International Journal of PharmTech Research
CODEN (USA): IJPRIF, ISSN: 0974-4304
Vol.7, No.1, pp 85-89, 2014-2015

Cryptography using A Pair of Dice

V.M.Chandrasekaran[1], A. Manimaran[2], Akhil Ranjan[3,*]

[1, 2]School of Advanced Sciences,VIT University, Vellore-632014, India.
[3]School of Computing Science and Engineering,VIT University, Vellore-632014 India.

Abstract: Communication signals are propagated and they are open. Various methods are proposed for smart and secured transmission of messages. In this paper we propose a method of encryption of any message using a pair of dice.
Keywords: Encryption, Decryption, dice, LSB (least significant byte) and MSB(most significant byte)

1. Introduction

Communication has become a very important aspect in today's life. As the rapid development of network and multimedia technologies, the digital worldly technologies has been applied to real world applications and the security has become a very key importance regarding this issue. There are many ways to secure the data, one such way to secure the information is cryptography.

The word cryptography refers to the science of transforming messages to make them secure and immune to attacks. Cryptography allows a process in a way that the authorized person or party can read it. We have several encryption and decryption algorithms for encrypting the data at sender end and decrypting the same at receiver side ensuring secure data transfer. (1)

2. Preliminaries

In this section we provide the details of pair of dice for encryption of a binary string using the proposed encryption scheme. As the proposed encryption scheme requires the user to know the conversion of decimal to binary and the decryption requires the users to know the conversion of binary to decimal.

2.1 Decimal to Binary

Encryption can be done by using the proposed scheme by converting decimal number to binary number

<u>**Steps**</u>:

1. Start by writing a column of numbers. On the first row, write down the decimal number you wish to convert.
2. In the next row, write the value above it divided by 2. Write only the integer portion of the number, ignoring any fractional part. Repeat this step until the value written is 1.
3. Start a second column of number, to the right of the first. In this column, write a 1 if the number beside it is odd or a zero if the number beside it is even. Write down a column of 1's and 0's corresponding to each number in the first column.
4. Starting from the bottom of the second column and working upward, write down the 1's and 0's, from left to right. The bottom digit (1 or 0) is written first. Then the second from bottom is written, and so on for each binary digit. The resulting digits are the binary representation of the number you started with.

Example 1: Convert the number 46 to binary

1. Start by writing down the number as a start of a new column

46

2. Fill out the rest of the column by dividing the number above it by 2. Write only the integer portion of each value, and use this integer value when computing the one below it. Continue dividing until the last value written is 1.

46
23
11
5
2
1

3. Write a second column of values next to the first, as a column of binary 1's and 0's. Write a 1 if the number beside it is odd, or a 0 if even.

46	
23	1
11	1
5	1
2	0
1	1

4. Read the second column from bottom to top, writing out the binary value from left to right:

101110

2.2. Binary number to Decimal number

Decryption can be done by using the proposed scheme by converting binary number to decimal number **(2)**

Step 1: First, we will have to make a tabular column with three rows R1,R2,R3 and 8 columns C0,C1,C2,C3,C4,C5,C6,C7 as shown below

C7 C6 C5 C4 C3 C2 C1 C0

R1								
R2								
R3								

Here, each element of the table will hold one bit and there are 8 columns which means 8 bits in one row (i.e. 1 byte). In this shortcut the maximum value that we cover is (255) in decimal number system and we can extend it.

Step 2: Now insert the values into the first row of the table (R1) as shown below

	C7	C6	C5	C4	C3	C2	C1	C0
R1	128	64	32	16	8	4	2	1
R2								
R3								

It is simply the values of powers of 2 ranging from (2^0 to 2^7 starting from C0 to C7 respectively). The following table will give the exact idea how the values are obtained.

Binary	Decimal
2^0	1
2^1	2
2^2	4
2^3	8
2^4	16
2^5	32
2^6	64
2^7	128

Step 3 : The given binary number that needs to be converted to decimal is inserted bit by bit from **LSB** to **MSB** into third row (**R2**) starting from C0 to C7 respectively.

Step 4: Multiply each element from the first row (**R1**) with the corresponding value in the second row (**R2**) and put the product into the third row (**R3**) in the same column.

Step 5: Now add the individual columns of third row and the sum gives the decimal equivalent of the binary number.

Example 1: Convert $(1001)_2$ to $(?)_{10}$

Step 1: Draw the tabular column with the values

	C7	C6	C5	C4	C3	C2	C1	C0
R1	128	64	32	16	8	4	2	1
R2								
R3								

Step 2: Insert given binary number into 2nd row as stated in **step 3**

	C7	C6	C5	C4	C3	C2	C1	C0
R1	128	64	32	16	8	4	2	1
R2					1	0	0	1
R3								

The empty columns can be ignored

Step 3: Multiply R1 and R2 with the corresponding elements and put the product in **R3**

	C7	C6	C5	C4	C3	C2	C1	C0
R1	128	64	32	16	8	4	2	1
R2					1	0	0	1
R3					8	0	0	1

Step 4: Now add the individual elements of third row **R3,** this sum gives the decimal equivalent of the given binary number as illustrated

$8 + 0 + 0 + 1 = (9)_{10}$

2.3. Notations of Dice

When rolling two dice, distinguish between them in some way that is, a first one and second one and a left and a right. Let (a, b) denote the possible outcome of rolling the two dice, with 'a' be the number on the top of the first die and 'b' be the number on the top of the second die. Note that each of 'a' and 'b' can be any of the integers from 1 through 6. Here is a listing of all the joint possibilities for (a, b)

(1,1) (1,2) (1,3) (1,4) (1,5) (1,6)

(2,1) (2,2) (2,3) (2,4) (2,5) (2,6)

(3,1) (3,2) (3,3) (3,4) (3,5) (3,6)

(4,1) (4,2) (4,3) (4,4) (4,5) (4,6)

(5,1) (5,2) (5,3) (5,4) (5,5) (5,6)

(6,1) (6,2) (6,3) (6,4) (6,5) (6,6)

There are 36 possibilities for (a, b). This total number of possibilities can be obtained from **the multiplication principle** such that there are 6 possibilities for 'a' and for each outcome for 'a', there are 6 possibilities for 'b'. So, the total number of joint outcomes (a, b) is 6 times 6 which is 36. The set of all possible outcomes for (a, b) is called **the sample space** of this probability experiment. **(3)**

3. Proposed Encryption Scheme

Here we have proposed a method of encryption of any message using a pair of dice. We roll the pair of dice and we obtain a joint outcome in which we encrypt using a binary string using the proposed encryption scheme. We are employing this since the decryption of the code will be very lengthy as it will be very cumbersome to decode a seven digit binary string.

Below is the list of the joint outcomes which we represent accordingly

$(1,1) \rightarrow A$ $(1,2) \rightarrow B$ $(1,3) \rightarrow C$ $(1,4) \rightarrow D$ $(1,5) \rightarrow E$ $(1,6) \rightarrow F$

$(2,1) \rightarrow G$ $(2,2) \rightarrow H$ $(2,3) \rightarrow I$ $(2,4) \rightarrow J$ $(2,5) \rightarrow K$ $(2,6) \rightarrow L$

$(3,1) \rightarrow M$ $(3,2) \rightarrow N$ $(3,3) \rightarrow O$ $(3,4) \rightarrow P$ $(3,5) \rightarrow Q$ $(3,6) \rightarrow R$

$(4,1) \rightarrow S$ $(4,2) \rightarrow T$ $(4,3) \rightarrow U$ $(4,4) \rightarrow V$ $(4,5) \rightarrow W$ $(4,6) \rightarrow X$

$(5,1) \to Y$ $(5,2) \to Z$ $(5,3) \to \mathbf{0}$ $(5,4) \to \mathbf{1}$ $(5,5) \to \mathbf{2}$ $(5,6) \to \mathbf{3}$
$(6,1) \to \mathbf{4}$ $(6,2) \to \mathbf{5}$ $(6,3) \to \mathbf{6}$ $(6,4) \to \mathbf{7}$ $(6,5) \to \mathbf{8}$ $(6,6) \to \mathbf{9}$

Then we convert the joint outcomes into the digits then to the seven bit binary digit.

11 → 0001011 **12** → 0001100 **13**→ 0001101 **14** → 0001110 **15**→ 0001111 **16**→ 0010000
21 → 0010101 **22**→ 0010110 **23**→ 0010111 **24**→ 0011000 **25**→ 0011001 **26**→ 0011010
3 1→ 0011111 **32**→ 0100000 **33**→ 0100001 **34**→ 0100010 **35**→ 0100011 **36**→ 0100100
41→ 0101001 **42**→ 0101010 **43**→ 0101011 **44**→ 0101100 **45**→ 0101101 **46**→ 0101110
51 → 0110011 **52**→ 0110100 **53**→ 0110101 **54**→ 0110110 **55**→ 0110111 **56**→ 0111000
61→ 0111101 **62**→ 0111110 **63**→ 0111111 **64**→ 1000000 **65**→ 1000001 **66**→ 1000010

To increase the difficulty we can include blank spaces which can be 0000000

3.1 Example

Let's consider an example for encrypting

GLYCOMET GP2

G – 21 – 0010101 ,L – 26 – 0011010, Y- 51 – 0110011, C- 13- 0001100, O-33- 0100000,
M-31- 0011111, E-15- 0001111, T -42- 0101001, G-21- 0010101, P-34- 0100010, 2-55- 0110100

The Code for GLYCOMET GP2 will be

0010101 0011010 0110011 0001100 0100000 0011111 0001111 0101001 0000000 0010101 0100010 0000000 0110100

3.2 Example

Let's now decrypt a given code as an example

0100010 0001011 0100100 0001011 0001101 0001111 0101010 0001011 0011111 0100001 0011010

Now converting the given binary code into the joint outcome

34 11 36 11 13 15 42 11 31 33 26

Now converting the joint outcomes into alphabets **Paracetamol**

4. Conclusion:

In this paper, we considered the outcomes of a pair of dice and we converted the outcomes into the respective characters and digits. These joint outcomes are modified into binary codes. We have encrypted the data and the receiver will decrypt the message by converting the binary codes into numbers and characters. In future we can explore these concepts.

References:

1. http://www.webopedia.com/TERM/C/cryptography.html.
2. http://www.schoolelectronic.com/2012/01/shortcut-for-converting-binary-to.html3.
3. Tremblay J. P, Manohar. R. Discrete Mathematical Structures with Applications to Computer Science. Tata Mc Graw Hill. 38th print 2010.

*****