Implementing Encryption Algorithm for Addressing GSM Security Issues

Mr.Mandar M. Kulkarni[1], Mr.Anant S.Bhide[2],
Mrs.Amruta M. Kulkarni[3], Mr.Prafulla P.Chaudhari[4]

[1] Assistant Professor, E&C Department, SSGBCOET Bhusawal, Maharashtra, India.
[2] Associate Professor, E&C Department, SSGBCOET Bhusawal, Maharashtra, India.
[3] Assistant Professor, E&TC Department, SSBT Bhambhori Jalgaon, Maharashtra, India.
[4] Assistant Professor, E&TC Department SIEM Nasik , Maharashtra, India.

---***---

Abstract – *The Advanced encryption standard (AES) is an algorithm that was formerly considered to be the most popular method for private key encryption. AES is still appropriate for moderately secured communication. In this paper we have implemented AES algorithm for voice data encryption and decryption by using the MATLAB. The GSM speech service is secure up to the point where speech enters the core network. However to achieve end-to-end security it is desired that the GSM subscriber, not the network operator controls the encryption on the speech channel. A new approach of encryption at the user-end is introduced. The MATLAB Software was used as program module of the system implementing the encryption and decryption algorithm.*

Key Words: AES, GSM, NIST, QAM

1. INTODUCTION

Mobile phones are used on a daily basis by hundreds of millions of users, over radio links. Emerging wireless networks share many common characteristics with traditional wire-line networks such as public switch telephone/data networks, and hence many security issues with the wire-line networks also apply to the wireless environment. The GSM system doesn't provide end-to-end security and lacks in provision of traffic confidentiality to its subscribers. Anonymity, authentication, and confidentiality are the security services which are offered by the world's largest mobile telephony system. Still this system is defenseless against many attacks and fails to ensure taut safety of the user's telephone conversations and data transfer sessions. Confidentiality of transmitted data is achieved by encrypting the information flow between the communicating parties. In GSM networks, only the radio link between the mobile terminal and the base station is encrypted whereas the rest of the network transmits data in clear-text. Radio link confidentiality in GSM is not sufficient for attaining end-to-end security. As a result, a need for investigating mechanisms for implementing absolute confidentiality of traffic arises. As per Saad Islam the GSM system doesn't provide end-to-end security [1].

The modern field of cryptography can be divided into several areas of study. Cryptosystem is a system in which the information is made unintelligible to all but the intended receiver. The process of disguising a message, often referred as plaintext, in such a way as to hide its substance is called encryption. An encrypted message is called cipher text. The process of turning cipher text back into plaintext is called decryption. A cryptographic algorithm, also called a cipher, is a mathematical function for encryption and decryption. The security of algorithm is based on secret key. A cryptosystem consist of an algorithm, all possible plaintexts, cipher texts and keys.

Now days there are many situations to keep voice secret in voice communication. This can be achieved by voice encryption by using different encryption algorithms. AES-Rijndael is suitable on all aspects and future research in optimization techniques will definitely make it the de facto encryption for resource constrained wireless networks. [2].

In the following chapters a complete picture of our proposed work has been explain. The proposed algorithm for encryption/decryption has been explained in chapter 2.

2. SYSTEM DEVELOPMENT

In this project first we have write a MATLAB code for the AES algorithm to encrypt & decrypt the recorded voice signal. Two separate codes were written for the encryption & decryption. Here we have taken 128-bit (16 byte) data as a plaintext and 128-bit key for encryption. The recorded signal is digitized and sampled at a rate of 8000 Hz generally a sampling rate of at least 2f. (According to Nyquist criteria).

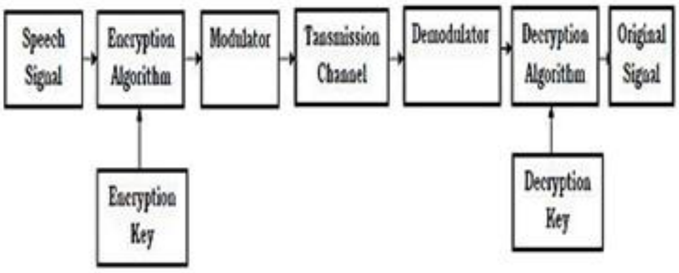

Fig -1 : Block Diagram of Proposed System

Encryption is done on each individual sample of audio file which is recorded. Our encryption algorithm was aimed to randomize the speech signal in such a manner that the encrypted speech signal becomes un-understandable while maintaining the speech-like waveform of the signal.

The Advanced Encryption Standard (AES) was published by the National Institute of Standards and Technology (NIST) in 2001. AES is a symmetric block cipher that is intended to replace DES as the approved standard for a wide range of applications. Figure 2 shows the overall structure of the AES encryption process. The cipher takes a plaintext block size of 128 bits, or 16 bytes. The key length can be 16, 24, or 32 bytes (128, 192, or 256 bits). The algorithm is referred to as AES-128, AES-192, or AES-256, depending on the key length. The input to the encryption and decryption algorithms is a single 128-bit block [3].

This block is copied into the State array, which is modified at each stage of encryption or decryption. After the final stage, State is copied to an output matrix.. Similarly, the key is depicted as a square matrix of bytes. This key is then expanded into an array of key schedule words. Each word is four bytes, and the total key schedule is 44 words for the 128-bit key. The cipher consists of *N* rounds, where the number of rounds depends on the key length: 10 rounds for a 16-byte key, 12 rounds for a 24-byte key and 14 rounds for a 32-byte key. The first *N-1* rounds consist of four distinct transformation functions: Sub Bytes, Shift Rows, Mix Columns, and Add Round Key, which are described subsequently. The final round contains only three transformations, and there is a initial single transformation (Add Round Key) before the first round, which can be considered Round 0. Each transformation takes one or more *4×4* matrices as input and produces a *4×4* matrix as output [3].

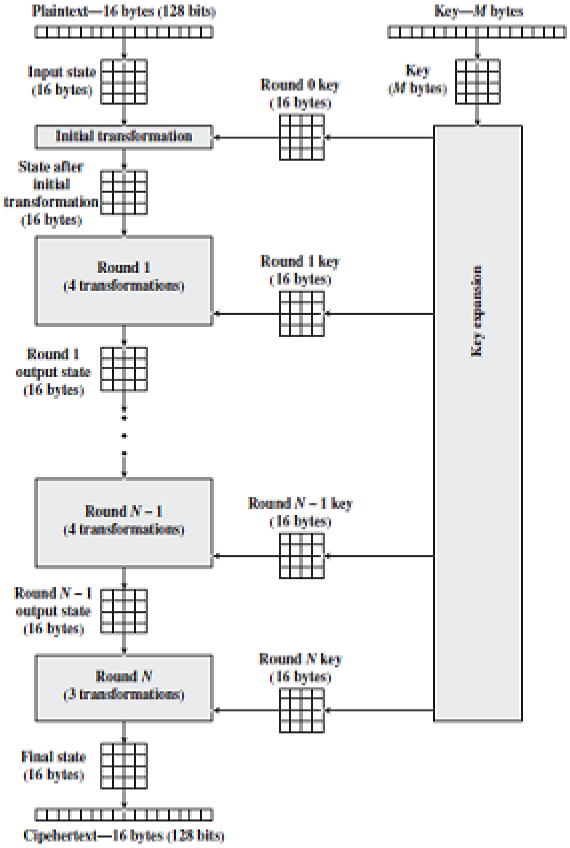
Plaintext—16 bytes (128 bits)
Key—M bytes
Input state (16 bytes)
Round 0 key (16 bytes)
Key (M bytes)
Initial transformation
State after initial transformation (16 bytes)
Round 1 (4 transformations)
Round 1 key (16 bytes)
Key expansion
Round 1 output state (16 bytes)
Round N – 1 (4 transformations)
Round N – 1 key (16 bytes)
Round N – 1 output state (16 bytes)
Round N (3 transformations)
Round N key (16 bytes)
Final state (16 bytes)
Ciphertext—16 bytes (128 bits)

Fig -2: AES Encryption Process

A modulation scheme is needed to transmit information over a communication channel. Among the various modulation methods are, amplitude modulation (data encoded by changing the amplitude of the signal), frequency modulation (data encoded by changing the frequency of the signal), and phase modulation (data encoded by changing the phase of the signal). As per Toufic Chmayssani, Geneviève Baudoin, & Gael Hendryckx Digital modulations can handle data transmission through a GSM speech-dedicated channel [4]. In our proposed work we are using 4- QAM Technique. The transmitting channel is supposed to be AWGN.

At the receiving end just reverse process is used. For the decryption each stage is easily reversible. For the Substitute Byte, Shift Rows, and Mix Columns stages, an inverse function is used in the decryption algorithm. For the Add Round Key stage, the inverse is achieved by XORing the same round key to the block, as with most block ciphers, the decryption algorithm makes use of the expanded key in reverse order [3].

3. EXPERIMENTAL RESULT

Experiments were performed for both encrypted and non encrypted voice to determine the utility of our proposed technique. The encrypted speech signal was not understandable for our proposed encryption algorithm. This encrypted speech was considerably different from the original speech and was unintelligible. Nevertheless, introduction of decryption at the receiving end recovered the original signal back. To view the performance of the proposed scheme graphically, plots of the waveforms of original and encrypted speech signals were obtained.

1. Original Voice Signal

The duration of the audio recorded can vary according to the user requirement. In order to record an audio file of more duration user has to accomplish some hardware improvement in the project.

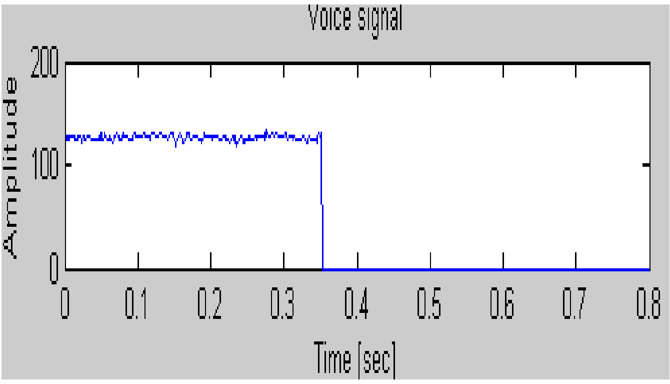

Fig -3: Original Voice Signal

2. Encrypted Voice Signal

The program will perform the first encryption on the recorded voice.

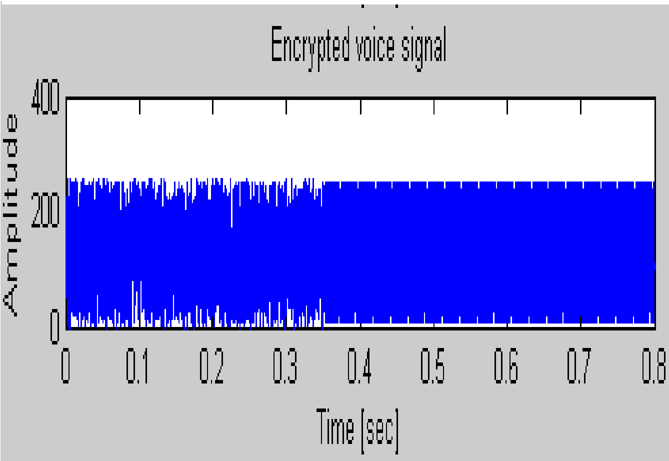

Fig -4: Encrypted Voice Signal

3. Decrypted Voice Signal

The program will perform for decryption on the encrypted voice signal.

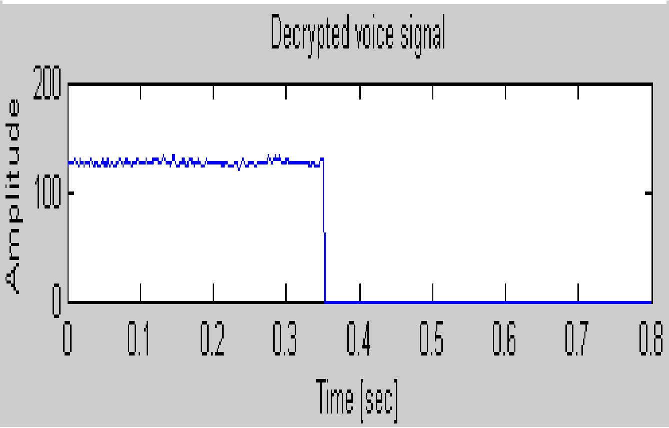

Fig -5: Decrypted Voice Signal

4. SNR Vs BER

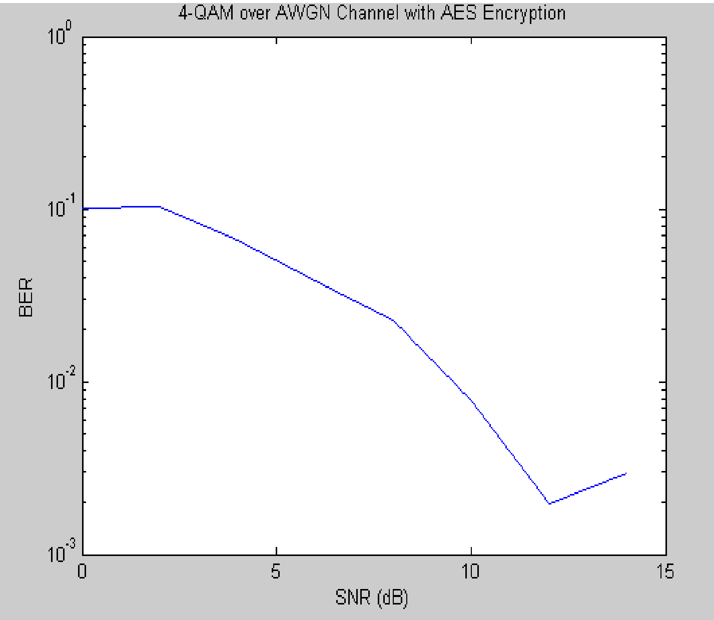

Fig -6: SNR Vs BER for 4-QAM over AWGN Channel with AES Encryption

3. CONCLUSIONS

The technique used in this paper guarantees a secure communication. In the proposed technique the audio file which is achieved after decryption is exact copy of the original file. In this paper, we have proposed a cryptography technique, which provides security to the audio data which is meant to be used for audio transfer within GSM, Here we have applied encryption on the whole audio data which will provide a very good security to our audio transmission. With this technique we have achieved a loss less transfer between the sender and receiver on a single system.

GSM is the most commonly used system for mobile communications. Lack of security and privacy are the major issues of GSM that need to be addressed. Various encryption techniques exist that aim to make the GSM system secure and confidential yet there are some flaws and short-comings. In future we also the implement proposed technique on ARM, DSP Processor.

ACKNOWLEDGEMENT

First of all, I would like to express my deep sense of respect and gratitude towards my advisor and guide Mr. A. S. Bhide, who has been the guiding force behind this work. I am greatly indebted to him for his constant encouragement, invaluable advice and for propelling me further in every aspect of my academic life. His presence and optimism have provided an invaluable influence on my career and outlook for the future

Next, I want to express my respects to HOD Mr. G. A. Kulkarni for teaching me and also helping me how to learn. They have been great sources of inspiration to me and I thank them from the bottom of my heart. I would like to thank all faculty members and staff of the Department of Electronics and Communication Engineering, SSGBCOET Bhusawal for their generous help in various ways for the completion of this thesis.

Also I would also like to thank my wife Amruta and my friend Prafulla for helping me a lot during the thesis period.

REFERENCES

[1] Saad Islam and Fatima Ajmal *Developing and Implementing Encryption Algorithm for Addressing GSM Security Issues*, International Conference on Emerging Technologies, 978-1-4244-5632-1/09 ©2009 IEEE pp 358-361.

[2] Mandar M. Kulkarni, A. S. Bhide, and Prafulla P.Chaudhari *Encryption Algorithm Addressing GSM Security Issues- A Review,* International Journal of Latest Trends in Engineering and Technology (IJLTET) ISSN: 2278-621X Vol. 2 Issue 2 pp 268-273 March 2013.

[3] Cryptography & Network Security, Principles and Practice, Fifth edition, Willam Stallings.

[4] Toufic Chmayssani, Geneviève Baudoin, & Gael Hendryckx *Secure Communications Through Speech Dedicated Channels Using Digital Modulations* ICCST 2008, 978-1-4244-1817-6 ©2008 IEEE pp 312-317.

BIOGRAPHIES

He received his Bachelor of Engineering degree in Electronics and Communication Engineering from SSGBCOET Bhusawal in 2009. He is currently pursuing Masters of Engineering degree in Electronics and communication from SSGBCOET Bhusawal MH India.

He is working as Associate Professor in SSGBCOET Bhusawal. He received Bachelor of Engineering in Electronics and Telecoms and Masters of Engineering in Electronics, with Honors, having Work Experience of 12 years.

She is working as Assistant Professor in SSBT Jalgaon. She received Bachelor of Engineering in 2010 in Electronics and Telecoms from SSBT Bhambori Jalgaon, M.H. INDIA, with Honors and Masters of Engineering in 2013 in Digital Electronics from Government College of Engineering Jalgaon M.H India with Honors, having Work Experience of 4 years.

He is working as Assistant Professor in SIEM Nasik. He received Bachelor of Engineering in 2008 in Electronics and Telecoms with Honors and Masters of Engineering in 2014 in Electronics & Communication from SSGBCOET Bhusawal M.H India with Honors, having Work Experience of 7 years.