Encryption of Speech Signals Using El-Gamal's method and elliptical curve method

Nagaraju S M
20BEC0278
VIT University
Vellore, Tamil Nadu
nagaraju.sm2020@vitstudent.ac.in

Ankit Raj
20BEC0766
VIT University
Vellore, Tamil Nadu
ankit.raj2020@vitstudent.ac.in

Leela Praneeth
20BEC0771
VIT University
Vellore, Tamil Nadu
leelapraneeth.puli2020@vitstudent.ac.in

***Abstract*—**Information Security is an important aspect of data sharing. A large portion of Corporate, Government, and legal documents are being primarily shared over the internet. Prime among these are audio signals which are easy to manipulate and doctor, which can cause a lot of strife and wasted time or sometimes physical risk to the parties sharing the information. We propose different encryption techniques. El-Gamal Algorithm is a very secure and efficient way to transmit speech signals wirelessly without the worry of a privacy breach or high noise. We will also look at elliptical curve cryptography. ECC here is a complex encryption technique and is harder to breach using brute force or a stolen key.

Keywords—ECC, Cryptography, Encryption, El-Gamal's algorithm MATLAB

I. Introduction

Cryptography is a really important part of our daily lives due to our constant reliance on the internet and the threat of cyber attacks from malicious third parties. Anything we transmit that is either text, images, or audio.

Audio signals are becoming more and more important with the introduction and popularization of remote work and home automation. There are many purposes for which we need a safe transmission of speech and audio of a conversation or the transcript of a meeting. thus arises the many encryption schemes and algorithms that aid in this aspect.

For our purpose here we will take an audio signal with speech and take down its transcript; these are encrypted with different encryption schemes. We are using ECC for the encryption of the audio signal as it is a viable and efficient option while El-gamal's method is used for the encryption of the transcript text and the audio..

When the encryption of messages in both these forms is safely done, assuming the necessary keys are all present with the senders and recipients they are transmitted over a channel between the concerned parties.

II. Overview of the cryptography methods

A. Elliptical Curve Cryptography (ECC)

The elliptical curve despite its name is different from an ellipse. In ECC we use an elliptical curve over a finite field,

where it is a cubic function and the solutions (x,y). Victor Miller and Neal Kobitz first put it forward as an alternative to existing algorithms like RSA, but with a smaller key size

for the same level of security. Like any cryptosystem, ECC is a one-way function and it is easy to perform the prime multiplication but hard to get the prime factors of the resulting number, this makes brute force hacking and guessing of the keys really improbable.

We use Diffie–Hellman key exchange to generate a shared key from the private keys of the sender and recipient along with their public keys and in this case the general information available such as the parameters a, b, and the prime number p of the elliptical curve over a finite field.

The above cryptographic techniques work in tandem to provide an easy-to-use and secure way to transmit data over the internet which is able to fend off cyber attacks and is up to modern standards. ECC using Diffie-Hellman is a perfect example of harmonious integration of age-old proven methodologies with new innovations that help the technology exceed the sum of its parts.

..

B. El-Gamal's Algorithm

Data communication and data protection depend heavily on security. It helps prevent unwanted access to sensitive data that could lead to data loss or alteration by unidentified parties, making data transmission unsafe. El Gamal encryption uses public key cryptography. It encrypts the message and uses asymmetric key encryption for two-party communication. This cryptosystem is based on the fact that it is quite challenging to calculate gak even if we know gk and ga, the discrete logarithm in the cyclic group. If we want to understand the whole picture, we have to go step by step by actually encrypting and decrypting the messages. We will use the example of two peers who are willing to use the El Gamal algorithm to communicate data in a secure manner.

III. ALGORITHMS

A. *Elliptical Curve Cryptography(ECC)*

- Step 1:1.Input X is taken as an audio file.
- Step 2:2.The message m, i.e. each value of audio file X, can be turned into the coordinate (Xm,Ym) so that it can be used as a point on an elliptical curve.

$$Xm = m*K + J, \quad J= 0,1,2,3$$

$$Ym = x3 + ax + b$$

Where; message is m , Random Positive integer is K , Square modulo P is (Xm,Ym), where P is the prime number and P K*m.

- Step 3:3.Encryption/ Decryption system needs a point on G and an elliptic group Ep(a,b). A secret integer s is chosen by the user and is used to compute Q=s.G. User B's public key comprises Ep(a,b), and the points G & Q, while private key is s. To encrypt plus transmit message Pm to user B, user A selects a random positive integer k and generates the ciphertext Cm consisting of the pair of points. Cm={kG,Pm+kQ}
  - Step 4:4.Ciphertext is decrypted using the method {Pm + kQ s.(kG) = Pm + k(s.G) s.(kG)}= Pm

B. *El-Gamal's Algorithm*

- Step 1: Public and Private Key Generation. User 1 tries to select a very long or large integer x while also selecting a cyclic group. It will also select the next element c and the component b from this cyclic group. The values will be chosen so that when a particular function is used, the result is equal to 1. After the value selection phase, the value will be calculated and used to generate the private key. The value will be determined using the formula fm=bc. User1 in the current case chooses F as his public key, fm = bc, a and b. The values of a will be kept as a private key, which will then be used as a private key.
- Step 2: User2 encrypts the data using user-1's public key. There are specific settings that user2 must select in order to begin encrypting a message. In addition, user2 will have to choose one of the p values of the cyclic group. As with user1, a cyclic group will be used. The value should be chosen in such a way that Inc passes through and results in a 1 in the specified function. The message will be encrypted with the public key using some additional values generated by user2. Pm=bp is the value that will be created. The second revaluation will make bc equal to bap. To get closer to the encryption method, the result of this calculation will be multiplied by the second variable Z. At some point, the value will be transferred using the results of the calculations to bp,Z*bap.
- Step 3: Decrypting the message at the end of user 1. User 1 then determines the correct number that will be used to decrypt the encrypted message by computing the values chosen in the first and second stages. To get the decrypted value, user1 processes bap and divides the result by Z. The value that was decrypted was something that was encrypted in the second step. In the above case, user 1 started the procedure by calculating the private and public keys, which are the heart and soul of the algorithm. User2 continues to use the key in the next step to encrypt the method. The message is encrypted so it can be decrypted using the value calculated in the initial phase. In the third stage, it was seen that after dividing the full value by the number generated in the third step, the message was completely decrypted, allowing the end user to read it. The same procedure is used every time the impulse arises to send a message securely

IV. RESULTS AND DISCUSSION

A single plaintext can be encrypted to a large number of different ciphertexts thanks to the probabilistic nature of El Gamal encryption. As a result, a general El Gamal encryption results in a 1:2 expansion of the size of the ciphertext over the plaintext. Two exponentiations are necessary for El Gamal encryption, but they are independent of the message and can be computed beforehand if necessary. One exponentiation and one computation of a group inverse are needed for decryption, although they can both be readily combined into a single exponentiation.

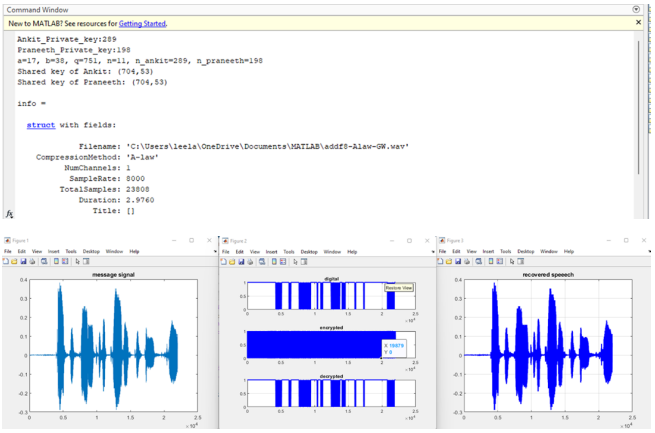

Fig.1: *Elliptical Curve Cryptography(ECC) Output*

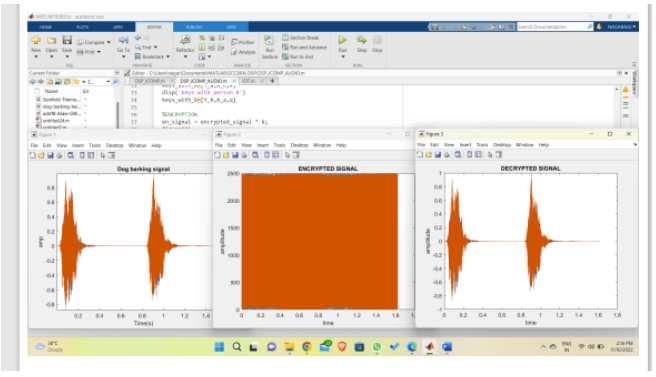

Fig.2: *El-Gamal's Algorithm Output*

ACKNOWLEDGMENT

First and foremost we would like to express our deepest thanks to Dr. Kalaivan S, our faculty who diligently guided us through all the steps of this project from its conception to the final presentation, without her the quality of this project would not have been up to this quality.

We also want to show our gratitude towards VIT, which provided us with resources to research and helped us get sources from which to pull ideas and improve our project.

References.

[1] Stoyanov, B.; Ivanova, T. Novel Implementation of Audio Encryption UsingPseudo Random Byte Generator. Appl. Sci. 2021, 11,10190.https://doi.org/10.3390/app112110190J.

[2] G. V. S. Raju and R. Akbani, "Elliptic curve cryptosystem and its applications, "Elliptic curve cryptosystem and its applications | IEEEConference Publication

[3] S. M. C. Vigila and K. Muneeswaran, "Implementation of text based cryptosystem using Elliptic Curve Cryptography,"|IEEE ConferencePublication

[4] Omar A. Imran, Sura F. Yousifa, Isam Salah Hameeda, Wisam Najm Al-DinAbeda, AliThaeerHammi, https://reader.elsevier.com/reader/sd/pii/S1877050920308681?

[5] Amer Daeri, Amer R. Zerek, Mohamed A. Abuinjam,http://ipco-co.com/PET_Journal/Papers%20CEIT'14/025