ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

ENCRYPTION AND DECRYPTION USING ALGEBRAIC CHESS NOTATIONS

A. Manimaran[1,*], V. M. Chandrasekaran[2], Aayush Gupta[3], Ritik Porwal[4]
School of Advanced Sciences, VIT University, Vellore-632014[1,2]
School of Information Technology, VIT University, Vellore-632014[3]
Email: marans2011@gmail.com

Received on: 18.10.2016 *Accepted on: 11.11.2016*

Abstract:

Propagation of communication signal is an open medium process. Various methods are proposed for securing the transmission of messages in communication process. Cryptography provides us with a specific form or key by which the corresponding person or receiver could only retrieve the message transferred. There are several encryption and decryption algorithms for encrypting the data at sending edge and decrypting the encrypted data at receiver edge ensuring the secure data communication. Decryption is the reverse process to encryption. In this paper we propose a method of encryption of any message using algebraic chess notation or chessboard mapping.

Keywords: Encryption, Decryption, Chessboard, Literal, ASCII, numerals, index

1. Introduction

Communication is one of the basic necessity in today's world. Due to the rapid development of network and multimedia technologies, security of the messages communicated has a very key importance and require a secure framework for transfer purpose. One of the greatest challenge posing in today's techniques is the static cryptographic code, as mentioned by authors Manimaran et al. [1]. The authors Obaida et al. [4] enhanced the security goals by maintaining the security on the communication channels thereby making it difficult for attacker to predicate a pattern as well as speed of the encryption / decryption scheme. Encryption is the most effective way to achieve data security. This process achieves an effective role in hiding the contents of the message, because the original information can only be recovered through the description process [5].

There are several ways to transfer the data in secure and reliable mode, one such way to secure the information in communication is using cryptography. Cryptography refers to the science of transfiguring messages to make them secure

and invulnerable to hacking or outbreaks. In 1999 Zimmerman [6] described the detailed concepts of cryptography. The main motto of encryption is to hide the information from third parties for viewing [7]. The authors Manish et al. [3] mentioned that in encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable cipher text. The authors Chandrasekaran et al. [2], discussed about cryptography concept using pair of dice. They considered sample space of two dice and converted binary to decimal and vice versa for giving the concepts in detail. This paper is structured as follows, encrypting and decrypting data using a standard notation called algebraic chess notation, the columns (called files) are labeled by the letters *a* to *h* from left to right from the white player's point of view, and the rows (called ranks) by the numbers 1 to 8, with 1 being closest to the white player [8].

2. Preliminaries

In this section we use the algebraic chess notation for the encryption of binary string using the proposed encryption scheme. As this scheme requires the user to know the addressing of squares on a chess board and ASCII representation of the input for encryption and decryption of data.

2.1 ASCII conversion

ASCII table provides us with the binary values for several alphanumeric characters comprising alphabets (A to Z, a to z, 0 to 9 and special characters)

Binary	Character	Binary	Character	Binary	Character	Binary	Character
00000000	NUL	00100000	SP	01000000	@	01100000	`
00000001	SOH	00100001	!	01000001	A	01100001	a
00000010	STX	00100010	"	01000010	B	01100010	b
00000011	ETX	00100011	#	01000011	C	01100011	c
00000100	EOT	00100100	$	01000100	D	01100100	d
00000101	ENQ	00100101	%	01000101	E	01100101	e
00000110	ACK	00100110	&	01000110	F	01100110	f
00000111	BEL	00100111	'	01000111	G	01100111	g
00001000	BS	00101000	(	01001000	H	01101000	h
00001001	HT	00101001	)	01001001	I	01101001	i
00001010	LF	00101010	*	01001010	J	01101010	j
00001011	VT	00101011	+	01001011	K	01101011	k
00001100	FF	00101100	,	01001100	L	01101100	l
00001101	CR	00101101	-	01001101	M	01101101	m
00001110	SO	00101110	.	01001110	N	01101110	n
00001111	SI	00101111	/	01001111	O	01101111	o
00010000	DLE	00110000	0	01010000	P	01110000	p
00010001	DC1	00110001	1	01010001	Q	01110001	q
00010010	DC2	00110010	2	01010010	R	01110010	r
00010011	DC3	00110011	3	01010011	S	01110011	s
00010100	DC4	00110100	4	01010100	T	01110100	t
00010101	NAK	00110101	5	01010101	U	01110101	u
00010110	SYN	00110110	6	01010110	V	01110110	v
00010111	ETB	00110111	7	01010111	W	01110111	w
00011000	CAN	00111000	8	01011000	X	01111000	x
00011001	EM	00111001	9	01011001	Y	01111001	y
00011010	SUB	00111010	:	01011010	Z	01111010	z
00011011	ESC	00111011	;	01011011	[	01111011	{
00011100	FS	00111100	<	01011100	\	01111100	|
00011101	GS	00111101	=	01011101	]	01111101	}
00011110	RS	00111110	>	01011110	^	01111110	~
00011111	US	00111111	?	01011111	_	01111111	DEL

For the encryption and the decryption process of string data we use the ASCII values for the capital, small alphabets, numerical digits and the special characters as in the given table.

2.2 Algebraic chess notation: Chess board mapping

A chess board is an 8 × 8 square, hence comprising 64 squares. These square further have alternating black and white color resulting in 32 black tiles and 32 white tiles.

8	a8	b8	c8	d8	e8	f8	g8	h8
7	a7	b7	c7	d7	e7	f7	g7	h7
6	a6	b6	c6	d6	e6	f6	g6	h6
5	a5	b5	c5	d5	e5	f5	g5	h5
4	a4	b4	c4	d4	e4	f4	g4	h4
3	a3	b3	c3	d3	e3	f3	g3	h3
2	a2	b2	c2	d2	e2	f2	g2	h2
1	a1	b1	c1	d1	e1	f1	g1	h1
	a	b	c	d	e	f	g	h

According to the given mapping of the chess board each square of the board possess a unique address resulting in 64 different locations with unique addresses. Hence according to the indexes of the chess board we can derive a specific address for each of the location.

3. Proposed Encryption Scheme:

Here we propose a method of encryption of any message using a chessboard.

In this methodology we are assigning each of the alphabet and numerals with a particular square of chessboard

8	A	B	C	D	E	F	G	H
7	I	J	K	L	M	N	O	P
6	Q	R	S	T	U	V	W	X
5	Y	Z		0	1	2	3	4
4	5	6	7	8	9		a	B

3	c	d	e	f	g	h	i	J
2	k	l	m	n	o	p	q	R
1	s	t	u	v	w	x	y	Z
	a	**b**	**c**	**d**	**e**	**f**	**g**	**H**

3.1 Process of encryption:

1. At first, write the corresponding address of the alphabets of the input string as in the given above table.
2. Find if the tile of the concerned address is Black or white.
3. While writing the values in binary, firstly the alphabetical part of the address for the alphabetical data is split into two sections (4-Bit each)
4. While writing the code we have 4 parts,

- 1st and the 4th part will contain the value of the above split section representing the alphabetical part of the address of corresponding alphabetical data input.
- 2nd part will contain value 1111 for if the tile is Black and 0000 if the tile is White.
- 3rd part will contain the binary value of the numerical part of the address of the data input.

5. If the tile is black then the front and back parts are interchanged while writing (i.e. first 4 bits will be written in the 4th part and the last 4 bits are written in the 1st part) else if the tile is found to be white in color then the two split parts are written in the same sense (i.e. first 4 bits are written in 1st part and the last 4 bits are written in the 4th part).

Note: In case of special characters, the 1st and the 2nd part will contain the entire binary form of the ASCII value of that special character. The 3rd and the 4th part will contain sets of 0000.

Example:

The message to be encrypted is "Rat$"

On comparing each character with the chessboard, the following values are assigned to the letters

R – 3B (lies on white tile)

a – 5G (lies on black tile)

t – 8B (lies on black tile)

As for the special character, it will be converted directly.

R – (0011)(0100 0010)(0000) = 0100 0000 0011 0010

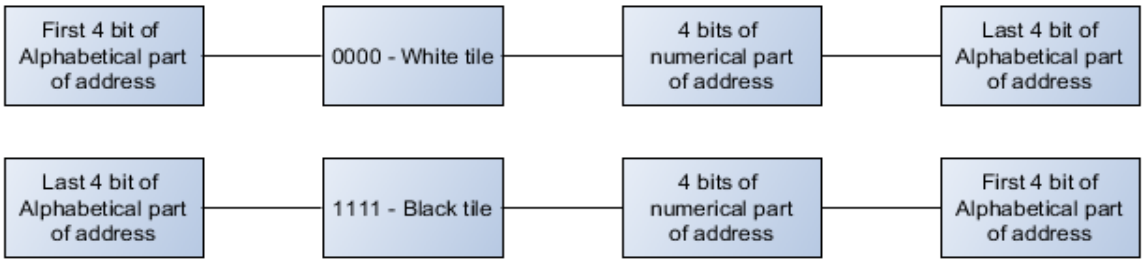
a – (0101)(0100 0111)(1111) = 0111 1111 0101 0100

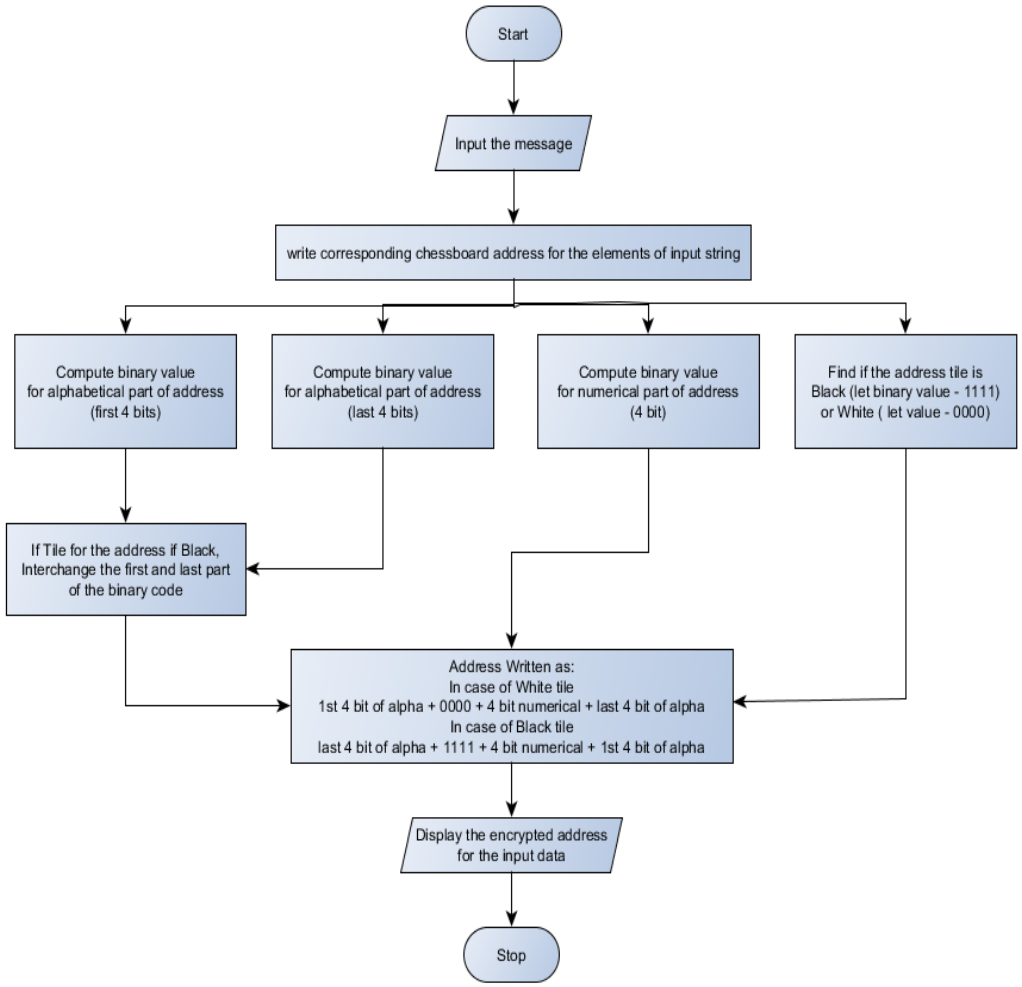
t – (1000)(0100 0010)(1111) = 0010 1111 1000 0100

$ – (00100100)(00000000) =0010 0100 0000 0000

Thus, the encrypted message:

0100000000110010011111110101010000101111100001000010111110000100





1. **Process of Decryption:**

1. Read the Encrypted message in binary digits.
2. Divide Data into sections of 16 - Bits.
3. Further divide these sections into 4 bits units.
4. If the 2nd unit is 1111 then swap the 1st and the 4th unit.
5. Write the alphabetical part of the address for message literal by the combined binary value of 1st and 4th unit.
6. Write the numerical part of address for the message literal by the 4 bit binary value in the 3rd unit.
7. By the obtained address retrieve the corresponding data using the layout of chessboard key proposed under the scheme.

Note: If the 3rd segment is 0000, then the character is a special character, further which we have to only consider the 1st and the 2nd part which when converted to ASCII value will give the special character.

Example:

The encrypted message received is as follows:

0100000000110010011111110101010000101111100001000010111110000100

Let us try to decrypt it. Firstly, groups of 16bits are formed and then divide the groups into 4 parts of 4 bits each

(0100 0000 0011 0010) (0111 1111 0101 0100) (0010 1111 1000 0100) (0010 0100 0000 0000)

0100 0000 0011 0010 – 2nd segment is 0000, meaning that it lies on a white tile and hence no swapping is required

R – 3G

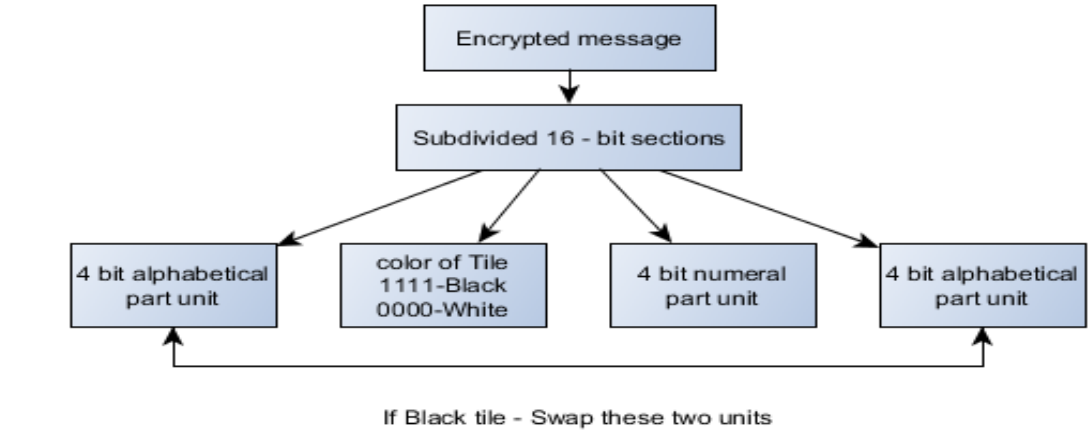
0111 1111 0101 0100 – 2nd segment is 1111, meaning that it lies on black tile and hence 1st and 4th segment will exchange

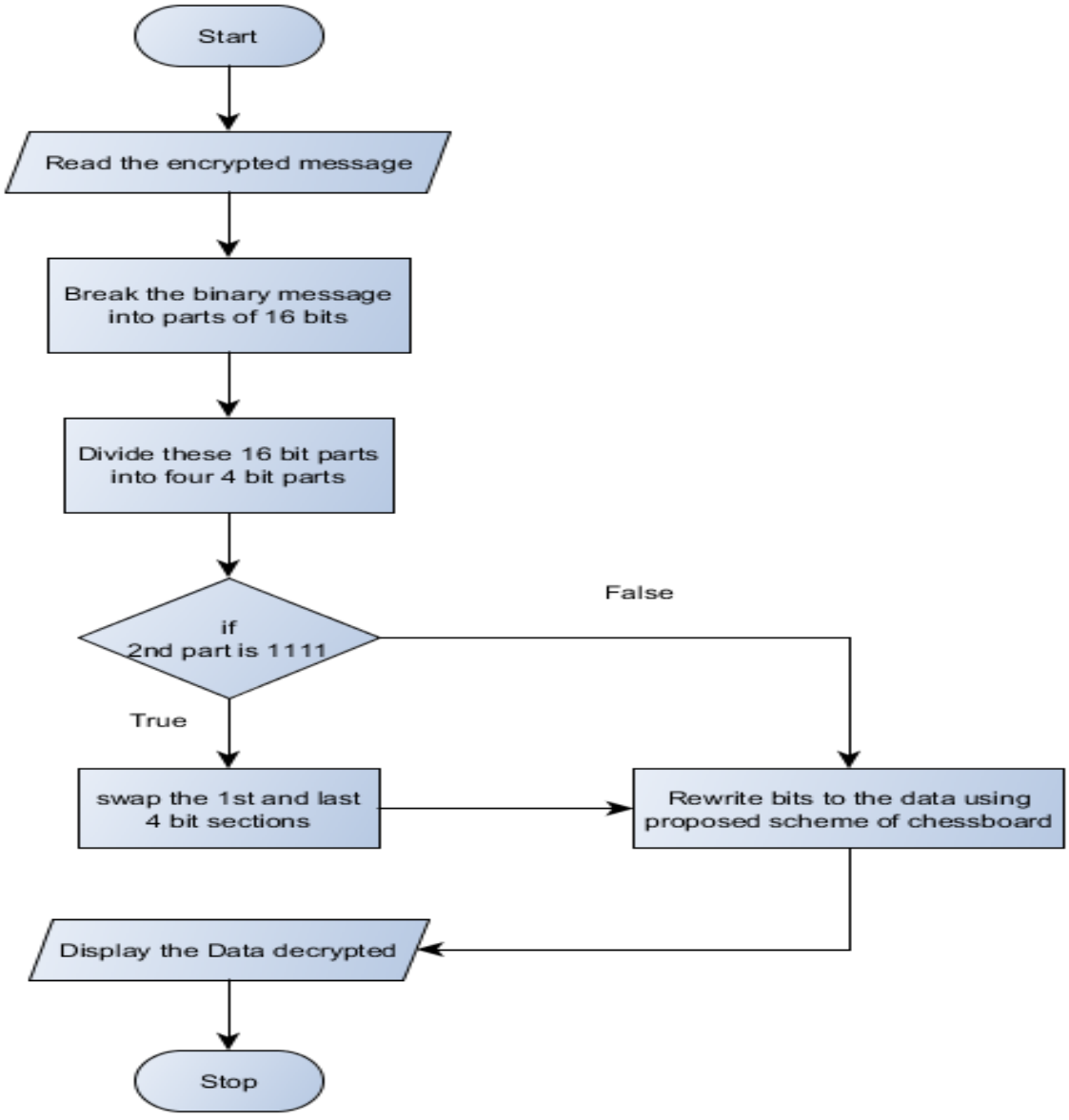
Thus, 0100 1111 0101 0111 is the corrected data

a – 5G

Similarly, t – 8B will be calculated

Now, 0010 0100 0000 0000 has 3rd part as 0000, which means that the character is a special character. Thus, 00100100 - $ and the decrypted is: “Rat$”;





4. Conclusion:

In this paper we considered the chessboard layout and used the addresses of squares. These provided us with 64 unique locations for all the literals in which input message can be given (i.e. A to Z, a to z, 0 to 9). Hence we can encrypt the

data and the receiver will decrypt the message by converting the sections of data from binary to corresponding numbers and characters according to the given unique keys.

References:

1. A. Manimaran, V. M. Chandrasekaran, Archit, Dynamic Key Cryptography in Sharing Medicine, International Journal of Applied Engineering Research, 10(14), 34068-34071, 2015.
2. V. M. Chandrasekaran, A. Manimaran, Akhil Ranjan, Cryptography using A Pair of Dice, CODEN (USA): IJPRIF, ISSN: 0974-4304, 7(1), 85-89, 2015.
3. A. Manimaran, V. M. Chandrasekaran, Manish Gaur, Ayush Gupta, Pulkit Narwani, Data Encryption and Decryption Using Guitar Strings, International Journal of Pharmacy and Technology, 7(3), 9774 – 9778, 2015.
4. Obaida Mohammad, Awad Al-Hazaimeh, A New Approach For Complex Encrypting And Decrypting Data, International Journal of Computer Networks & Communications, 5(2), 2013.
5. A. Manimaran, V. M. Chandrasekaran, Vivek Mallineni, Gangireddy Koushik Reddy, P. M. Karthick, A New Approach For Encrypting And Decrypting Phone Numbers, International Journal of Pharmacy and Technology, 7(3), 9904 – 9908, 2015.
6. P. Zimmerman, An Introduction to Cryptography, Doubleday & Company, Inc., United State of America, USA, 1999.
7. http://en.wikipedia.org/wiki/encryption and decryption.
8. https://en.wikipedia.org/wiki/Chessboard.