INTERNATIONAL JOURNAL OF
INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211 (Online)

Speech To Text Encryption Using Cryptography Techniques

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

Er. Kanwal preet Singh
Department of Computer Engineering, Assistant Professor of University College of engineering, Punjabi university Patiala, Punjab, India

Abstract:

The number of techniques are used for speech encryption. However in our approach the work is done on different kind of techniques i.e. MD-5 , SHA-2 and Rinjdael these three popular techniques are used for text encryption. In this work of thesis the speech is first converted into text then further the text is converted into cipher text. At the end the performance is analyzed of these three approaches respectively. The parameters calculated are Encryption and Delay time, Throughput no of bits per second, complexity, packet lost, Delay time, Security level.

Key words: *Cryptography, MD5, SHA-2, Rijndael*

1.Introduction

A speech communications become more and more widely used and even more vulnerable, the importance of providing a high level of security is dramatically increasing. Does increased security provide comfort to paranoid people? Or does security provide some very basic protections that we are naive to believe that we don't need? During this time when the Internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce, security becomes a tremendously important issue to deal with. There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of cryptography. But it is important to note that while cryptography is necessary for secure communications, it is not by itself sufficient. Cryptography is the science of writing in secret code and is an ancient art; Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any entrusted medium, which includes just about any network, particularly the Internet.Within the context of any application-to-application communication,There are some specific security requirements, including:

- Authentication: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.
- Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
- Non-repudiation: A mechanism to prove that the sender really sent this message.

Cryptography then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below.

In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into cipher text, which will in turn (usually) be decrypted into usable plaintext.

2.Speech Encryption

Encryption is a much stronger method of protecting speech communications than any form of scrambling. Voice encryption work by digitizing the conversation at the telephone and applying a cryptographic technique to the resulting bit-stream. In order to decrypt the speech, the correct decryption method and key must be used.

- Software Based Encryption System: Soft encryption systems are exactly what they sound like, software based encryption. While the inconvenience of having to use a computer is the primary drawback to soft voice encryption, most of the available programs use good crypto and are free.

  There are several ways of classifying cryptographic algorithms. They will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three types of algorithms that will be discussed are

- Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption
- Public Key Cryptography (PKC): Uses one key for encryption and another for decryption
- Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information

2.1.MD5 Algorithm

MD5 or message digest 5 is an encryption algorithm widely used for password comparisons. Basically MD5 is a hashing algorithm which takes a message of any length as input and produces a 128 bit or 32 hexadecimal digit digest as output. Even a very small variation in the input string like one character can produce significant change in the output MD5 encrypted hash.

MD5 is a one way algorithm. That means a reverse algorithm of MD5 cannot decode the message digest back to its original message. MD5 is a very popular and widely used form of encryption with a 128 bit hash function. This is a great way to encrypt passwords that you would use on search forums and any other data that needs encrypting. By making your data unreadable you gain an extra level of security which is why MD5 is so popular with web designers and developers. MD5 can be encrypted but it cannot be unencrypted which is very useful if you want to check whether your data has been tampered with in any way. The intention of MD5 was to be able to encrypt and check the integrity of files.

3.Rijndael Algorithm

Rijndael is a substitution linear transformation cipher, not requiring a Feistel network. It uses triple discreet invertible uniform transformations (layers). Specifically, these are: Linear Mix transform; Non-linear Transform and Key Addition Transform. Even before the first round, a simple key addition layer is performed, which adds to security. Thereafter, there are Nr-1 rounds and then the final round. The transformations form a State when started but before completion of the entire process. The State can be thought of as an array, structured with 4 rows and the column number being he block length divided by bit length (for example, divided by32). The cipher key similarly is an array with 4 rows, but the key length divided by 32 to give the number of columns. The blocks can be interpreted as uni dimensional arrays of 4-byte vectors. The exact transformations occur as follows: the byte sub transformation is nonlinear and operates on each of the State bytes independently – the invertible S-box (substitution table) is made up of 2 transformations. The shift row transformation sees the State shifted over variable offsets. The shift offset values are dependent on the block length of the State. The mix column transformation sees the State columns take on polynomial characteristics over a Galois Field values (28), multiplied x4 + 1 (modulo) with a fixed polynomial. Finally, the round key transform is XOR to the State. The key schedule helps the cipher key determine the round keys through keys expansion and round selection.

Overall, the structure of Rijndael is plays a high degree of modular design, which should make modification to counter any attack developed in the future much simpler than with past algorithm designs. The Rijndael algorithm is a new generation symmetric block cipher that supports key sizes of 128, 192 and 256 bits, with data handled in 128-bit blocks - however, in excess of AES design criteria, the block sizes can mirror those of the keys. Rijndael uses a variable number of rounds, depending on key/block sizes, as follows:

- 9 rounds if the key/block size is 128 bits

- 11 rounds if the key/block size is 192 bits
- 13 rounds if the key/block size is 256 bits

4.SHA-2 Algorithm

4.1.SHA Stands For Secure Hash Algorithm.

SHA-2 was designed by the National Security Agency (NSA) and was published in the Federal Information Processing Standard (FIPS) FIPS PUB 180-2. SHA-2 is a cryptographic hash function similar to MD5 and SHA-1 and it generates a 224, 256, 384 or 512-bit message digest or, in other words, a hash value from a variable length input depending upon the function used. Unlike SHA-1, SHA-2 is a set of cryptographic hashing functions. SHA-2 consists of SHA-224, SHA-256, SHA-384 and SHA-512. So SHA-224 would generate a 224-bit hash value, SHA-256 would generate a 256-bit hash value and so on. SHA-256/224 use data with a block size of 512 bits of data for processing with a 32-bit word size and 64 rounds of cryptographic functions. SHA-512/384 use data with a block size of 1024 bits with a 64-bit word size and 80 rounds of cryptographic functions. The functions that are used under SHA-2 are +, and, or, nor, not. As of now there are no known attacks on SHA-2 and it is considered the most secure of hashing algorithms to date. Even though the security provided by SHA-2 is very high, the adoption rate for SHA-2 has not increased because of the lack of compatibility with most operating systems. Only the newer operating systems support SHA-2 whereas most parts of the web are comprised of systems that are not compatible with SHA-2. Similar to SHA-1, SHA-2 is used for implementation under secure protocols, namely TLS, SSL, PGP, IPSec & S/MIME. SHA-2 is being enforced by the US government for implementation at the national level for all government projects and the private sector has also been encouraged to adopt the SHA-2 version of hashing as it is the most secure to date. Work on SHA-3 has already commenced at the NSA. There is no dependence on SHA-2 or SHA-1 and SHA-3 is said to be designed entirely from scratch and with completely different design fundamentals from SHA-1 and SHA-2.

5.Literature Survey

Jayeeta Majumder “Dictionary Attack on MD5 Hash” May-Jun 2012

Dicusses the MD5 message-digest algorithm takes as input a message of arbitrary length and produces as output 128-bit "fingerprint" or "message digest" of the input. The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem. Message Digest 5 is commonly used to create hash of passwords that is an encrypted form of password to be sent over network or stored in file system. Throughout this paper L.Thulasimani, M.Madheswaran “Design And Implementation of Reconfigurable Rijndael Encryption algorithms For Reconfigurable Mobile Terminals” in 2010

In any wireless communication security is crucial during data transmission. The encryption and decryption of details the major role in the wireless communication for security of the data. Encryption algorithms are used to ensure the security in the transmission channels. Similarly the area and the power consumption is not the major thing to be viewed since most of the mobile terminals are battery operated. So a mobile terminal which has an encryption unit with less area and power consumption is appreciated. This paper deals with the Advanced Encryption Standard (AES) which works on a128 bit data encrypting it with 128,192,256 bits of keys (ciphers) in a single hardware unit.

Harsh Kumar Verma,Ravindra Kumar Singh “ Performance Analysis of RC6, Twofish and Rijndael Block Cipher Algorithms in 2012

In this paper, Performance analysis of RC6, Twofish and Rijndael block cipher algorithms have been done on the basis of execution time and resource utilization. CPU utilization and memory utilization both are considered for determining resource utilization. These algorithms are parameterized algorithm and were designed to meet the requirements of the Advanced Encryption Standard (AES) competition and selected among five finalists of that competition. These three algorithms have a variable block size and a variable key size in their structure and encrypt four w-bits at a time. Allowable choices for w are 16 bits, 32 bits, and 64 bits. Twofish and Rijndael have same structure for encryption and decryption while RC6 have different. RC6, Twofish and Rijndael have 20, 16 and 10 rounds respectively. Performances of these three algorithms have been evaluated on key size of 128-bits

D.Ambika, V.Radha “ Secure Speech Communication – A Review” in 2012

Secure speech communication has been of great importance in civil, commercial and military communication systems. As speech communication becomes widely used and even more vulnerable, the importance of providing a high level of security becomes a major issue. The main objective of this paper is to increase the security, and to remove the redundancy for speech communication system under the global context of secure communication. So it deals with the integrating of speech coding, with speaker authentication and strong encryption. This paper also gives an overview and techniques available in speech coding, speaker Identification, Encryption and Decryption. The primary objective of this paper is to summarize some of the well known methods used in various stages for secure speech communication system.

Yaser Yaser Jararweh1, Lo'ai Tawalbeh2, Hala Tawalbeh1, Abidalrahman Moh'd3 "Hardware Performance Evaluation of SHA-3 Candidate" in 2010

Secure Hashing Algorithms (SHA) showed a significant importance in today's information security applications. The National Institute of Standards and Technology (NIST), held a competition of three rounds to replace SHA1 and SHA2 with the new SHA-3, to ensure long term robustness of hash functions. In this paper, we present a comprehensive hardware evaluation for the final round SHA-3 candidates. The main goal of providing the hardware evaluation is to: find the best algorithm among them that will satisfy the new hashing algorithm standards defined by the NIST. This is based on a comparison made between each of the finalists in terms of security level, throughput, clock frequency, area, power consumption, and the cost. We expect that the achieved results of the comparisons will contribute in choosing the next hashing algorithm (SHA-3) that will support the security requirements of applications in todays ubiquitous and pervasive information infrastructure.

6.Objectives

The main objective of this work will be analysis of various parameters of encryption algorithms on speech. Speech security which is very important in terms of privacy preservation. So there is a need of better encryption algorithms. These various mentioned cryptography algorithms studied in base papers are gone through and how they can be implemented on speech/voice is a part of research. Further the analysis of various parameters such as:

- Study of various speech encryption algorithms MD5,SHA2, RIJENDAEL

- Comparisons of MD5, SHA2, Rijndael based on following parameters :
    - Encryption and Delay time
    - Throughput no of bits per second.
    - complexity
    - packet lost
    - Delay time
    - Security level
- Performance evaluation of above mentioned speech encryption algorithms based on above mentioned parameters.

7.Methodology

The methodology of the work will require the three basic encryption algorithms approach to the encryption the voice into text and then into cipher text.Md5 hashing, SHA2, Rinjdael algorithms will be implemented on voice then these algorithms will perform their encryption and convert the voice into cipher text, Hence voice will be encrypted. The methodology is a software encryption .This is a software based encryption system of voice. Java the open source powerful language will be used to carry out such an implementation.

At the end the parameters :

- Encryption and Delay time.
- Throughput no of bits per second.
- Complexity
- Packet lost
- Delay time
- Security level

will be calculated and analyzed

8.Facilities Required

- Java version 6 or 7
- Windows Xp or later
- Intel Pentium or later CPU
- Android programming
- Eclipse Java platform compilers.

- Java Sound Api.

8.Significance Of Proposed Work

The proposed work will help in knowing the various parameters of the mentioned algorithms not into simply text encryption but the voice encryption . The proposed work leads a new way of research when these three algorithms will be applied and analyzed. As Encryption is a need now days because everyone needs to maintain his/her privacy of speech. This research will also help in identifying the best fitting approach to the speech encryption in future. The parameters calculated will give the brief robustness and efficiency of the proposed algorithms in this approach of research.

9.Conclusion

Cryptography is a field of network security. By this work we can successfully applied the security to the speech of in peer to peer communication or server based communication. The number of techniques used are required to encrypt the speech into text form then further encrypting it into cipher text. By the end of the work types of parameters calculation lead to identification of these three approaches and its robustness in the field of speech encryption.

10.Reference

1. 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
2. A. Jameel, “Transform-domain and DSP based secure speech communication”, Microprocessors and Microsystems,2007, 335–346
3. http://en.wikipedia.org/wiki/Cryptographic_hash_function
4. http://csrc.nist.gov/groups/ST/hash/sha-3/index.html
5. Mark Hasegawa-Johnson et al,” Speech Coding: Fundamentals And Applications”, Wiley Encyclopedia of Telecommunications
6. Akella Amarendra Babu et al, ,”Robust speech processing in EW environment”, International Journal of Computer Applications (0975 – 8887) Volume 38– No.11, January 2012
7. Dr.V.Radha et al,” Comparative Analysis of Compression Techniques for Tamil Speech Datasets, IEEE, ICRTIT, June 3-5, 2011
8. Venkatesh Krishnan,” A Framework For Low Bit-Rate Speech Coding In Noisy Environment”, A school of Electrical and Computer Engineering
9. P.Cummiskey et al,”Adaptive Quantization in Differential PCM Coding of speech, “Bell sys.Tech.J.Vol.52.No.7.p.1105.sept.1973
10. G.Kang and D.Coutler,”600 Bit-per-second voice digitizer(linear predictive format coder),”NRL Report 8043,Nov 1976
11. Jorgen Ahlberg,” Speech & Audio Coding” TSBK01 Image Coding and Data Compression Lecture 11, 2003
12. G.Kang,”Application of linear prediction to a narrow band voice digitizer,”NRL Report 7774,Oct.1974 of Speech Processing”