Encryption of a Binary String Using Music Notes and Graph theory

M. Yamuna [#1], A. Sankar [#2], Siddarth Ravichandran [#3], V. Harish [#4]

VIT University, Vellore, Tamilnadu, India, 632 014

[1] myamuna@vit.ac.in

[2]sankar0509@rediff.com

[3] siddusathu@yahoo.co.in

[4] harisankar004@gmail.com

***Abstract*— Secured communication in networks is critical because the communication signals are openly available as they propagate. Efficient encryption mechanism is required to assure confidentiality, integrity and authentication of transmitted data. In this paper, we propose encryption of any binary string using cipher chain blocking method. Any musical note consists of seven basic keys. We use a musical note in this method. The degree sequence of the graph constructed from any music note is used as the key.**

Keyword- Music note, Binary string, Degree sequence.

I. Introduction

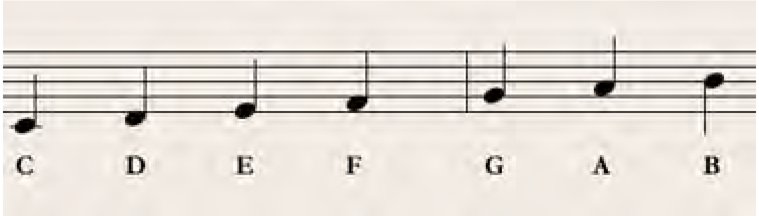
The word cryptography refers to the science and art of transforming messages to make them secure and immune to attacks. Basically, it is based on the concept of abstract algebra. Network security is mostly achieved through the use of cryptography. More generally, it is about constructing and analysing protocols that overcome the influence of adversaries and are related to various aspects of information security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Graph Theory is a recent concept that has been successfully integrated to provide stronger cryptographic algorithms which are hard to break by any modern day software or adversary. It is emerging as a new tool for ethical hackers, government agencies, and other security-related organizations to use in encryption and communication of highly sophisticated data across domains. Because of its broad applicability in this field, graph theory technology is likely to withstand future developments.

II. Preliminary Note

In this section, we provide the details of music notes, the propagating cipher block chaining (PCBC) method and the graph theory required for encryption of a binary string using the proposed encryption scheme.

A. Musical Notation

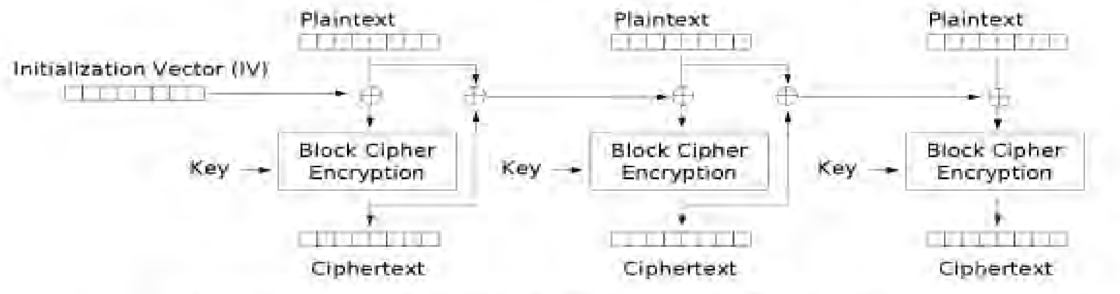
Musical notation is the representation of sound with symbols. Any music can be represented using these symbols. The basic notes in music are C, D, E, F, G, A and B. A pause in music is represented by -.
The following diagram represents the musical notation from C to B. [2]



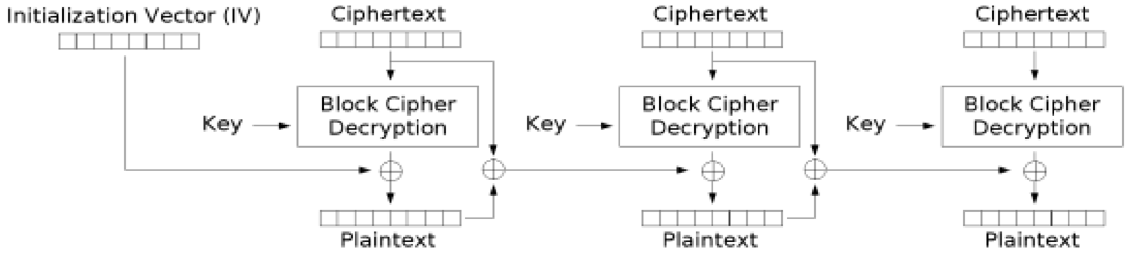
B. Propagating Cipher Block Chaining (PCBC)

The mode of operation in cryptography is the procedure of enabling repeated and secure use of a block cipher under a single key. A block cipher by itself allows encryption only of a single data block of the cipher's block length. When targeting a variable-length message, the data must first be partitioned into separate cipher blocks. Typically, the last block must also be extended to match the cipher's block length using a suitable padding scheme. A mode of operation describes the process of encrypting each of these blocks, and generally uses randomization based on an additional input value, often called an initialization vector, to allow safe execution. An initialization vector (IV) is a block of bits that is used by several modes to randomize the encryption and hence to produce distinct cipher texts even if the same plaintext is encrypted multiple times without the need for a slower re-keying process. The IV has different security requirements than a key, and so the IV usually does not need to be confidential. However, in most cases, it is important that an initialization vector is never reused under the same key. A block cipher works on units of a fixed size (known as a block size), but messages come in a variety of lengths. So some modes namely (ECB and CBC) require that the final block be padded before encryption. Several padding schemes exist. The simplest is to add null bytes to the plaintext to bring its length up to a multiple of the block size, but care must be taken such that the original length of the plaintext can be recovered.

The propagating cipher-block chaining or plaintext cipher-block chaining mode was designed to cause small changes in the cipher text to propagate indefinitely while decrypting, as well as while encrypting [3].



Propagating Cipher Block Chaining (PCBC) mode encryption



Propagating Cipher Block Chaining (PCBC) mode decryption

Encryption and decryption algorithms are as follows:

$$C_i = E_K(P_i \oplus P_{i-1} \oplus C_{i-1}), P_0 \oplus C_0 = IV$$
$$P_i = D_K(C_i) \oplus P_{i-1} \oplus C_{i-1}, P_0 \oplus C_0 = IV$$

C. Graph

A graph G = < G, V, ϕ > consists of a nonempty set V called the set of vertices of the graph, E is said to the set of edges of the graph, and ϕ is a mapping from the set of edges E to a set of ordered pair of $V \times V$, which is called a directed edge of G.

For a directed graph G in which V = { v_1, v_2,…, v_n } the nodes are assumed to be ordered from v_1 to v_n. An n x n matrix A whose elements a_{ij} are given by

$$a_{ij} = \begin{cases} 1 & \text{if } < v_i, v_j > \in E \\ 0 & \text{otherwise} \end{cases}$$

is called the adjacency matrix of the graph G [1].

III. Proposed Encryption Scheme

A. Method 1 (Improved PCBC method)

We improve the PCBC method. In this method, the binary string to be encrypted should be a multiple of 8. To enable this we prefix the missing values by 0s. We also attach one more string of length 8 to indicate the number of 0s prefixed. The last three bits will be the binary conversion of the number of 0s prefixed, that is if the last 8 entries in the binary string to be encrypted is 00000000, then it means the original string to be encrypted is a multiple of 8. So every binary string to be encoded is prefixed by a minimum of 00000000.

We introduce a new way of choosing the Initialization vector and the Key E_k.

To convert the sheet music to binary digital form, consisting of only 0s and 1s, we use the following substitution.

TABLE I
Binary Conversion

Music note	Binary
C	000
D	001
E	010
F	011
G	100
A	101
B	110
-	111

1) *Initialization Vector (C_0)*

We choose any music note of our choice. Using the binary conversion table we obtain the binary conversion of first four bits of the string. This is a binary string S of length 12. The first eight bits of S are taken as the IV.

2) *Shift*

The last four bits of the string S is our shift.

3) *Key (E_k)*

We first construct a graph G as follows

The vertices of G are the eight music notes C, D, E, F, G, A, B, Rest. The edges are constructed following the music notes. We draw an edge from each music note to the next music note in the order they appear in our chosen music string. If the music note is EDDA, then there is an edge from E to D, D to D … A to D. We also assign weights to the edges of the graph. These edge weights represent the number of edges between the corresponding vertices. For example, the graph corresponding to EDDDAD is as seen in Fig 1.

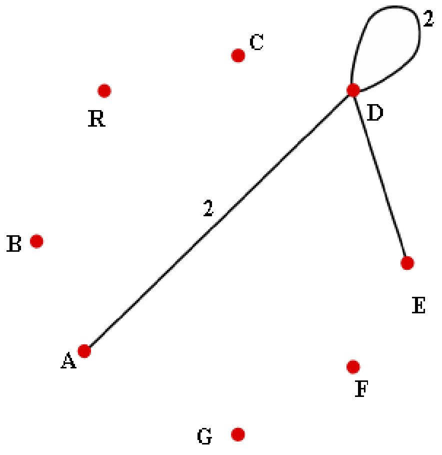


Fig. 1. Graph Corresponding to EDDDAD

The degree of the each vertex form C – Rest is listed, that is we have a sequence of integers of length 8 say S = $a_1, a_2, \ldots, a_8$. We generate a binary string S1 of length 8 as follows.

$$S1 = \begin{cases} 1 & \text{if } a_i \text{ is odd} \\ 1 & \text{if } a_i \text{ is even}, r = \text{odd} \\ 0 & \text{if } a_i \text{ is even}, r = \text{even} \end{cases}$$

where r is the quotient when a_i is divided by 2.

For the graph in Fig 1, the degree sequence is 00100100, and the resulting string S1 is 00100100. This resulting binary string S1 is our E_k.

Use of Shift

The value of E_k calculated is used for encryption of the first block. The shift value is now converted into its numerical conversion, which would be a value ranging from 0 to 7. Say the converted value of the shift is p, then each position of E_k is shifted by p place. Say if E_k is 10110101 and shift value is 2, then the new E_k value for block two is 01101101. For each block different E_k values are calculated.

Encryption Algorithm

Step 1 Determine the IV (C_0), Shift and E_k as explained.

Step 2 Set P1 as the first eight bits of the binary string to be encrypted.

Step 3 The first block is encrypted using $C_i = E_k (P_i P_{i-1} \oplus C_{i-1})$, P_0C_0 = IV.

Step 4 For block 2 the new value of E_k is calculated using the shift for the problem as explained.

Step 5 Continue the iteration till all blocks are encrypted.

Step 6 Send to the receiver

B. Method 2 (Improved PCBC using adjacency matrix)

This method is similar to method 1 except that we modify the way E_k is calculated. We construct the graph as described in method 1, and then we create the adjacency matrix of G, which is of order 8 x 8. Each row of the adjacency matrix will be used as E_k. If the number of iterations exceed 8, then we cycle the rows again from row one till all the iterations are complete.

Encryption Algorithm

Step 1 Determine the IV (C_0), Shift and E_k as explained.

Step 2 Set P1 as the first eight bits of the binary string to be encrypted.

Step 3 The first block is encrypted using $C_i = E_k (P_i P_{i-1} \oplus C_{i-1})$, P_0C_0 = IV.

Step 4 For block 2 the new value of E_k is the second row of the adjacency matrix A.

Step 5 Continue the iteration till all blocks are encrypted (cycle the rows of A if needed).

Step 6 Send to the receiver.

IV. ILLUSTRATION

In this section we provide illustration of how the proposed methods work

Let S: 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 1 0 1 0 0 1 1 0 1 1 1 1 1 0 1 0 1 0 1 1 1 0 1 0 0 1 1 1 0 1 1 0 1 be the binary string to be encrypted.

Method 1

Padding

Splitting S into segments each of k = 8 bits

10110100 10110101 01001101 11110101 01110100 11101101. Since length of the string is a multiple of 8, the string is padded by 00000000. Our P1 is hence 10110100.

IV

Let us choose M to be the musical note of jingle bells.

|EEE-|EEE-|EGCD|E---|FFFF|FEEE|EDDD|ED--|EEE-|EEE-|EGCD|E---|

The first four note of jingle bell is EEE-The equivalent binary conversion from the binary conversion table 1 is 010010010111, so that IV = 01001001 and Shift = 0111.

E_k

Our jingle bell note is

EEE-EEE-EGCDE---FFFFFEEEEDDED---EEE-EEE-EGCDE---FFFFFEEEGGFDC---

The equivalent graph constructed as explained in the method is given in Fig. 2.

From the graph in Fig 2 the degree sequence of the vertices from C to R is 6, 12, 47, 22, 8, 0, 0, 32. Converting it into a binary string as explained we get E_k = 10110000.

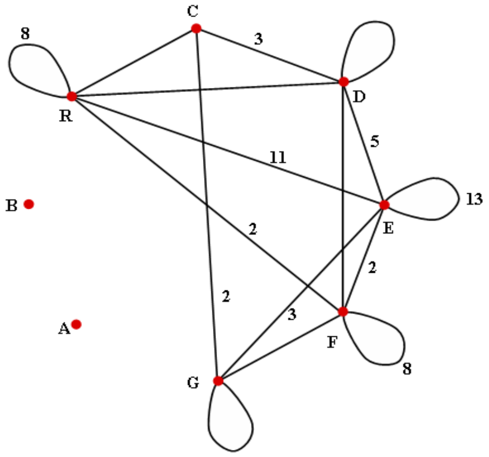


Fig. 2. Graph Equivalent to Jingle Bells

- We have 10110100 ⊕ 01001001 = 11111101
- E_k function is now performed, 11111101 ⊕ 10110000 = 01001101 (this is the cipher text C_1)
- Xor $P_1$and C_1, 01001101 ⊕ 10110100 = 11111001 (this will act as a key for the next iteration).
- now take the 2nd block, 10110101 ⊕ 11111001 = 01001100
- There will be a right shift of 7 (shift = 0111) spaces in the E_k function string. Thus the new key in E_k becomes 01100001.
- E_k function: 01001100 ⊕ 01100001 = 00101101 (the cipher text C_2)
- C_2 ⊕ P_2 = 00101101 ⊕ 10110101 = 10011000 (the key for the next iteration)
- 01001101 ⊕ 10011000 = 11010101
- 11010101 ⊕ 11000010 = 00010111 (C_3)
- 01001101 ⊕ 00010111 = 01000111 (P_3 xor C_3)
- 11110101 ⊕ 01000111 = 10110010
- 10110010 ⊕ 10000101 = 00110111 (C_4)
- 11110101 ⊕ 00110111 = 11000010
- 01110100 ⊕ 11000010 = 10110110
- 10110110 ⊕ 00001011 = 10111101 (C_5)
- 10111101 ⊕ 01110100 = 11001001
- 00000000 ⊕ 11001001 = 11001001
- 11001001 ⊕ 00010110 = 11011111 (C_{pad})
- The concatenated message that is sent is: 0100110100101101000101110011011110111101110111011111

Method 2

Padding and IV value is as in method 1. The corresponding directed graph is given in Fig 3.

In the digraph G in Fig 3 an edge represents there is atleast one edge between the corresponding vertices. Bidirectional edge between x and y represents that there is atleast one edge directed from x to y and y to x.

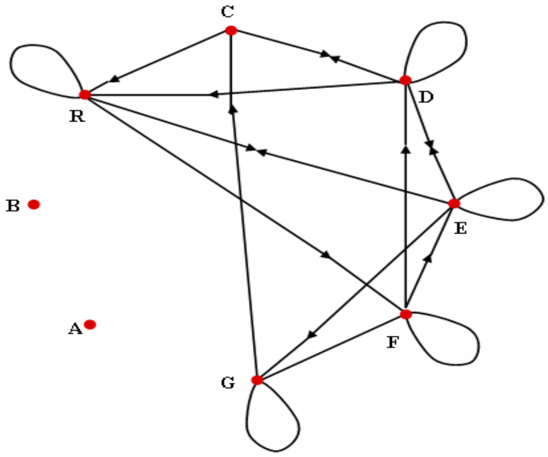


Fig. 3. Directed Graph for Jingle Bells

The adjacency matrix corresponding to the graph in Fig 3 is

$$A=\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Each row represents our function Ek to be used in the algorithm.

10110100 ⊕ 01001001 = 11111101 ($P_1 \oplus IV$)
11111101 ⊕ 01000001 = 01111100 ($P_1 \oplus IV \oplus E_k = C_1$)
01111100 ⊕ 10110100 = 11001000 ($P_1 \oplus C_1$)
10110100 ⊕ 11001000 = 01111100 ($P_1 \oplus C_1 \oplus P_2$)
01111100 ⊕ 11100001 = 10011101 ($P_1 \oplus C_1 \oplus P_2 \oplus$ (row 2 of E_k) $= C_2$)
10011101 ⊕ 10110100 = 00101001 ($P_2 \oplus C_2$)
01001101 ⊕ 00101001 = 01100100 ($P_3 \oplus P_2 \oplus C_2$)
01100100 ⊕ 01101001 = 00001101 ($P_3 \oplus P_2 \oplus C_2 \oplus$ row 3 of $E_k = C_3$)
01001101 ⊕ 00001101 = 01000000 ($P_3 \oplus C_3$)

Encrypt the padding

00000000 ⊕ 01000000 = 01000000 (pad $\oplus P_3 \oplus C_3$)
01000000 ⊕ 01110000 = 01110000 (pad $\oplus P_3 \oplus C_3 \oplus$ row 4 of the $E_k = C_4$)

So we send 01111100100111010000110101110000 to the receiver.

V. Conclusion

Two methods had been proposed and demonstrated, which is based upon a reference sequence known only to the sender and the receiver. This reference sequence can be selected from website for music notes. PCBC method is merged with music notes, that provides more security, flexibility with less complexity. These methods are based on the selection of the music notes and hence the graphs constructed. This improves the security of the regular PCBC. So the proposed method are more secured than the regular PCBC.

References

[1] J. P. Tremblay, R. Manohar, Discrete Mathematical Structures with Applications to Computer Science, Tata Mc Graw Hill, 38th print 2010.
[2] http://www.readsheetmusic.info/readingmusic.shtml.
[3] http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation#Propagating_cipher-_.
[4] https://class.coursera.org/crypto-2012-003/lecture/index.
[5] http://staff.neu.edu.tr/~fahri/cryptography_Chapter_6.pdf.
[6] http://www.music-for-music-teachers.com/jingle-bells-2.html.