Comparative Study of Speech Encryption Algorithms Using Mobile Applications

Jaspreet kaur[#1] , Er. Kanwal preet Singh[*2]

1M tech. Student, University College of engineering, Punjabi university Patiala. Punjab, India,

2Department *of Computer Engineering, Assistant Professor of University College of engineering, Punjabi university Patiala, Punjab, India,*

Abstract Speech communication is most popular now days. Everyone wants secure communication that's way use encrypts and decrypt data scheme. It is basically used for military and business purpose. People want high security level during their communication..The numbers of algorithms are used for speech encryption and decryption. However in this paper the work is done on three different kinds of algorithms i.e. NTRU, RSA and RINJDAEL these three popular algorithms are used for speech encryption and decryption approach. Basically NTRU and RSA algorithms are asymmetric in nature and RINJDAEL algorithm is symmetric in nature. In speech encryption, first the speech is converted into text then further the text is converted into cipher text. The cipher text is sent to be particular receiver in which transmitter want to communicate. At the receiver end, receiver receives the original data through decryption process. At the end the performance is analyzed of these three approaches respectively. The parameters calculated are Encryption, Decryption and Delay time, complexity, and packet lost, Security level. In this three approaches, Encryption, decryption and delay time, are varying according to the number of bits per seconds. On the Other hand, complexity and packet lost are approximately same. There is no packet lost during transmitting and receiving the data. After the analysis of these three algorithms, The NTRU algorithm is faster in encryption and decryption time than others algorithms. The security level are very high than other algorithms. The android platform are used for these three algorithm to find the results in which algorithm took less time for encrypt or decrypt the data and help to evaluate the performance in speech encryption algorithms.

Keywords: - NTRU, RSA and RINJDAEL algorithms, Speech cryptography.

1. Introduction

Speech is the ability to speak or the act of speaking. One can express their feelings and views by speech sounds and gesture. Speech is the continuous streaming data. Speech signal consists of number of bits .It contains both negative and positive bit values. Although speech signal is defined as a specific kind of audio signal But it process different properties then conventional audio signal. Speech is a narrow band signal and audio has a broader band signal. Speech signal is represented in two forms: analogue and digital form. In analogue representation, it is represented in wave form which represents the frequency and amplitude of the signal. It also represents the variation in amplitude and frequency with respect to time. Digital representation is the numeric representation of analogue form. In this, signal is represented in the form of zeros and ones.

In our approach , encrypt the speech using three encryption algorithms mainly RSA,NTRU and RIJENDAEL ..In this approach convert speech into text and then into cipher text. The resulting system can securely encrypt the speech files for the purpose of storing speech messages and transmitting them over the Internet. The resulting system has many advantages. The main advantage of system is that the performance of which technique is higher. Our system is systematically evaluated, and it shows a high level of security. This paper is organized as follows. Section 2 explains the encryption process, Section3 gives the result and discussion, section 4 gives the conclusion and section 5 gives a future scope.

2. Present work

1. The methodology of the work will require the three basic encryption algorithms approach to encrypt the speech into text and then into cipher text.

2. NTRU, RIJENDAEL and RSA algorithms will be implemented on speech then these algorithms will perform their encryption and convert the speech into text and then into cipher text, Hence speech will be encrypted.

3. Use Android platform to implement these three algorithms.

4. Calculated and analyzed these parameters which are described as follows:

- Encryption time.
- Decryption time.
- Complexity.

- Packet lost.
- Delay time.
- Security level

5. At last, the comparison of these three algorithms which was implemented in Android platform.

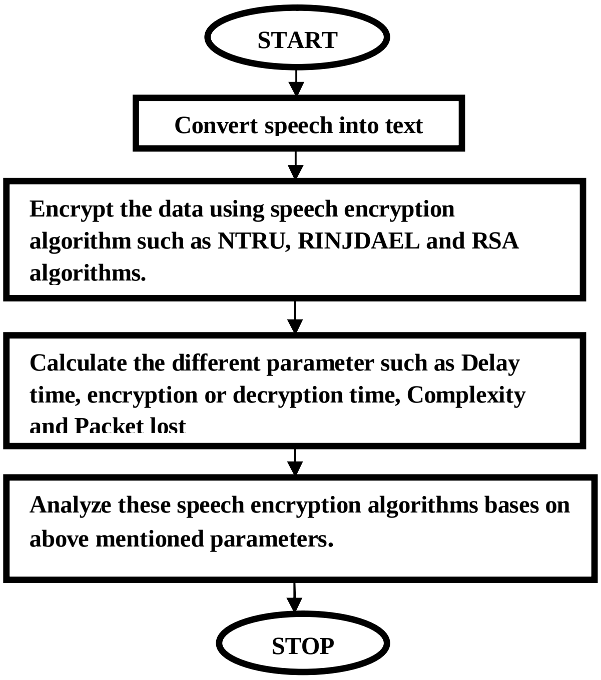
START
Convert speech into text
Encrypt the data using speech encryption algorithm such as NTRU, RINJDAEL and RSA algorithms.
Calculate the different parameter such as Delay time, encryption or decryption time, Complexity and Packet lost
Analyze these speech encryption algorithms bases on above mentioned parameters.
STOP

Figure1. Flow chart of work methodology

2.1 NTRU algorithm

NTRU cryptosystem is a relatively new Public Key Cryptosystem. Public Key Cryptography or Asymmetric Cryptography is used in areas of digital signatures and key exchange. RSA is an acclaimed Public Key cryptosystem that is in use since 1977. However, it is very slow in comparison with Symmetric Cryptography systems in processing bulk data encryption and decryption. In contrast, NTRU runs much faster on large data systems than RSA and has become a very popular algorithm today in terms of data encryption and decryption. The key generation process in NTRU is much faster than that in RSA, and this process is one of the most important processes in Public Key Cryptography. The NTRU algorithm involves three steps: key generation, encryption and decryption.

- **Key generation**

NTRU involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the NTRU algorithm are generated the following way:

1. Choose two distinct prime numbers p and q.
For security purposes, the integers p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primality test.
2. Compute $n = pq$.
3. Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1)$, where φ is Euler's totient function.
4. Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e. e and $\varphi(n)$ are coprime.
5. e is released as the public key exponent.e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $2^{16} + 1 = 65{,}537$. However, much smaller values of e (such as 3) have been shown to be less secure in some settings.
6. Determine d as $d^{-1} \equiv e \pmod{\varphi(n)}$, i.e., d is the multiplicative inverse of e (modulo $\varphi(n)$).

   - This is more clearly stated as solve for d given $de \equiv 1 \pmod{\varphi(n)}$
   - This is often computed using the extended Euclidean algorithm .d is kept as the private key exponent.

By construction, $d{\cdot}e \equiv 1 \pmod{\varphi(n)}$. The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and $\varphi(n)$ must also be kept secret because they can be used to calculate d.

Encryption

Alice, who wants to send a secret message to Bob, puts her message in the form of M. In modern applications of the encryption, the message can be translated in a binary or ternary representation. With Bob's public key e the encrypted message E (M) is compute d (M) = M^e mod n Where E(M) is the encrypted message, M is plaintext and e is receiver's public key used for encryption.

Decryption

M = D (E $(M)^d$ mod n) Where M is plaintext after decryption, E (M) is the encrypted message, d is private key of receiver and D denotes the decryption process.

NTRU PERFORMANCE

Table 1 Calculation of parameters in different text size using NTRU algorithm

S.no	Test Size	Encryption time	Delay Time	Decryption Time
M1	40 bits	5 ms	1 ms	11 ms
M2	64 bits	9 ms	3 ms	7 ms
M3	136 bits	6 ms	4 ms	10 ms
M4	200 bits	13 ms	4 ms	14 ms
M5	128 bits	12 ms	5 ms	13 ms

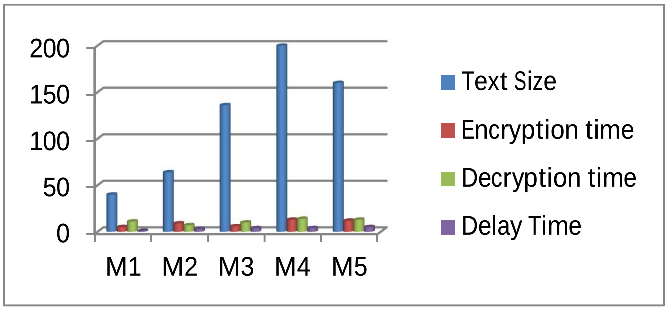

Fig 2. Parameters analysis in NTRU algorithm

2.2 RIJNDAEL Algorithm

In the 1990s, the US Government wanted to standardize a cryptographic algorithm, which was to be used universally by them. It was to be called Rijndael was accepted. Rijndael was developed by Joan Daeman and Vincent Rijmen. I was to be based on 128-bit blocks with 128-bits keys.Rijndael supports key length and plain text block size from 128 bits to 256 bits, in the step of 32 bits. The key length and the length of the plain texts blocks need to be selected independently.

Operation

The basics of Rijndael are in a mathematical concept called as a Galois field theory. Similarly to the way DES function, Rijndael also uses the basic techniques of substitution and transposition. The key size and plain text block size decide how many rounds need to be executed. The minimum numbers of round is 10 and maximum number of rounds is 14. One key differentiator between DES and Rijndael is that all the Rijndael operation involves entire byte and not individual bits of a byte. This provides for many optimized hardware and software implementation of the algorithm.

(i) Do the following one-time initialization process:
  (a) Expand the 16-byte key to get the actual key block to be used
  (b) Do one time initialization of the 16-byte plain text block.
  (c) XOR the state with the key block.
(ii) For each round, do the following:
  (a) Apply S-box to each of the plain text bytes
  (b) Rotate row k of the plain text block by k bytes
  (c) Perform a mix columns operation
  (d) XOR the state with the key block

Fig 3.Description of RIJNDAEL

One-time Initialization Process

a) Expand the 16-byte key to get the actual key block to be used The input to the algorithm are the key and the plain text, as usual. The key size is 16 bytes in this case. This Step expands this 16-bytes key into 11 arrays; each array contains 4 rows and 4 columns.
b) Do One Time Initializations of the 16-bytes Plain text Blocks This step is relatively simple. Here, the 16-byte plain text block is copied into a two-dimensional 4*4 array called as state.
c) XOR the State with the key block first 16 bytes of the expanded key are XORed into the 16- byte state array. Process in each round

The following steps are executed 10 times, one per round

- Apply S-box to each of the plain text bytes. This step is very straightforward. The contents of the state array are looked up into the S-box. Byte by Byte substitution is done to replace the contents of the state array with the respective entries in the S-box.
- Rotate Row k of the plain text block by k bytes. Each of the 4 rows of the state array is rotated to the left. This helps in diffusion of data. Thus, if the original 16 bytes of the state contain values 1, 2, 3, 4,…….,16 then the rotate operation would change.
- Perform a mix columns operation each column is mixed independent of the other. Matrix multiplication is used. The output of this step is the matrix multiplication of the old values and a constant values.XOR the state with the key block this step XORs the key for this round into the state array. For decryption, the process can be executed in the reverse order.

RIJENDAEL PERFORMANCE

Table2. Calculation of parameters in different text size using RIJENDAEL algorithm

S.no	Test Size	Encryption time	Delay time	Decryption Time
M1	40bits	99ms	1 ms	83 ms
M2	64bits	112ms	2 ms	87 ms

M3	136bits	91ms	6 ms	82 ms
M4	200bits	87ms	1 ms	81 ms
M5	128bits	91ms	2 ms	84 ms

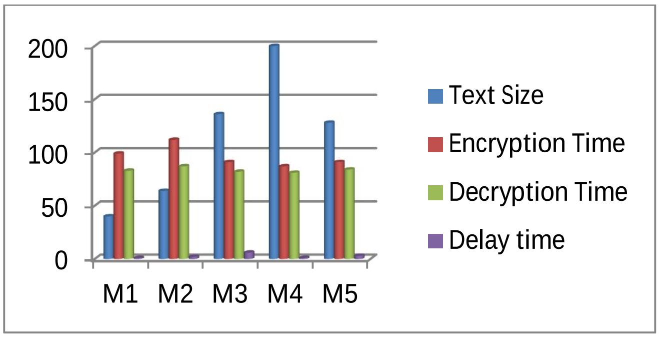

Figure 4. Parameter analyses in RINJDAEL algorithm

2.3 RSA Algorithm

RSA is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Microsoft and Netscape. Briefly, the algorithm involves multiplying two large prime numbers. Once the keys have been developed, the original prime numbers are no longer important and can be discarded. Both the public and the private keys are needed for encryption /decryption but only the owner of a private key ever needs to know it. Using the RSA system, the private key never needs to be sent across the Internet. The private key is used to decrypt text that has been encrypted with the public key.

Operation

The RSA algorithm involves three steps: key generation, encryption and decryption.

Key generation

RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q.
2. Compute $n = pq$.
3. Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1)$, where φ is Euler's totient function.
4. Choose an integer e such that $1 < e < \varphi(n)$ and gcd $(e, \varphi(n)) = 1$; i.e. e and $\varphi(n)$ are co-prime.
5. Select the private key (i.e. decryption key) d such that the following equation is true:(d * e) mod $\varphi(n)$ = 1 d is kept as the private key exponent.

By construction, $d \cdot e \equiv 1 \pmod{\varphi(n)}$. The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and $\varphi(n)$ must also be kept secret because they can be used to calculate d.

Encryption

Alice transmits her public key (n, e) to Bob and keeps the private key secret. Bob then wishes to send message M to Alice.

$c = m^e$ (mod n) This can be done quickly using the method of exponentiation by squaring. Bob then transmits c to Alice.

Decryption

Alice can recover m from c by using her private key exponent d via computing $m = c^d$ (mod n)

RSA Performance

Table 3.Calculation of parameters in different text size using RSA algorithm

S.NO	Test Size	Encryption time	Delay Time	Decryption Time
M1	40 bits	58 ms	1 ms	54 ms
M2	64 bits	53 ms	1 ms	53 ms
M3	136 bits	54 ms	3 ms	62 ms
M4	200 bits	57 ms	4 ms	64 ms
M5	128 bits	64 ms	4 ms	69 ms

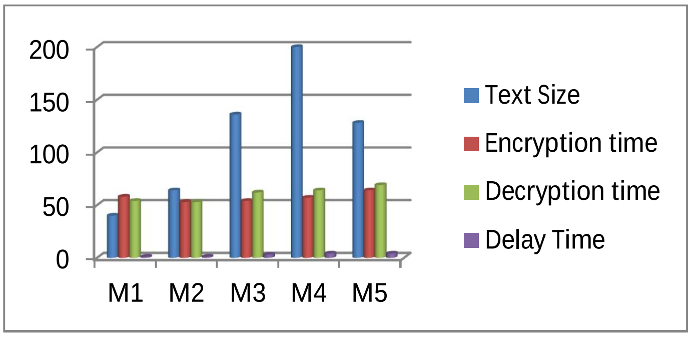

Fig 5 . Parameter in RSA algorithm

3. Result and Discussion

The result are analyzed and discussed, different speech are analyzed in different algorithm and complexities, and security level have been discussed and simulated.

The result based on graphs and tabulated value of each speech encryption algorithms according to the scenario wise observation are given below:

b) The NTRU and RSA are asymmetric approach on the other hand RINJDAEL has symmetric approach.

c) The packet lost is 0% in three of three algorithms.

d) The security level is high in NTRU algorithm than other two algorithms.

Table 4 . Comparison of Speech encryption algorithms

S. No.	**Method**	**NTRU**	**RINJDEAL**	**RSA**
1	Approach	Asymmetric	Symmetric	Asymmetric
2	Encryption	Faster	Low	Moderate
3	Decryption	Faster	Low	Moderate
4	Complexity	Moderate	High	Low
5	Security level	High	Moderate	Low
6	Packet lost	No	No	No

4. Conclusion

Now-a-days speech communication is more popular for different applications in our daily real life. Errorless data transmission with security is important in wireless environment. In this paper discussed about cryptography, speech cryptography, encryption or decryption of data, types of programming platforms for mobile phones and NTRU cryptosystems. From the above mentioned last 3 tables, concluded that NTRU cryptosystem is faster and providing stronger security level than other traditional cryptosystems. NTRU provided better result so it will improve the current security level, fastest speed and provide reliable message at receiver end with respect to key generation, encryption and decryption with small key size.

5 Future Work

In the area of security, research area of speech security is very wide. Speech security is required in military, banking and radio or satellite communication. Android is now days very power OS booming in market, it will replace over 65% of smart phones. More future studies and research will be done on this. Our work involves various technologies like network security which is been implemented in Android OS smart phones. RSA, RINJDAEL, and NTRU algorithms are studied and implemented on speech encryption. The future scope of our work

- To Secure Voipe Calling.
- Voice Mail Encryption.
- To Secure Voice Chat.

a) The encryption and decryption of NTRU algorithm are faster than other algorithms.

References

[1] "*SpeechSignal*"Onlineavailableatwww.cs.haifa.ac.il/~nimrod/Compression/Speech/S1Basics2010.pdf

[2] A. Jameel et al, *"A robust secure speech communication system using ITU-T G.723.1 and TMS320C6711 DSP"*, Microprocessors and Microsystems, volume 30,2006,Pages 26-32.

[3] A. Jameel, *"Transform-domain and DSP based secure speech communication"*, Microprocessors and Microsystems, 2007, 335–346.

[4] Akella Amarendra Babu et al *"Robust speech processing in EW environment"*, International Journal of Computer Applications (0975 – 8887) Volume 38– No.11, January 2012

[5] Venkatesh Krishnan *"A Framework For Low Bit-Rate Speech Coding In Noisy Environment"*, A school of Electrical and Computer Engineering

[6] Ashok Kumar Nanda, Prof. Lalit Kumar Awasthi **"***SMS Security Using NTRU Cryptosystem for M-Commerce***"**,May 2012

[7] Raj Kumar G.V.S. Naveen Kumar K, Chandra Sekhar P, Bhargav Nunna V. V. S., Vinod Kumar B**"***Modified Mutual Authentication and Keyagreement Protocol based on Ntrucryptography for wireless communications***"**, International Journal of Computer Science and Network (IJCSN)Volume 1, Issue 4, August 2012.

[8] P.Saveetha & S.Arumugam**,** **"***Study on Improvement in RSA Algorithm and its Implementation***"**, International Journal of Computer & Communication Technology ISSN (PRINT): 0975 - 7449, Volume-3, Issue-6, 7, 8, 2012.

[9] Xin Zhou, Xiaofei Tang, *"Research and implementation of RSA algorithm for encryption and decryption"* IEEE 24 August 2011.

[10] Challa Narasimham, Jayaram Pradhan **"***Evaluation of Performance Characteristics of Cryptosystem using Text files"*, Journal of Theoretical and Applied Information Technology, May 2008

[11] L.Thulasimani, M.Madheswaran *"Design And Implementation of Reconfigurable Rijndael Encryption algorithms For Reconfigurable Mobile Terminals"*, in 2010.

[12] Harsh Kumar Verma, Ravindra Kumar Singh " *Performance Analysis of RC6, Twofish and Rijndael Block Cipher Algorithms* " , in 2012.

[13] Artan Berisha , Behar Baxhaku , Artan Alidema " *Performance Analysis of RC6, Twofish and Rijndael Block Cipher Algorithms"*, in September 2012.

[14] D.Ambika, V.Radha " *Secure Speech Communication – A Review"* ,in 2012.

[15] Rashmi Jha, Anil Kumar saini *"A Comparative Analysis & Enhancement of NTRU Algorithm for Network Security andPerformance Improvement"*, International Conference on Communication Systems and Network Technologies,2011.

[16] Mircea Frunza, Luminita Scripcari " *Improved RSA Encryption Algorithmfor Increased Security of Wireless Networks"* ,IEEE ,2007.

[17] Sattar J Aboud " *An Efficient Method for Attack RSA Scheme*",IEEE,2009.

[18]Abdullah Al Hasib and Abul Ahsan Md. Mahmudul haque *"A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography"*,IEEE ,2008.