Efficient Audio Encryption Algorithm For Online Applications Using Transposition And Multiplicative Non-Binary System.

Raghunandhan K R[1], Radhakrishna Dodmane[2], Sudeepa K B[3],Ganesh Aithal[4]
[1]*Department of CSE, Asst Professor, NMAMIT, NITTE*
[2]*Department of CSE, Asst Professor, NMAMIT, NITTE*
[3]*Department of CSE, Asst Professor, PACE, Manglore*
[4]*Department of CSE, Professor & Head, PACE, Manglore*

ABSTRACT - *Audio Encryption is a technique used to transmit secure information. This ensures audio security between Sender and Receiver. With the fast growth of communication technology, security of sending confidential audio information plays a vital role. Protection of audio from the eavesdroppers plays a critical task for the technologist. The paper presents two layer securities, which includes both transposition and substitution cipher. The time taken for the transposition cipher in hardware as well as software is very small compared to substitution cipher. We first process the audio signal with transposition cipher. In the second stage Modulus Multiplication is used as substitution cipher, for this the key is generated using Pseudo Random Number Generation (PRNG). This Method proposed in which we get secured transmission with less time completion for the algorithm. This indicates the Technique can be used for Online process in communications.*

I. INTRODUCTION

1.1. Cryptography [1]:

The Demand on Information security has extensively increased due to the sensitivity of the audio signal exchanged over public communication channels. One of the primary goals of cryptographic systems (cryptosystems) is to help communicators exchanging their information securely.

Audio cryptography:

Audio cryptography encryption is the method of including the noise (key) to the plain text audio and while decryption is the process of taking out the original plain text back by using the same key. [8][9][14].

Cryptography provides a number of security goals to ensure the privacy of data, non alteration of data cryptography, it is widely used today due to the great security advantages of it. Here are the various goals of cryptography.

Confidentiality: Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.

Authentication: The information received by any system has to check the identity of the sender that whether the information is arriving from a authorized person or a false identity.

Integrity: Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.

Non Repudiation: Ensures that neither the sender, nor the receiver of message should be able to deny the transmission.

Access Control: Only the authorized parties are able to access the given information.

Cryptography itself can be divided into transposition and substitution.

I. Transposition
II. Substitution

Transposition : Transposition is a rearrangement of letters of a message according to a certain algorithm. In other words Transposition is an encryption in which the letters of the message are rearranged– (permutation of bits)[2][5].

Substitution : Substitution is a more robust and versatile form of cryptography. As the name suggests, characters in the original text (known as plaintext in crypto speak), are substituted by other characters or symbols using certain algorithm. [2][5]

Cryptographic systems are divided into two types of systems:

I. Secret-key (Symmetric) cryptosystems [3].
II. Public-key (Asymmetric) cryptosystems [4].

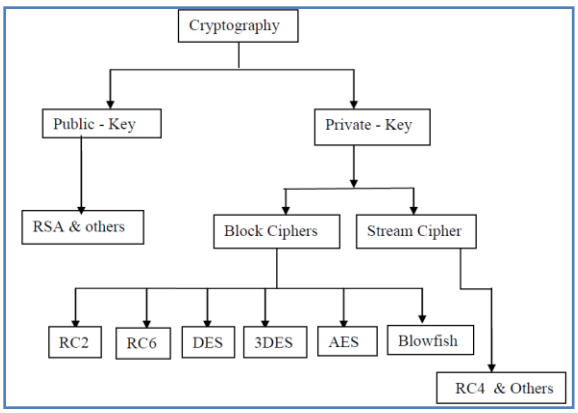

Fig: overview of the field cryptography.

1.1 Secret-Key (Private or Symmetric) Cryptosystems:

Symmetric key encryption use only key to encrypt and decrypt data. Key plays an important role in encryption and decryption.

The size of the key determines the strength of Symmetric key encryption.

Symmetric algorithms are of two types:

i. Block ciphers
ii. Stream ciphers.

The block ciphers are operating on data in groups or blocks. Examples are of Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Blowfish.

The Stream ciphers are operating on a single bit at a time. RC4 is stream cipher algorithm. [3].

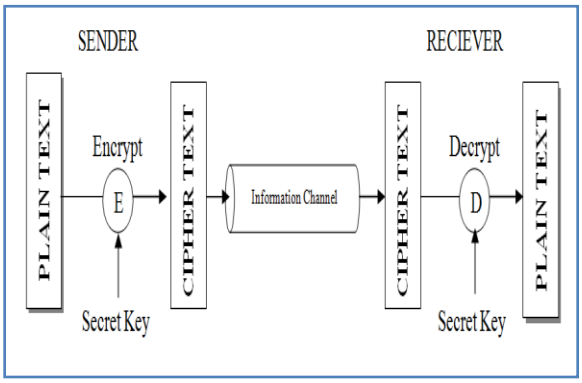

Fig 1.1.Secret key cryptosystems

1.2 Public-Key(asymmetric) Cryptosystems:

In Asymmetric key encryption, two keys are used; private keys and public keys. Public key is used for encryption and private key is used for decryption (e.g Digital Signatures). Public key is known to the public and private key is known only to the user.

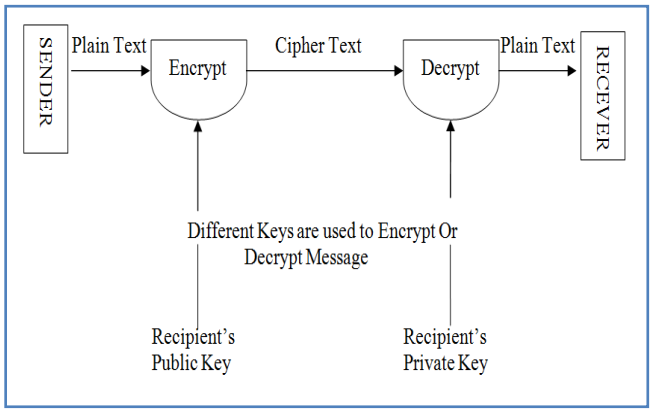

Fig 1.2. Public key cryptosystems

2. LITERATURE REVIEW

However, number theory or algebraic concepts based traditional ciphers, such as Advanced Encryption Standard (AES)[15], A5/1, A5/2, A5/3 type cipher systems algorithms mentioned are bit by bit XOR function. In this XOR is operates bit by bit and will consume more time compared to byte by byte. The fallowing drawbacks are listed for the bit by bit operation, they are.

i. It is slower when we compare with byte by byte system.
ii. Encryption algorithm is only X-OR in nature.
iii. In key generation keys are either 0 or 1.

Proposed system in which operation is not using bit by bit by adopting byte by byte we can have more no of algorithms. They are

i. Modulo Additive
ii. Modulo Multiplicative
iii. Exponential
iv. Combination of all above

However in the proposed system we uses only modular multiplicative as our algorithm. The explanation of that is given in the next section.

3. PROPOSED SYSTEM

Secure Audio Encryption Using Transposition and Multiplicative Non-Binary System highlights use of cryptography and their use in highly Secured Audio cryptography system (ACS).

The proposed audio cryptography scheme is perfectly secure and easy to implement.

The system is called perfectly secured, since we can generate the key such that it makes a onetime pad. This can be achieved by sufficiently larger stages of Feedback Shift Registers (FSR)

The scheme is said to be easy to implement because all the stages of the substitution process can be designed using hardware very easily. The main objective of this Paper is to provide a secure audio communication.

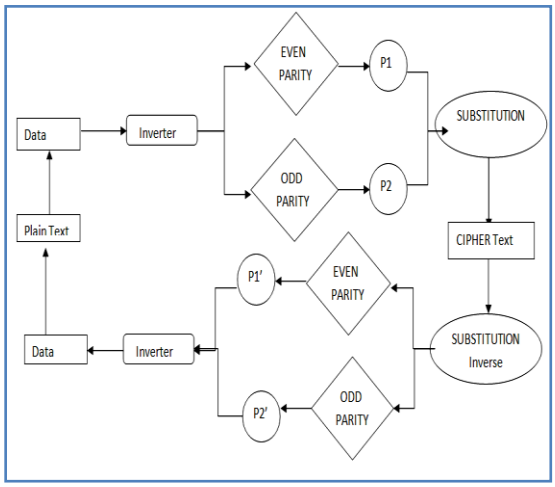

Figure 3.1: Hybrid Transposition and Multiplicative Non-Binary System for Audio encryption model

This paper relies on 2 phases on Encryption as well as in Decryption part.

3.1 Encryption

The process of Encryption is as follows:

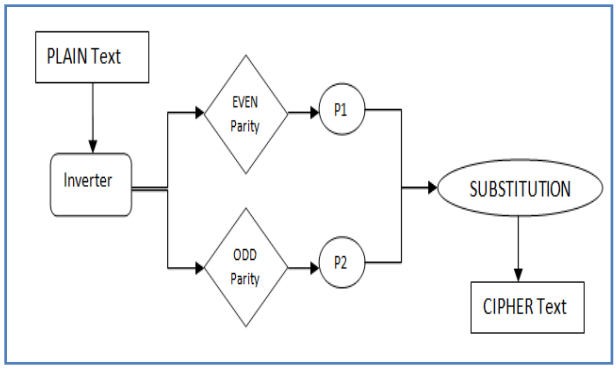

Fig 3.1.1. Encryption Part of Secure Audio Encryption Using Transposition and Multiplicative Non-Binary System.

After getting audio information of one byte, it is complemented such that the system secure.

This complemented audio data goes through two phases of encryption they are.

i. Transposition
ii. Substitution

In First phase this complimented byte uses permutation using a key for encryption, depending on two categories. That is First on even parity byte, second on odd parity byte. If the byte is even parity permutation key P1 is used. In case of odd parity permutation key P2 is used.

The generation of key P1 and P2 are explained in Table 3.1

Table 3.1 Generation of Permutation Key in Encryption.

Step1.Take ones compliment for the given 8 bit Original Audio signal

Step2.Check Parity

If the number of ones are Even then use Permutation 1.
Permutation of Even no of 1's=6 4 7 1 2 8 5 3

If the number of ones are ODD then use Permutation 2.
Permutation of Odd no of 1's =5 8 6 1 2 4 3 7

Step3. From Step 3 based on transposition we generating first level of Cipher.

In the Second phase the partial encrypted information of the first phase is taken as plain text and is encrypted using a substitution cipher. The key is generated by a Pseudo Random Number Generation (PRNG) using Feedback Shift Registers (FSR). The output of this stage is stored or transmitted securely. The algorithm used in the second phase in that is Substitution cipher of multiplication mod 255. During the key generation process the care should be taken such that the initial values of feedback shift registers should have multiplicative inverse.

3.2 Decryption

The process of Decryption is as follows:

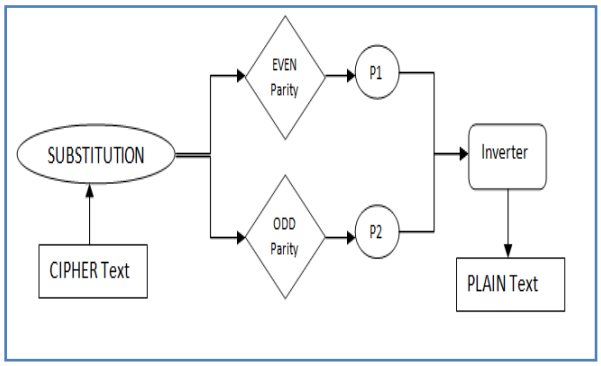

Fig 3.1.2. Decryption Part of Secure Audio Encryption Using Transposition and Multiplicative Non-Binary System.

Transforming an encrypted message to its original form is accomplished by a process known as Decryption. This also includes two phases

In the first phase the cipher text is taken and it is get multiplied with the key which is generated by a Pseudo Random Number Generation (PRNG) using Feedback Shift Registers (FSR). The algorithm used in this phase, substitution cipher is multiplication mod 255. During the key generation process the care should be taken such that the initial values of Feedback shift Registers should have inverse numbers of multiplicative inverse numbers taken in Encryption process. The outcome of this stage is partially decrypted information from the Cipher text.
The algorithm used in the second phase function transposition cipher uses permutation using a key, depending on two categories.. First Depending on even parity Byte, second depending on odd parity Byte. If the byte is even parity permutation key P1 is used. In case of odd parity permutation key P2 is used. Here we obtain the original information once after Permutation got complemented.

3.3 Example:

Encryption Part
Audio information→Plain text=123 i.e. 01111011
After taking 1's complement= 132 i.e. 10000100

Phase1: Transposition Cipher
Checking Parity: 10000100→Even Parity
Permutation p2 is used because Even Parity
P2=6 4 7 1 2 8 5 3
Now after 1st phase the cipher text is =144 i.e. 10010000

Phase 2: Substitution Cipher
[In the initial stage we using some initial key values of PRNG keys are 2,3,7,8.
No of stages are 4
Feedback shift register is connected as k1 ⊠k2=k5]
Generated Key from PRNG =2
Now Key Generated is 2 is multiplied with the output of Phase1 i.e. 144, (144*2=288 mod255=33) we obtain secure cipher text.
Cipher text after encryption=33

Decryption Part:
Cipher Text=33

Phase 1: Substitution Cipher
[In the initial stage we using some initial key values which are inverse number of encryption side keys. so PRNG keys are 128,64,73,32.
No of stages are 4
Feedback shift register is connected as k1 ⊠k2=k5]
Key generated from PRNG is inverse number of 2 i.e.128 is get multiplied with the cipher text 144 we get,
(128 *33)%255 =144

Phase 2: Transposition Cipher
Checking Parity: 10010000→Even Parity
Permutation P2 used for even Parity.
P2=1 2 3 4 5 6 7 8
Now after Decryption = 132
After taking 1's Complement we obtain =132
We obtain the Plain Text =01111011 ➔ 123

4. RESULTS AND ANALYSIS

The Histogram of original audio signal and corresponding encrypted audio signal is shown in figure 4.1 and figure 4.2. It is clear that the histogram of the encrypted audio signal is nearly uniformly distributed, and significantly different from the histogram of the original audio signal. So, the encrypted audio signal does not provide any clue to

employ any statistical attack on the proposed encryption of audio signal procedure, which makes statistical attacks difficult. These properties tell that the proposed audio signal encryption has high security against statistical attacks**.** The information is split into two parts according to their parities. Thus the operation of faster encryption can be done in parallel. This limits the side channel attack

Histogram for the original Audio signal is shown in the bellow graph.

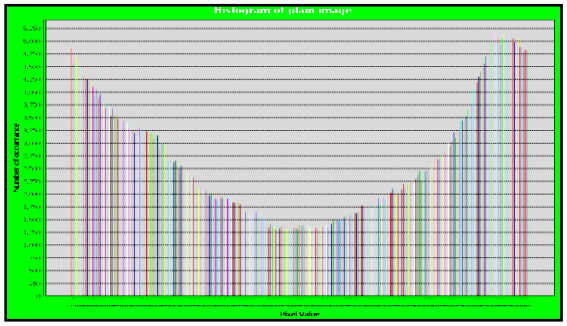

Fig 4.1: Histogram for Plain Audio signal

Cipher text which we got for given input audio signal is uniformly distributed as shown in the below graph.

Fig 4.2.Histogram of Cipher Audio signal showing uniform distribution

Since Histogram what we got from Cipher text is uniform we conclude this system is secure.

Fallowing Table gives Comparison of our proposed cipher system with a known standard cipher system i.e., A5/1.

From the table, proposed system is secure for online application by calculating Entropy, standard deviation and mean absolute difference we can clearly say that the signal has got immunity to attack.

Hence it can be shown that the proposed work has achieved more strength with respect to its application in the field of cryptography

Table4.1 Comparison of our proposed cipher system with a known standard cipher system i.e., A5/1

SL No	Type Of Cipher System	Entropy	Standard Deviation	Mean Absolute Difference
1	Standard A5/1 stream cipher	7.73	1.940032	68.012
2	The proposed cipher system	7.96	2.64	97

5. CONCLUSION

This paper attempts to say that the proposed system is secure for online application by hearing the Audio signal after encryption it clearly say that the signal has got immunity to attack.

At the time this paper is written, only few references available. Audio cryptography still has wide prospect to grow. We are still dreaming for a *reversible* lossless audio compression, which can play major role in future audio cryptography.

REFERENCES

[1]. Mactaggart, M., "*Introduction to cryptography*, Part 2: Symmetric cryptography," 2001, http://www.ibm.com/developerworks/library/scrypt02.html

[2]. Khaled Suwais and Azman Samsudin (university Sains Malasia(USM) Malaysia) *"New classification of existing stream ciphers"*2007

[3].Symmetric Cryptosystems and Symmetric Key Management- Brian A. Carter, Ari Kassin, and Tanja Magoc, September 18, 2007

[4].Neal Koblitz, Alfred J. Menezes, *"A Survey on Public key Cryptosystems"* August 2007, pp 2- 40

[5].Chris Christensen, *"Transposition Ciphers –"* 'Fall 2006 MAT/CSC 483, pp1 to 31.

[6]. Daniel Socek, "*General Access Structures in Audio Cryptography"* Department of Computer Science and Engineering Florida Atlantic University

Boca Raton, Florida 33431.0991Email: dsocek@brain.math.fau.edu

[7]. Kenta Kasai, At.al., "*Multiplicatively Repeated Non-Binary LDPC Codes" Member, IEEE,* and Kohichi Sakaniwa, *Senior Member, IEEE*

[8].Yusuf Adriansyah, "*Simple Audio Cryptography* " 13507120 1,*Program Studi Teknik Informatika Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia* 1 *if17120@students.itb.ac.id*

[9]. Amresh Nikam, Poonam Kapade, Sonali Patil, *"Audio Cryptography-A (2, 2) Secret Sharing for Wave File"* International Journal of Computer Science and Application Issue 2010- ISSN 0974-0767

[10]. "*Non binary audio cryptography***'** Desmedt, Y and Le, TV and Quisquater, JJ (2000) *Non binary audio cryptography.* In: Pfitzmann, A, (ed.) *INFORMATION HIDING, PROCEEDINGS***.** (pp. 478 - 489). SPRINGER-VERLAG BERLIN

[11]. Y. Desmedt, S. Hou, and J. Quisquater, "*Audio and optical cryptography*," Advances in Cryptology - Asiacrypt'98, Lecture Notes in Computer Science, LNCS 1514, pp.392–404, Springer-Verlag, 1998.

[12]. Mao, "Wenbo *Modern Cryptography: Theory & Practice",* Upper Saddle River, NJ: Prentice Hall PTR,2004.

[13] Yusuf Adriansyah, " *Simple Audio Cryptography"*
Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia

[14]. Yvo Desmedt, Tri V. Le and Jean-Jacques Quisquater, *"NonBinary Audio Cryptography"*Department Of Computer Science, Florida State University Fl 32306-4530

[15]. " *Advanced Encryption Standard"*
http://www.axantum.com/axcrypt/etc/About-AES.pdf

[16]. Majid Bakhtiari, Mohd Aizaini Maarof *"An Efficient Stream Cipher Algorithm for Data Encryption"* Department of Computer Science & Information Systems, University Technology Malaysia,City Campus Jalan Semarak, 54100 Kuala Lumpur, Malaysia, pp 248 to 250

[17] .Ganesh Aithal,*" Implementation of Stream Cipher System Based on Representation of Integers In Residue Number System",* Department Of Electronics and Communication National Institute of Technology Karnataka, Srinivasanagr, Suratkal,Mangalore, India.ganeshaithal@gmail.com,978-1-4244-4791-6/10/$25.00_c 2010 IEEE, pp 211 to 213