Benha University
Faculty of Engineering at Shoubra
Electrical Engineering Department
Computer Systems Engineering
Academic Year 2021/2022

Audio Encryption &Decryption

Submitted By:
Mahmoud Mohamed Abdelwahab
Mohamed Ramadan
Amr Kamal
Marwa Adel
Mariam Maher

Supervised By:
Prof :Sahar

Table of Contents

ABSTRACT

One of the most important methods to protect and verify information that is exchanged over public communication channels in the existence of third parties called antagonists is encryption. The stored or transmitted message is transformed in the encryption process to unreadable or gibberish form. The reverse process in which the intended recipient can reveal the encrypted message content is called decryption. The encryption and decryption processes are achieved using secret keys that are exclusively exchanged between the sender and recipient. This method can be applied to any form of message such as audio, video, image or text data. The current work applies symmetric and asymmetric methods for audio signal encryption and decryption.In asymmetric cryptography, we use two keys: the public key and the private key. Information gets encrypted with the public key. The process of getting data from the sender and the public key is straightforward. but it's difficult to decrypt data with the receiver's private key. the well known RSA Algorithm for audio signal used in encryption and decryption. In symmetric method to encrypt an audio file we read the files as raw bytes or more accurately binary numbers. These binary numbers are then converted into either Hexadecimal or Integer
and then these Hexadecimals and Integers are used for encryption. The symmetric method can be achieved using Hill Cipher. Monoalphabetic Cipher and Playfair Cipher.

Chapter one

1.1 Introduction

The digital transformation seeks new applications which are faster, quicker, simpler and most important is Secure.The quick development in computer technologies and the internet has made the security of information as the most important factor in information technology and communication.

Cryptography plays an important role in the field of network security. It is the science of altering information and changing it to a chaotic state. So It is the physical process that scrambles the information by rearrangement and substitution of content, making it unreadable to anyone except the person capable of unscrambling it.The stored or transmitted message is transformed in the encryption process to be unreadable. The reverse process means that only the intended user can recover the content of the encrypted message by decryption operation using a secret key which is shared between the transmitter and receiver.The encryption and decryption processes are achieved using secret keys that are exchanged between the sender and recipient. This method can be applied to any form of message such as audio, video, image or text data. Cryptosystems can be categorised to two main types based on the way in which encryption and decryption processes are carried out. symmetric key cryptosystems and asymmetric key cryptosystems.In symmetric key cryptosystems, the same key is shared between the transmitter for encryption and the receiver for decryption the data. The strength of symmetric algorithms depends on the size of the secret key. Blowfish, Advanced Encryption Standard (AES) and Data Encryption Standard (DES) are examples of symmetric key encryption techniques. In asymmetric key cryptosystems, each user in the system has two different keys private which is used for encryption at the transmitter and public which is used for decryption at the receiver. Although these two keys are different, they are mathematically related. Thus, reconstructing the original message by decrypting it is feasible. Asymmetric ciphers have several advantages over conventional symmetric ciphers. Our current project is to apply symmetric and asymmetric cryptographic algorithms for audio signal encryption and decryption.[1][2]

1.2 Problem Statement

Most of the communication between the sender and the receiver is via voice. With this availability comes the problem of maintaining the security of information that is displayed in public. we used encryption and decryption are critical security measures that are designed to ensure that communication is received and processed correctly and security.

1.3 Project Scope

In this system, the audio will be saved in encrypted form. and will be sent to the receiver to decrypt it.

1.4 Objectives

Audio encryption ensures secure audio transmission. With the fast growth of communication technology, protection of audio from the hackers became a critical task for the technologist. So there is always a need of a more secure and faster audio encryption technique [3]. So we Focused in our Project to Design and develop audio encryption/decryption algorithms and to develop a system that has a high level of security.

1.5 Background

1.5.1 Symmetric Algorithms

- **DES**

The cryptosystem which is most used throughout the world for protecting information is the Data Encryption Standard (DES) which was announced by the National Bureau of Standard (NBS). The DES must be stronger than the other cryptosystems in its security. But, because the process time required for cryptanalysis has lessened, and because hardware technique has developed rapidly, the DES may be attacked by various kinds of cryptanalysis using parallel process. It may be especially vulnerable to attack by differential cryptanalysis. Therefore, the DES will require strengthening to ensure cryptographic security in the days to come.[4]

DES works on bits, or binary numbers--the 0s and 1s common to digital computers. Each group of four bits makes up a hexadecimal, or base 16 number. DES works by encrypting groups of 64 message bits, which is the same as 16 hexadecimal numbers. To do the encryption, DES uses "keys" where are also apparently 16 hexadecimal numbers long, or apparently 64 bits long. However, every 8th key bit is ignored in the DES algorithm, so that the effective key size is 56 bits.[6]

- **AES**

Advanced Encryption Standard (AES) algorithm is one on the most common and widely symmetric block cipher algorithm used in worldwide. This algorithm has an own particular structure to encrypt and decrypt sensitive data and is applied in hardware and software all over the world. It is extremely difficult to hackers to get the real data when encrypting by AES algorithm. Till date is not any evidence to crake this algorithm. AES has the ability to deal with three different key sizes such as AES 128, 192 and 256 bit and each of this ciphers has 128 bit block size.[7]

1.5.2 Asymmetric Algorithms

- **RSA**

RSA is basically an authentication system and Internet encryption method. This algorithm was developed by its inventors in 1977 (Ron Rivest, Adi Shamir and Leonard Adleman). It is one of the most common asymmetric key cryptosystems that it is included as a part from Netscape and Microsoft of the Web browsers. Initially, two large prime numbers are chosen and multiplied in this algorithm to create the public and the private keys pair which are further used in the encryption and decryption operations. There is no need to send the private key throughout the Internet if the RSA algorithm is used. The private key is used to decrypt the secret message at the receiver which has been ciphered or encrypted by using the public key at the transmitter. Everyone can know the public key which is used to encrypt the messages, but the encrypted messages by the public key can be decrypted only with the private key. [5] It is a public key encryption technique. It is safe for exchange of data over the internet. It maintains confidentiality of the data. RSA has high toughness as breaking into the keys by interceptors is very difficult. It is very easy to implement the RSA algorithm. Cracking the RSA algorithm is very difficult as it involves complex mathematics. Sharing public keys to users is easy. It has a slow data transfer rate due to large numbers involved. High processing is required at the receiver's end for decryption.[8]

- **ECC**

Elliptic curve cryptography (ECC) is a class of cryptographic algorithms, although it is sometimes referred to as though it were an algorithm in and of itself. ECC is named for the type of mathematical problem on which its cryptographic functions are based. ECC has several advantages over other types of algorithms. It has a higher cryptographic strength with shorter keys than many other types of algorithms, meaning that we can use shorter keys with ECC while still maintaining a very secure form of encryption. It is also a very fast and efficient type of algorithm, allowing us to implement it on hardware with a more constrained set of resources, such as a cell phone or portable device, more easily.[9]

References

[1] Fahmy, Sura. (2018). ENCRYPTION AND DECRYPTION OF AUDIO SIGNAL BASED ON RSA ALGORITHN. 5. 57-64. 10.5281/zenodo.1341956. http://dx.doi.org/10.5281/zenodo.1341956

[2] International Journal & Magazine of Engineering,Technology,Managment and Research . A peer Reviewed open Access International Journal . “Audio Cryptography System”Shaik Abdul Muneer Assosiate Professor, Department of Physics, Osmania College (Autonomous), Kurnool.

[3] Rashmi A. Gandhi,Dr.Atul M. Gosai. MCA Department,Shri Sunshine College, Rajkot,Gujarat Department of Computer Science. Saurashtra University, Rajkot,Gujarat .International Journal for Research in Applied Science & Engineering Technology (IJRASET).’’Audio Encryption with AES and Blowfish” November 2016 .www.ijraset.com

[4] Seung-Jo Han, Heang-Soo Oh and Jongan Park, "The improved data encryption standard (DES) algorithm," Proceedings of ISSSTA'95 International Symposium on Spread Spectrum Techniques and Applications, 1996, pp. 1310-1314 vol.3, doi: 10.1109/ISSSTA.1996.563518.

[5] Al-Kateeb, Zeena N., and Saja J. Mohammed. "Encrypting an audio file based on integer wavelet transform and hand geometry." Telkomnika 18.4 (2020): 2012-2017.

[6] Grabbe, J. Orlin. "The DES algorithm illustrated." (2010).

[7] Abdullah, Ako Muhamad. "Advanced encryption standard (AES) algorithm to encrypt and decrypt data." *Cryptography and Network Security* 16 (2017): 1-11.

[8] "RSA Full Form - GeeksforGeeks" https://www.geeksforgeeks.org/rsa-full-form/#:~:text=It%20is%20very%20easy%20to,key%20to%20users%20is%20easy.

[9] The Basics of Information Security (Second Edition)"Understanding the Fundamentals of Infosec in Theory and Practice "2014, Pages 69-88 . https://doi.org/10.1016/B978-0-12-800744-0.00005-1