors concluded that ECC has the best method in terms of key size and in terms of security level, RSA has small keys compared to NTRU, the greater the size of the RSA key provides higher levelof security and for actual performance analysis, we get the same security levels, NTRU has a good performance which is better than ECC and RSA. NTRU has very fast encryption and decryption method and it also provides high security.

II. IDENTIFY, RESEARCH AND COLLECT IDEA

In this paper [7], authors proposed a study of different algorithm of symmetric algorithm such as DES, 3DES, AES, Blowfish and Asymmetric algorithm such RSA, Diffie Hellman. Security is an important part in any communication. By using cryptography, it is possible to secure data over communication channel by encrypting data at sender side and decrypted at receiver side. In this paper [7], they provided comparison study between is based on different parameter includes Key used, throughput, Encryption ratio, Power consumption, key length, speed, security against attack.

In this paper [8], authors proposed system for authentication and confidentiality of information during transportation using RSA Algorithm for encryption and description purpose. The main focus is on the key length. The long length of the keys takes huge time but it provides more security. They have analyzed that when we increase the key size in RSA algorithm than key generation time increase respectively.

RSA encryption algorithm [10] which is based on the idea of ensuring the secure transfer of data in the digital environment and the algorithmic difficulty of separating the integer factorization is a type of public-key encryption method. In this paper [10], they proposed RSA encryption algorithm and the secure messaging process on the SMS channel are realized in the devices with the Android operating system.This application is tested for different key sizes for fast and powerful messaging. Key size with 512 bit size can be selected for communication purpose by allocating messages into blocks.

In this paper [9], authors proposed client/server architecture to develop a secure messaging and chat between clients in which server is not able to decrypt the message by applying two layer security: one layer of encryption between the clients and the server, and the second layer of encryption between the clients in the chat room RSA is used for digital messaging transactions such as e-mail over the Internet, to encode and decode messages in a terminal window is developed. In this paper [11], they proposed a system like SMS messenger, implemented an application that enables you to text or send small images without charge. RSA algorithm is used for encryption and decryption process. Every message byte contains 140 bytes of effective data. Message byte defines upper bound of an SMS message to be 160 characters using 7-bit encoding.

In this paper[2], they have designed application software to implement RSA and RC4 algorithms on different file sizes. The factor that isconsidered for measuring the performance of the algorithms is the speed of execution.Time of execution (TE)is a parameter for the evaluation for speed. Authors concluded that between RC4 is better compare to RSA. RSA is the most secure algorithm. However, the RC4 seems to be faster in encryption and decryption process but rather less secure.

Elliptical curve cryptography (ECC)[3] is a trending and commonly used cryptography scheme that currently many researchers experiment

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 6 June 2021, pp: 433-437 www.ijaem.net ISSN: 2395-5252

about. The key size and security level are important factor of ECC algorithm which motivates many researchers to learn and explore about this schemes to know its strength and limit. The ECC is appropriatemethod for mobile devices because it has relatively small key size compared to other cryptography algorithms such as RSA and Diffie Hellman. In this paper[3], they have implemented ECC algorithm to secure text message in messaging application on android smartphone. They have provided experimental result of chat application performance such as the accuracy of the received text message, average encryption and decryption time.

In this paper[1], they have proposed a secure chatting application for smart phones that used the android Operating system. The proposed secure chatting application used the Elliptic Curve Diffie Hellman Key Exchange (ECDH) algorithm to generate the key pair and exchange that keys pair which produce the shared key that will be used for the encryption of data for symmetric algorithms. The authors proposed an Application allows the users to communicate with each other via text messages, voice messages and photos. For Security of text messages, the standard AES algorithm with a 128 bits key is used. The generated key which is of 160 bit length minimized to 128 bit length by selecting the first 128 bit of the generated key which is requirement of AES algorithm. For the voice and image security, the application used the symmetric algorithm RC4 for this purpose.

In this paper [13], proposed an android application for providing a security-focused institutionalized chat and document sharing platform. They have used Openfire, an instant messaging and group-chat server that use XMPP. Authors used NTRU and AES algorithm to implement security.In this paper [14], authors reviewed the RSA, Elliptic curve and NTRU algorithms that are used in encryption technology which is used for protecting information security such asdigitalsignatures, authentication, system security, confidentiality and data integrity. Comparison is done on different parameters key size, encryption generation, complexity, security of algorithm, mathematical problem and execution time.

III. NTRU ALGORITHM

NTRU is cryptography system that does not rely on operators or separate logarithmic problems. NTRU - N-polynomial ring units ($R = Z [X] / X^{N-1}$),

- Operations of NTRU Algorithm:

Its base objects on the polynomial ring are truncated $R=Z[X]/(X^{N-1})$, and the polynomial is N-1: $a^0 + a^1x + a^2x^2 + \ldots\ldots + a^{N-1}x^{N-1}$,

NTRU includes three steps: generation of key, encryption for NTRU and decryption for NTRU.

a. Generation of Key:

I. Randomly, user B selects polynomials l and f in R (polynomial).
a. Polynomial values must be kept secret.
b. There must be a polynomial chosen inverse.
II. An inverse will be calculated for both l modulo p and l modulo q: $l * l^{-1} q = 1$ (modulo q) and l * lp-1 = 1 (modulo p).
III. The polynomial product will be calculated: $n = p * ((l^{-1} q) * l) \bmod q$, Private Key B will be: (l and lp) and public key B:polynomial n.

b. Encryption for NTRU:

The sender A wishes to send a message will follow the following:

I. Sets the message in a polynomial form whose coefficients are selected coefficient that will be -p / 2 and p / 2 (central lift).
II. Randomly selects another polynomial is small p (to hide the message).
III. Message encoding: e = r * n + m (modulo q).

c. Decryption for NTRU Algorithm:

B receives the message e from A for decryption.

I. Using its polynomial counterpart l calculates the polynomial a = l * e (mod q). B needs to select the coefficients of length qwhich are considered as longitudinal separation for decoding.
II. Polynomial is calculated as b = a (mod p). B reduces both coefficient coefficients p.
III. B uses lp which is polynomial to compute the other c = l-1p * b (modulo p), which represents the original message of A.

- Benefits of NTRU

➢ The algorithm is more effective in coding and decrypting applications in both hardware and software.
➢ The process of creating a key is much faster than allowing the use of keys (because the account can be created because of keylicenses).
➢ Used in mobile devices and smart card for the advantage of low memory usage.

IV. THE PROPOSED APPLICATIONMODEL

The system is android application that enables users tocommunicate with each other in a safe way and providesthem with end to end

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 6 June 2021, pp: 433-437 www.ijaem.net ISSN: 2395-5252

security communication. Thiscommunication process is done through data encryption process andsubmitted to the internet server in an encrypted format andthen retrieved by certain queries and decrypted, then shownto the recipient user. The application consists of a set of interfaces design, which enables the user to perform the chatprocess with the rest of the users.

Fig. 1 Proposed System Diagram

Theprocedure in which the text, voice and image exchanged is illustrated in following algorithms:

Algorithm 1: Text message security model

1. The sender type Text Message (M)
2. Text Message converted to polynomial (P)
3. Encrypt the polynomial (Enc E): performed by NTRU withthe generated secure key
4. The recipient receive the encrypted message E
5. Decrypt the message E
6. Convert the received E to polynomial
7. Compute the Polynomial to other C which represent original message M.

Algorithm 2: Voice message security model

1. The sender record Voice Message (VM)
2. The VM converted to polynomial(P)
3. Encrypt the converted P (Enc E): performed by NTRU with the generated secure key
4. Store the Enc E to Audio File (AF)
5. Send the Audio file to the server
6. The recipient receive the Audio file
7. Extract the Enc E from the received Audio file
8. Decrypt the extracted message E
9. Parse the message E to File Output Stream (FOS)
10. Parse the FOS to the any Media Player (MP)
11. The recipient now able to play the voice message which is same as original.

Algorithm 3: Image message security model

1. The sender upload an image to be sent (IME)
2. The IME converted to Bitmap (BI)
3. Convert the BI to polynomial (P)
4. Encrypt the converted P (Enc E): performed by NTRU algorithm with the generated secure key
5. Store the Enc E to Image File (IF)
6. Then IF send to the server
7. The recipient receive the IF
8. Extract the Polynomial P from the received IF
9. Decrypt the extracted P .
10. Convert the P to bitmap to be shown to the recipient as image.

CONCLUSION

In this paper, a secure chatting application using asymmetric algorithm was developed. Expected outcomes improve speed and accuracy of chatting application. The proposed secure chatting application furnishes confidentiality, privacy and integrity. Users can be granted that even the provider of the service, cannot read their messages. The exchanged data is store at the server, and nothing of them is stored at the physical memory of the phone. For achieving end to end encryption, NTRU key exchange provides the key pair, which will be exchanged between the two parties to generate the secure shared key that will be used as a key for the encryption algorithms. The algorithm used for encryption and decryption text messages, voice and image messages we used NTRU algorithm techniques which is one of the fastest encryption/decryption algorithm.NTRU is a relatively good coding system. NTRU has a good performance which is better than ECC and RSA.

REFERENCES

[1] Ammar Hammad Ali, Ali Makki Sagheer, “Design of Secure Chatting Application with End to End Encryption for Android Platform,” in Iraqi Journal for Computers and Informatic, Vol.[43] Issue[1],2017.

[2] “RSA and RC4 Cryptosystem Performance Evaluation Using Image and Text File”, Akinyele A. Okedola, Yekini N. Asafe, International Journal of Scientific & Engineering Research, Volume 6, Issue 5, May-2015.

[3] Dimas Natanaela, Faisala, Dewi Suryanib,” Text Encryption in Android Chat Applications using Elliptical CurveCryptography”, International Conference on Computer Science and Computational Intelligence,Procedia Computer Science 135 (2018) 283–291.

[4] “A Secure Electronic Messaging System in Client Server Cryptography-RSA Algorithm”, G. Geeta Sai Sruthi, M. Raghupathi,International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8, Issue-6S3, September 2019.

[5] "Review on SMS Encryption of Android Mobile by Using Cryptography Algorithm",Zainab Khyioon Abdalrdha, Farah Neamah Abbas & Iman Hussein AL-Qinani,International Journal of Engineering Research and Advanced Technology (IJERAT), E-ISSN : 2454-6135 ,Volume.5, Issue 10 October -2019.

[6] Sujithra M, Padmavathi G, Sathya Narayanan, "Mobile Device Data Security: A Cryptographic Approach by Outsourcing Mobile data to Cloud", Procedia Computer Science 47 (2015) 480 – 485.

[7] Muhammad Aamir Panhwar, Sijjad Ali khuhro,Ghazala Panhwar, Kamran Ali memon: "SACA: A Study of Symmetric and Asymmetric Cryptographic Algorithms" in IJCSNS International Journal of Computer Science and Network Security, VOL.19 No.1,January2019.

[8] Abdul Ghaffar Khan, Sana Basharat, Muhammad Usama Riaz: "Analysis of asymmetric cryptography in information security based on computational study to ensure confidentiality during information exchange" in International Journal of Scientific & Engineering Research Volume 9, Issue 10, October-2018.

[9] Ferdi SÖNMEZ, Jalal Sadoon Hameed Al-Bayati, "Development Of A Client / Server Cryptography-Based Secure Messaging System Using RSA Algorithm " in Journal of Management Engineering and Information Technology (JMEIT) Volume - 4, Issue- 6, Dec. 2017, ISSN: 2394 – 8124

[10] Hüseyin Bodurand1Resul Kara, "Secure SMS Encryption Using RSA Encryption Algorithm on Android Message Application: in H. BODURet al./ ISITES2015Valencia-Spain.

[11] Zarni Sann, Thi Thi Soe andMoe Moe San, "Secure SMS System using RSA Encryption Based on Android platform" in International Journal of Advances in Scientific Research and Engineering (ijasre) Volume 6, Issue 4April -2020.

[12] A. Chandrasekar, V.R. Rajasekar & V. Vasudevan, "Improved Authentication and Key Agreement Protocol Using Elliptic Curve Cryptography" in International Journal of Computer Science and Security (IJCSS), Volume (3): Issue (4)2015.

[13] Abhishek Chaudhary, Abdullah Khan, Kishan Singh, Rahul Pandey, "NTRU Encrypted Android Chat Application using Openfire" in IJSRD -International Journal for Scientific Research& Development| Vol. 7, Issue 02, 2019.

[14] Ahmed Othman Khalaf ,Shaimaa Khudhair Salah, Hind Jumaa Sartep, and Zainab Khyioon Abdalrdha, "Subject Review: Comparison betweenRSA,ECC & NTRU Algorithms" in International Journal of Engineering Research andAdvanced Technology (IJERAT) volume 5, issue 11 November 2019.

[15] Muhammed Kuliya1, Hassan Abubakar "Secured Chatting System Using Cryptography", in nternational Journal of Creative Research Thoughts (IJCRT) Volume8,Issue9September2020.