Oct 31st, 1:30 PM - 4:15 PM

Usage of the symbols and Dionis square in the cryptosystem of Dionis

Dionis Shabani
University for Business and Technology - UBT, ds48199@ubt-uni.net

Usage of the symbols and Dionis square in the cryptosystem of Dionis

Dionis Shabani

UBT-Higher Education Institution

ds48199@ubt-uni.net

Abstract : The rapid developments of technology which have brought with them a host of benefits to humanity have also left behind a host of spaces which have mostly aided cyber piracy who exploit the many benefits of the internet for purposes that are in their favor,but these actions which negatively affect the privacy of all internet users.
In this project I will present some modifications which are enabled through the 16x16 square of Dionis with 256 elements based in the Masonic Cipher method, with the help of which based on the rules I have created and developed it is different from all the others that have been presented so far containing some specific specifications within it, in order to make the possibility of decryption as difficult as possible for the abusers, but understandable to implement.
Keywords: Encryption, Decryption, Dionis Square, Masonic Cipher

1. Introduction

By cryptographic structure we mean the transformation of a message called open text by means of an encryption function into a meaningless message called closed text, in such a way that only an authorized recipient can return the transformed message to its original state.

Definition. A cryptosystem is called a quintile (P, C, K, E, D) that meets the conditions: P- is a finite family of all open texts.

C-is a finite family of all encrypted texts.

The K-key space is a finite family of all possible keys.

Elements E and D are representations of P to C and C to P, respectively, such that for each K∈K, there is an ek∈E encryption rule and a decryption rule

d_k∈D that ∀x∈P 〖d〗 _k (e_k (x)) = x.

Encryption (encryption, encryption) is the conversion of data into a form called encrypted text (ciphertext), which can not be easily understood by unauthorized persons. Decryption is the process of converting encrypted data into their original form, which can be understood.

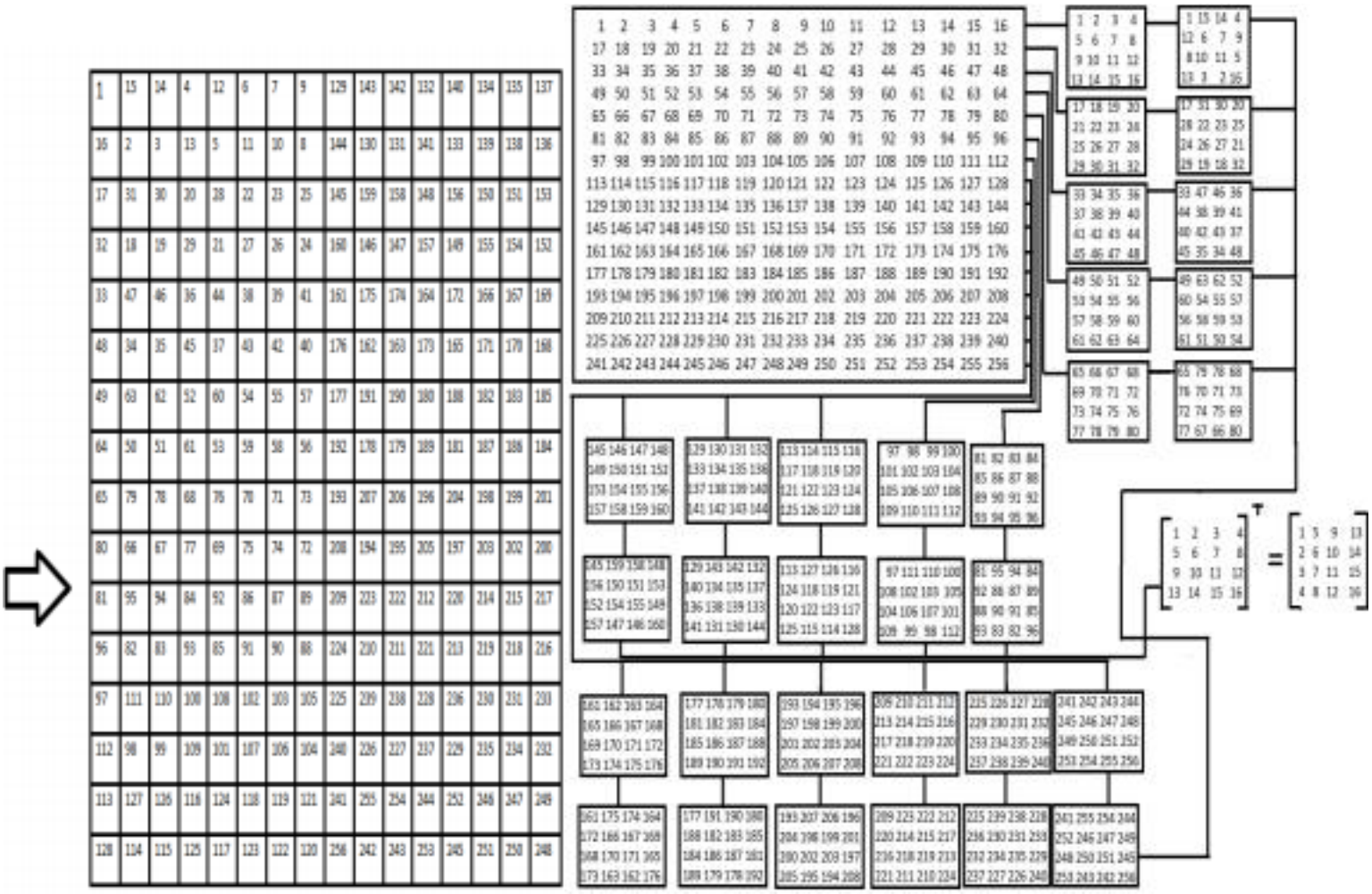
The use of encryption and decryption is as old as communication itself. In time of war, an encryption, often mistakenly called a code, can be used to prevent an opponent from reading the broadcast content.

Encryption is often just a replacement of letters with numbers, rotation of letters in the alphabet or replacements with special symbols. The most complicated cryptostructures use powerful computer algorithms, which transform the bits into digital signals, so that the recovery of the contents of the encrypted signal is done only with the help of the correct decryption key.

Some of the forms of encrypting messages through symbols such as the well-known Pig Pen form which was used 100 years ago by Masons, also this form was used by confederate soldiers during the US Civil War. This form is constantly used to encrypt messages, but having ideas for improvement, which ideas we can use by making perhaps some changes within it, where its shortcomings are more specific as well as providing a form, which will offer more security. Therefore the need to change and develop this method is more than necessary to achieve the adequate form which would provide more symbols as well as provide more security within the sent message so that it could be used further perhaps also for encrypting messages that are of high importance.

2. Rules for the creation of "Dionis Square"

"Dionis Square" represents a matrix of type 16x16 where inside are sorted numbers from 1 to 256, a form which can be generalized in the case "n x n" where n is an even number. The importance of "Dionis Square" lies in the fact that by using the box we can place the symbols that represent the encrypted message inside the box to provide more certainty that its content and its listed form is not known to others, except the person to whom the message is intended.



Tab.1 “Dionis Square” formation process

1 15 14 4 12 6 7 9 129 143 142 132 140 134 135 137 16 2 3 13 5 11 10 8 144 130 131 141 133

139 138 136 17 31 30 20 28 22 23 25 145 159 158 148 156 150 151 153 32 18 19 29 21 27 26 24

160 146 147 157 149 155 154 152 33 47 46 36 44 38 39 41 161 175 174 164 172 166 167 169 48

34 35 45 37 43 42 40 176 162 163 173 165 171 170 168 49 63 62 52 60 54 55 57 177 191 190

180 188 182 183 185 64 50 51 61 53 59 58 56 192 178 179 189 181 187 186 184 65 79 78 68 76

70 71 73 193 207 206 196 204 198 199 201 80 66 67 77 69 75 74 72 208 194 195 205 197 203

202 200 81 95 94 84 92 86 87 89 209 223 222 212 220 214 215 217 96 82 83 93 85 91 90 88 224

210 211 221 213 219 218 216 97 111 110 100 108 102 103 105 225 239 238 228 236 230 231

233 112 98 99 109 101 107 106 104 240 226 227 237 229 235 234 232 113 127 126 116 124 118

119 121 241 255 254 244 252 246 247 249 128 114 115 125 117 123 122 120 256 242 243 253

245 251 250 248 Tab.2 **“Dionis Square”**

Rules:

2.1. The sum of all the numbers on the two diagonals of "Dionis Square" is the same on both diagonals of the 16x16 square.

$D = n \cdot (n^2 + 1) / 2 = 16 \cdot (16^2 + 1) / 2 = 16 \cdot (256 + 1) / 2 = 16 \cdot (257) / 2 = 4112 / 2 = 2056$

2.2. The distance between any two numbers on the diagonals of any 2x2 square is the same distance is 1 distance

2.3 The distance between any two numbers from position (7) to position (0) as well as from position (15) to position (8) is the same distance 2, as an arithmetic sequence (1,3,5,7,9,11,13,15)

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

2.4. The symbolic representation of "Dionis Square", thus presenting the form of how each member of the square could be visited in its position and in this form represents the possibility that through the symbol the whole "Dionis Square" can be created.

Fig.1

2.5. Symbols used in the Dionis Cryptosystem:

2.5.1 *Symbolic representation of capital letters*

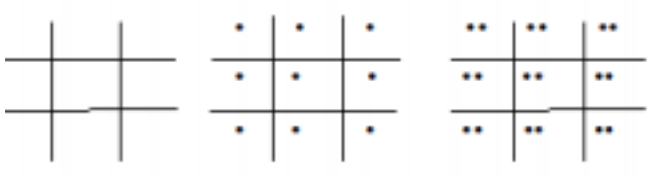


Fig.2

2.5.2 *Symbolic representation of lowercase letters*

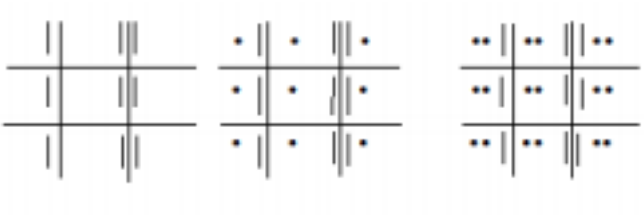


Fig.3

2.5.3 *Symbolic representation of numbers*

Fig.4

2.5.4 *Symbolic representation of punctuation*

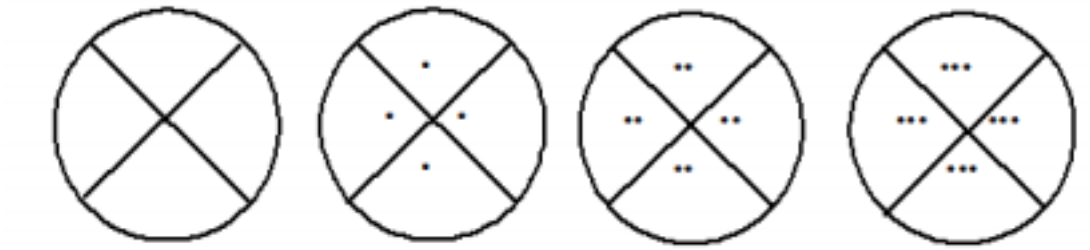


Fig.5

2.5. *Arithmetic operators* 2.5.6 *Comparative operators* 2. 5.7 *Space*

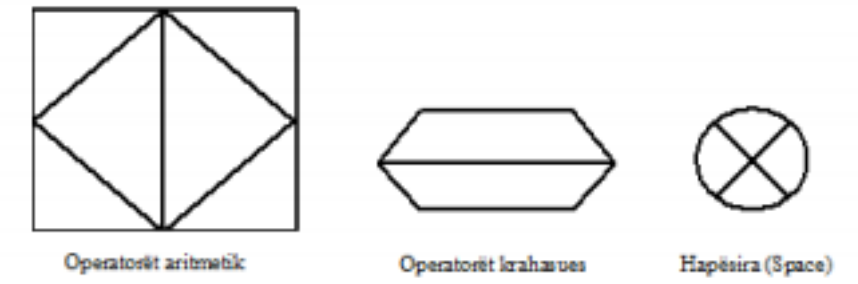


Fig.6

2.6. Symbolic representation of each uppercase, lowercase letter, number, punctuation, arithmetic operators, comparative operators and space

2.6.1 *Uppercase and lowercase letters*

- A •• - X - a •• - x

• - B - Y • - b - y

•• - C • - Z •• - c • - z

▌- D - d

▌• - E • - e

▌•• - F •• - f

▌- G - g

▌• - H • - h

•• - I •• - i

- J - j

• - K • - k

•• - L •• - l

- M - m

• - N • - n

•• - O •• - o

▌- P - p

▌• - Q • - q

•• - R •• - r

- S - s

• - T • - t

•• - U •• - u

- V - v

▌• - W • - w

2.6.2 *Numbers*

- 0 • - 4 • - 8

• - 1 - 5 •• - 9

•• - 2 - 6

- 3 - 7

2.6.3 *Punctuation*

- . - { - (- ! • - , - } -) • - ?

•• - ; - [- ‘ •• - _

••• - : ••• -] - “ ••• - =

2.6.4 *Arithmetic operators*

- + - /

- - - %

- * - ^

2.6.5 *Comparative operators*

- < - >

2.6.6 *Space*

3. Example of message encryption using "Dionis Square" and Dionis Cryptosystem symbols

ABC DEF GHI abc def ghi JKL MNO . , ; :

PQR jkl mno pqr STU VWX YZ stu { } [ ] ()’ ” ! ? - =

vwx yz

3.1 *Placement of letters in the corresponding positions in "Dionis Square"*

1 15 14 4 12 6 7 9 129 143 142 132 140 134 135 137 16 2 3 13 5 11 10 8 144 130 131 141 133

139 138 136 17 31 30 20 28 22 23 25 145 159 158 148 156 150 151 153 32 18 19 29 21 27 26 24

160 146 147 157 149 155 154 152 33 47 46 36 44 38 39 41 161 175 174 164 172 166 167 169 48

34 35 45 37 43 42 40 176 162 163 173 165 171 170 168 49 63 62 52 60 54 55 57 177 191 190

180 188 182 183 185 64 50 51 61 53 59 58 56 192 178 179 189 181 187 186 184 65 79 78 68 76

70 71 73 193 207 206 196 204 198 199 201 80 66 67 77 69 75 74 72 208 194 195 205 197 203

202 200 81 95 94 84 92 86 87 89 209 223 222 212 220 214 215 217 96 82 83 93 85 91 90 88 224

210 211 221 213 219 218 216 97 111 110 100 108 102 103 105 225 239 238 228 236 230 231

233 112 98 99 109 101 107 106 104 240 226 227 237 229 235 234 232 113 127 126 116 124 118

119 121 241 255 254 244 252 246 247 249 128 114 115 125 117 123 122 120 256 242 243 253

245 251 250 248 Tab.3

The form of placing the letters or only the symbols that represent the content of the message inside "Dionis Square" is taken based on the length of the encrypted message, with the sole purpose that only the recipient of the message can understand its content and the form of how from "Dionis Square" can be obtained encrypted message but in its correct order.

S n ^{o} b D l e p t i a , o r v i i m i O e t m e r r t a e e s e j u n e s a k a

d h

j i t g m e t d u t i h r k e n e p r d r e h z i e e j k e r e m i o v s d o k

r a s t m m i i e i n r g z i p e i e n s l l j a , a n h j e b m e e t e e l t

t e v a m r p s u d i n i c i j v a t n s k h i s d h r e e j e o r h k t e l a

e u u , a j m e a v , r s e t m i

v n u n r h s e a i p m i e t t e , t e m p i e z N A v A . . o t i i s k I h e

B e H S D Tab.4

3.2 *Placing symbols that represent the encrypted message inside "Dionis Square"*

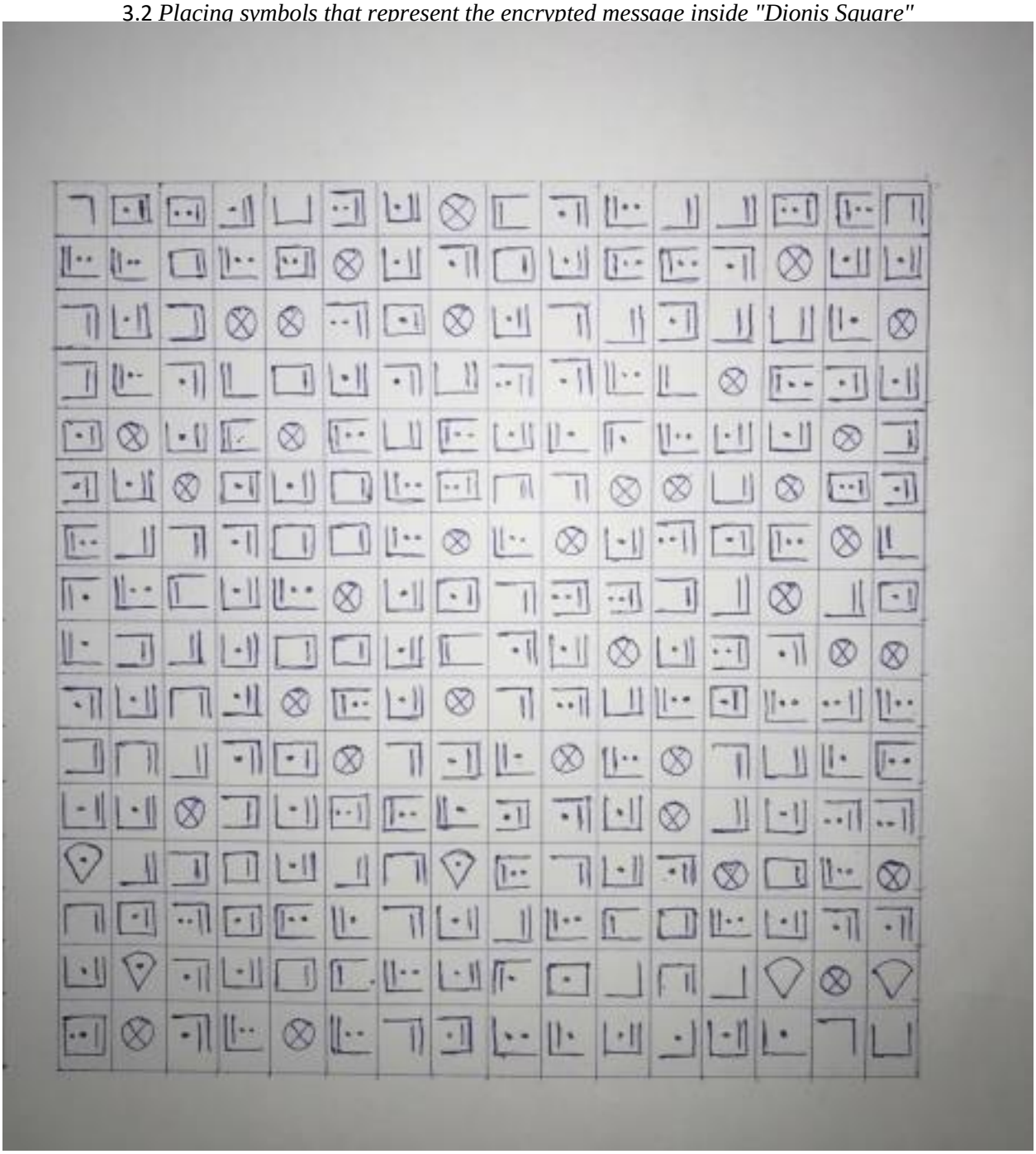


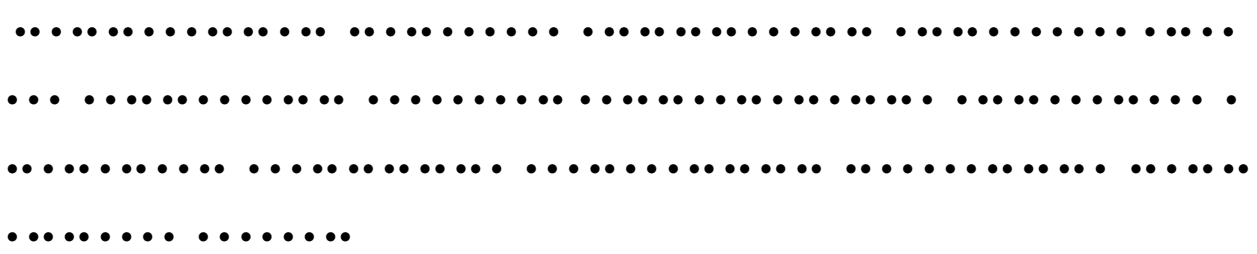
Fig .7

Placing the entire encrypted message inside "Dionis Square", which is enabled whenever the correct message order must be kept hidden and to exit from the box to get the correct message

order must use the positions of the symbols that represent numbers placed in "Dionis Square" or even through the symbol which shows the form how all members of "Dionis Square" are visited and used to create "Dionis Square".

3.3 *Exit from "Dionis Square" to get the correct order of the encrypted*

message **Encrypted message:**



Decrypted message:

Dionis symbols can be used in encrypting messages containing letters, numbers, punctuation, arithmetic operators and comparative, ideas developed by a student who is a fan of message encryption. D.Shabani

4. Conclusion

Dionis cryptosystem using "Dionis Square" is a unique derivative of the "Pig Pen" method which can be used for various purposes. With these changes we filled in some gaps that the Pig Pen method had, as well as offering greater security especially when the message sent may be in the wrong hands so crossing from "Dionis Square" can not be done without passing from the position of any the member within "Dionis Square" in the message listed in the correct form and here also calculating the possibility offered by the method for changing the positions of letters, numbers or characters used within the sent message where this allows you to use a key inside the text of encrypted to increase the security of the encrypted message, which assures us that, even if the message can be found on the wrong person, he will not be able to understand its exact contents.

The "Dionis Square" method can be used in the military, intergovernmental communications or even education, for all crypto enthusiasts.

References

[1] Brown, D : The Lost Symbol. Doubleday; 1st edition(2009).

[2] Gardner, M : Codes, Ciphers and Secret Writing. Dover Publications INC, New York(1984).

[3] Parrangan, D., Parrangan, Th : New Simple Algorithm for Detecting the Meaning of Pigpen Cipher. International Journal of Signal Processing, Image Processing and Pattern Recognition 2013, Vol.6, pp. 305 – 314 ,No.5 (2013).

[4] Pratt,F : Secret & Urgent : The Story of Codes and Ciphers. Bobbs-Merrill Company(1939).