MATRIX BASED CRYPTOGRAPHY VB.NET APPROACH

Dr. A. Prasanna
Assistant Professor, Jamal Mohamed College, Trichy-20
Dr. S. Ismail Mohideen
Associate Professor, Jamal Mohamed College, Trichy-20
Rajasekar. K
MCA, Jamal Mohamed College, Trichy-20

ABSTRACT

Cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as clear text) into cipher text (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers. This paper focuses on a confidential message which is encrypted by using secret matrix and is sent to the confident who will decrypt the message by using the secret matrix in vb.net approach. Which is known to the sender and the receiver only. There are enormous avenues thrown open for future research in this discipline.

Keyword: cryptography, encryption, decryption, matrix, vb.net

Introduction

The present scenario of mass hacking in computers, Hackers Hijack Millions of Computers in 'Massive' Fraud Case ' Cyber Criminals Hijacked 4 Million Computers, NSA chief seeks help from hackers, Saudi Aramco hacked; company confirms disruption In this context this paper gets importance as it explains the ways and means by which confidentiality and integrity are maintained in the transfer of information from important sources

Cryptography

Cryptography is the science of information security. The word is derived from the Greek *kryptos*, meaning hidden. Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric

world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

Modern cryptography concerns itself with the following four objectives:

1) Confidentiality (the information cannot be understood by anyone for whom it was unintended)

2) Integrity (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)

3) Non-repudiation (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)

4) Authentication (the sender and receiver can confirm each other?s identity and the origin/destination of the information)

Encryption and Decryption

Encryption is the conversion of data into a form, called a ciphertext that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

Matrices and Cryptography

Today governments use sophisticated methods of coding and decoding messages. One type of code, which is extremely difficult to break, makes use of a large matrix to encode a message. The receiver of the message decodes it using the inverse of the matrix. This first matrix is called the encoding matrix and its inverse is called the decoding matrix.

Encoding Matrix

It is the confidential matrix designed specially by the sender of the message to avoid hacking. This can be altered suited to the occasion. In this model the encoding matrix is designed as follows.

Message

In many circumstances we want to send a message so that it can only be read by the intended recipient in this case we talk about the message being encrypted or enciphered this is

an important and very activity studied area as computers grow more powerful we need to devise ciphers that are more difficult to break.

S	K	T	E	M	I	Q	Z	U	A	D	4	P	C
114	29	85	95	126	77	32	16	31	82	118	52	66	14
Q	D	J	L	G	A	V	I	W	L	F	K	W	N
81	116	3	74	93	101	123	7	124	19	97	46	6	21
M	B	O	5	F	Y	F	X	C	S	V	Z	F	B
41	43	13	37	105	47	73	125	45	128	12	84	64	127
N	R	Y	E	A	2	O	8	P	1	Y	J	G	D
24	65	48	26	2	8	68	76	67	57	28	107	87	86
7	W	V	B	U	H	C	L	K	X	U	6	A	H
4	11	91	9	22	17	30	117	96	90	113	80	38	109
D	O	G	I	G	N	H	R	V	S	I	L	J	X
40	78	35	49	69	33	55	92	44	36	60	94	70	111
H	U	X	T	P	3	Q	Y	T	G	O	K	E	Z
18	5	61	71	10	99	103	58	122	34	25	120	129	54
N	C	A	R	S	D	9	C	E	M	0	W	R	T
51	56	53	88	83	63	23	15	87	62	121	104	1	-114

Step: 1 Encryption:

Encoding Process

77, 21, 15, 41, 101, 51, 2, 53, 14, 77, 65, 30, 31, 41, 128, 71, 2, 24, 45, 26, 36, 63, 6, 26, 15, 6, 2, 33, 71, 34, 85, 13, 15, 128, 26, 24, 116, 53, 101, 15, 41, 26, 128, 36, 2, 87, 129, 15, 128, 13, 15, 71, 17, 38, 122, 63, 7, 71, 53, 45, 101, 24, 63, 68, 33, 19, 48, 63, 9, 26, 15, 65, 26, 2, 116, 15, 9, 28, 34, 71, 17, 26, 15, 49, 24, 122, 26, 33, 86, 129, 86, 63, 1, 26, 30, 7, 10, 49, 87, 33, 122, 63, 49, 51, 15, 122, 109, 60, 36, 53, 30, 2, 36, 87, 63, 6, 129, 15, -114, 2, 19, 120, 15, 101, 43, 68, 22, 71, 63, 71, 55, 26, 15, 62, 26, 36, 83, 2, 35, 129, 63, 43, 26, 7, 33, 69, 53, 129, 33, 30, 92, 28, 67, 122, 87, 40, 63, 13, 1, 63, 129, 33, 56, 77, 10, 17, 87, 1, 26, 40, 15, -114, 109, 49, 83, 53, 7, 36, 53, 2, 33, 15, 7, 41, 10, 13, 1, 71, 2, 51, 71, 63, 2, 86, 15, 12, 26, 81, 28, 15, 101, 45, 85, 7, 12, 26, 117, 28, 63, 36, 71, 22, 86, 49, 87, 116, 15, 2, 92, 26, 101, 63, 101, 36, 15, 30, 68, 41, 10, 113, 71, 26, 92, 36, 34, 93, 81, 13, 6, 15, 41, 13,

92, 26, 15, 10, 13, 6, 95, 81, 97, 5, 19, 15, 6, 26, 63, 24, 129, 95, 40, 63, 71, 13, 15, 116, 26, 12, 7, 36, 87, 63, 30, 49, 10, 17, 87, 81, 36, 34, 122, 109, 2, -114, 15, 82, 1, 87, 34, 41, 25, 1, 26, 34, 86, 7, 105, 97, 49, 30, 5, 19, -114, 53, 71, 13, 63, 9, 81, 26, 2, 29.

The encoding matrix of this model

$$A = \begin{bmatrix} -1 & 5 & -1 \\ -2 & 11 & 7 \\ 1 & -5 & 2 \end{bmatrix}$$

As the encoding matrix is 3 by 3matrix, so the above numbers are also arranged in 3 by 1 vectors and multiplied by the encoding matrix.

$$B = \begin{bmatrix} 77\ 41\ 2877\ 31\ 7145631533851281161512887\ 12871122 \\ 21\ 1015365\ 41\ 2\ 26\ 6\ 6\ 7113\ 26\ 53\ 41\ 36\ 129\ 13\ 17\ 63 \\ 15\ 51\ 1430128243626\ 2\ 3415\ 24\ 10126\ 2\ 15\ 15\ 38\ 7 \end{bmatrix}$$

$$\begin{matrix} 71101684826\ 26\ 153426\ 24\ 33\ 862610\ 33\ 4912236\ 2\ 63\ 15 \\ 53\ 24\ 336315\ 2\ 9\ 7115122\ 86\ 633049122511095336\ 6\ -114 \\ 45\ 63\ 19\ 9\ 65116281749\ 26\ 129\ 1\ 7\ 87\ 63\ 15\ 60\ 3087129\ 2 \end{matrix}$$

$$\begin{matrix} 19\ 10122711536\ 35\ 43331299212263\ 63\ 561726-114833633 \\ 120\ 43\ 715562831292669\ 33\ 28\ 87\ 13129778740\ 109575315 \\ 15\ 68\ 632626\ 2\ 63\ 7\ 53\ 30\ 67\ 40\ 1\ 33\ 15\ 1\ 15\ 49\ 7\ 2\ 7 \end{matrix}$$

$$\begin{matrix} 41\ 1\ 51\ 2\ 1581101\ 7\ 1173686116\ 92\ 63\ 15\ 41\ 713681159210 \\ 107171211228\ 45\ 12\ 28\ 7149\ 15\ 26\ 10130\ 10\ 263416412616 \\ 13\ 2\ 63862615\ 85\ 26\ 63\ 2287\ 2\ 101\ 36\ 681139293\ 6\ 1315\ 6 \end{matrix}$$

$$\begin{matrix} 95\ 5\ 6\ 24\ 40\ 13\ 26363017\ 36\ 109\ 1587253410530-114138129 \\ 81192612963\ 15\ 12874987\ 34\ 2\ 8234\ 1\ 86\ 97\ 5\ 53632615 \\ 971563\ 95\ 71116\ 7\ 631081122-114\ 1\ 4126\ 7\ 49\ 19\ 71\ 9\ 2\ 34 \end{matrix}$$

$$A = \begin{bmatrix} -1 & 5 & -1 \\ -2 & 11 & 7 \\ 1 & -5 & 2 \end{bmatrix} * B$$

$$\begin{bmatrix} 13\ 413\ 223\ 218\ 46-85\ 49-59\ 13\ 288-35-22\ 48\ 164\ 50\ 543-78-24 \\ 1821386\ 625\ 7711285\ 48\ 448\ 122\ 50\ 953\ 78\ 1981058\ 603\ 154\ 1350\ -8\ 311 \\ 2\ -362-209-188\ 82\ 109-13\ 85-11-254\ 50\ 46\ 53-138-48-528\ 93\ 62 \end{bmatrix}$$

$$\begin{matrix} 186\ 149-44\ 78\ 258-16-132\ 2\ 304\ 0\ 560\ 268\ 228\ 117\ 148\ 514\ 191 \\ 498\ 756\ 503\ 360\ 660\ 568\ 782265\ 832456\ 1476\ 1783\ 528\ 3271128\ 1717\ 568 \\ -179-104\ 107-59-249\ 81\ 248\ 26-287\ 49-534-139-227-110\ -61-451-176 \end{matrix}$$

363 199 91 −162 −587 566 101 270 178 269 377 547 80 259 6 −19 273
1375 721 1001 843 −1270 1387 43 1178 645 834 855 1790 249 1064 315 593 993
−303 −169 −4 291 589 −551 68 −207 −152 −243 −375 −484 −73 −206 24 86 −233

1 549 319 417 159 610 175 227 35 −4 352 241 17 19 44 39 27 −40 297
24 1524 805 930 493 1770 466 525 148 119 793 1120 829 284 251 888 300 515 863
0 −516 −309 −416 −144 −561 −168 −225 −28 17 −350 −178 96 7 −29 46 −1 103 −275

72 −43 −63 406 67 −104 −33 41 −22 177 23 49 213 75 61 526 204 −54 27
976 −53 809 1237 776 819 788 953 23 512 207 165 1380 304 715 2036 1110 951 129
15 45 164 −370 1 217 125 52 2 −164 −8 −43 −116 −60 2 −431 −113 170 −20

336 225 337 12 15 394 42 −46 389 331 −24 308 293 47 12
1326 549 1490 1156 −994 879 487 143 927 1200 128 1308 730 1383 45
−273 −195 −256 110 −129 −393 −1 72 −382 −282 43 −237 −284 −45 22

13, 182, 2, 413, 1386, -362, 223, 625, -209, 218, 771, -188, 46, 1285, 82, -85, 48, 109, 49, 448, -13, -59, 122, 85, 13, 50, -11, 288, 953, -254, -35, 78, 50, -22, 198, 46, 48, 1058, 53, 164, 603, -138, 50, 154, -48, 543, 1350, -528, -78, -8, 93, -24, 311, 62, 186, 498, -179, 149, 756, -104, -44, 503, 107, 78, 360, -59, 258, 660, -249, -16, 568, 81, -132, 782, 248, 2, 265, 26, 304, 832, -287, 0, 456, 49, 560, 1476, -534, 268, 1783, -139, 228, 528, -227, 117, 327, -110, 148, 1128, -61, 514, 1717, -451, 191, 568, -176, 363, 1375, -303, 199, 721, -169, 91, 1001, -4, -162, 843, 291, -587, -1270, 589, 566, 1387, -551, 101, 43, 68, 270, 1178, -207, 178, 645, -152, 269, 834, -243, 377, 855, -375, 547, 1790, -484, 80, 249, -73, 259, 1064, -206, 6, 315, 24, -19, 593, 86, 273, 993, -233, 1, 24, 0, 549, 1524, -516, 319, 805, -309, 417, 930, -416, 159, 493, -144, 610, 1770, -561, 175, 466, -168, 227, 525, -225, 35, 148, -28, -4, 119, 17, 352, 793, -350, 241, 1120, -178, 17, 829, 69, 19, 284, 7, 44, 251, -29, 39, 888, 46, 27, 300, -1, -40, 515, 103, 297, 863, -275, 72, 976, 15, -43, -53, 45, -63, 809, 164, 406, 1237, -370, 67, 776, 1, -104, 819, 217, -33, 788, 125, 41, 953, 52, -22, 23, 28, 177, 512, -164, 23, 207, -8, 49, 165, -43, 213, 1380, -116, 75, 304, -60, 61, 175, 2, 526, 2036, -431, 204, 1110, -113, -54, 951, 170, 27, 129, -20, 336, 1326, -273, 205, 549, -195, 337, 1490, -256, 12, 1156, 110, 15, -994, -129, 394, 879, -393, 42, 487, -1, -46, 143, 72, 389, 927, -382, 331, 1200, -282, -24, 128, 43, 308, 1308, -237, 293, 730, -284, 47, 138, -45, 12, 345, 22.

Step: 2 Decryption

The inverse of the encoding matrix is the decoding matrix.

The decoding matrix of the model is

$$A^{-1} = \begin{bmatrix} -57 & 5 & -46 \\ -11 & 1 & -9 \\ 1 & 0 & 1 \end{bmatrix}$$

To decode, the above numbers have to be converted in to 3 by 1 column matrices as follows.

$$C = \begin{bmatrix} 13 & 413 & 223 & 218 & 46 & -85 & 49 & -59 & 13 & 288 & -35 & -22 & 48 & 164 & 50 & 543 & -78 & -24 \\ 182 & 1386 & 625 & 7711 & 285 & 48 & 448 & 122 & 50 & 953 & 78 & 1981 & 058 & 603 & 154 & 1350 & -8 & 311 \\ 2 & -362 & -209 & -188 & 82 & 109 & -13 & 85 & -11 & -254 & 50 & 46 & 53 & -138 & -48 & -528 & 93 & 62 \end{bmatrix}$$

$$\begin{bmatrix} 186 & 149 & -44 & 78 & 258 & -16 & -132 & 2 & 304 & 0 & 560 & 268 & 228 & 117 & 148 & 514 & 191 \\ 498 & 756 & 503 & 360 & 660 & 568 & 782 & 265 & 832 & 456 & 1476 & 1783 & 528 & 327 & 1128 & 1717 & 568 \\ -179 & -104 & 107 & -59 & -249 & 81 & 248 & 26 & -287 & 49 & -534 & -139 & -227 & -110 & -61 & -451 & -176 \end{bmatrix}$$

$$\begin{bmatrix} 363 & 199 & 91 & -162 & -587 & 566 & 101 & 270 & 178 & 269 & 377 & 547 & 80 & 259 & 6 & -19 & 273 \\ 1375 & 721 & 1001 & 843 & -1270 & 1387 & 43 & 1178 & 645 & 834 & 855 & 1790 & 249 & 1064 & 315 & 593 & 993 \\ -303 & -169 & -4 & 291 & 589 & -551 & 68 & -207 & -152 & -243 & -375 & -484 & -73 & -206 & 24 & 86 & -233 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 549 & 319 & 417 & 159 & 610 & 175 & 227 & 35 & -4 & 352 & 241 & 17 & 19 & 44 & 39 & 27 & -40 & 297 \\ 24 & 1524 & 805 & 930 & 493 & 1770 & 466 & 525 & 148 & 119 & 793 & 1120 & 829 & 284 & 251 & 888 & 300 & 515 & 863 \\ 0 & -516 & -309 & -416 & -144 & -561 & -168 & -225 & -28 & 17 & -350 & -178 & 96 & 7 & -29 & 46 & -1 & 103 & -275 \end{bmatrix}$$

$$\begin{bmatrix} 72 & -43 & -63 & 406 & 67 & -104 & -33 & 41 & -22 & 177 & 23 & 49 & 213 & 75 & 61 & 526 & 204 & -54 & 27 \\ 976 & -53 & 809 & 1237 & 776 & 819 & 788 & 953 & 23 & 512 & 207 & 165 & 1380 & 304 & 715 & 2036 & 1110 & 951 & 129 \\ 15 & 45 & 164 & -370 & 1 & 217 & 125 & 52 & 2 & -164 & -8 & -43 & -116 & -60 & 2 & -431 & -113 & 170 & -20 \end{bmatrix}$$

$$\begin{bmatrix} 336 & 225 & 337 & 12 & 15 & 394 & 42 & -46 & 389 & 331 & -24 & 308 & 293 & 47 & 12 \\ 1326 & 549 & 1490 & 1156 & -994 & 879 & 487 & 143 & 927 & 1200 & 128 & 1308 & 730 & 138 & 345 \\ -273 & -195 & -256 & 110 & -129 & -393 & -1 & 72 & -382 & -282 & 43 & -237 & -284 & -45 & 22 \end{bmatrix}$$

$$A^{-1} = \begin{bmatrix} -57 & 5 & -46 \\ -11 & 1 & -9 \\ 1 & 0 & 1 \end{bmatrix} * C$$

$$B = \begin{bmatrix} 77 & 41 & 2877 & 31 & 7145 & 631 & 533 & 851 & 2811 & 615 & 128 & 87 & 12871122 \\ 21 & 1015 & 365 & 41 & 2 & 26 & 6 & 6 & 7113 & 26 & 53 & 41 & 36 & 129 & 13 & 17 & 63 \\ 15 & 51 & 1430 & 128 & 2436 & 26 & 2 & 3415 & 24 & 10126 & 2 & 15 & 15 & 38 & 7 \end{bmatrix}$$

$$\begin{bmatrix} 71101684826 & 26 & 153426 & 24 & 33 & 862610 & 33 & 4912236 & 2 & 63 & 15 \\ 53 & 24 & 336315 & 2 & 9 & 7115122 & 86 & 633049122511095336 & 6 & -114 \\ 45 & 63 & 19 & 9 & 65116281749 & 26 & 129 & 1 & 7 & 87 & 63 & 15 & 60 & 3087129 & 2 \end{bmatrix}$$

$$\begin{bmatrix} 19 & 10122711536 & 35 & 43331299212263 & 63 & 561726 & -114833633 \\ 120 & 43 & 715562831292669 & 33 & 28 & 87 & 13129778740 & 109575315 \\ 15 & 68 & 632626 & 2 & 63 & 7 & 53 & 30 & 67 & 40 & 1 & 33 & 15 & 1 & 15 & 49 & 7 & 2 & 7 \end{bmatrix}$$

41 1 51 2 1581101 7 1173686116 92 63 15 41 713681159210
107171211228 45 12 28 7149 15 26 10130 10 263416412616
13 2 63862615 85 26 63 2287 2 101 36 681139293 6 1315 6

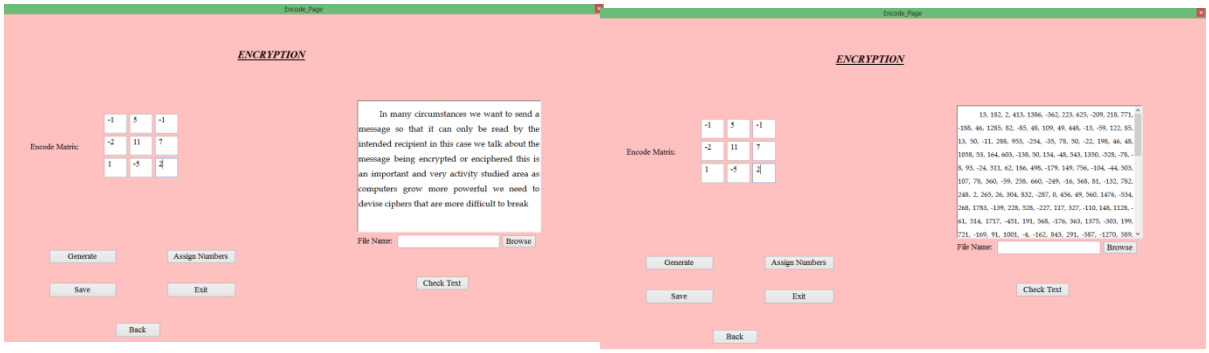
95 5 6 24 40 13 26363017 36 109 1587253410530−114138129
81192612963 15 12874987 34 2 8234 1 86 97 5 53632615
971563 95 71116 7 631081122−114 1 4126 7 49 19 71 9 2 34

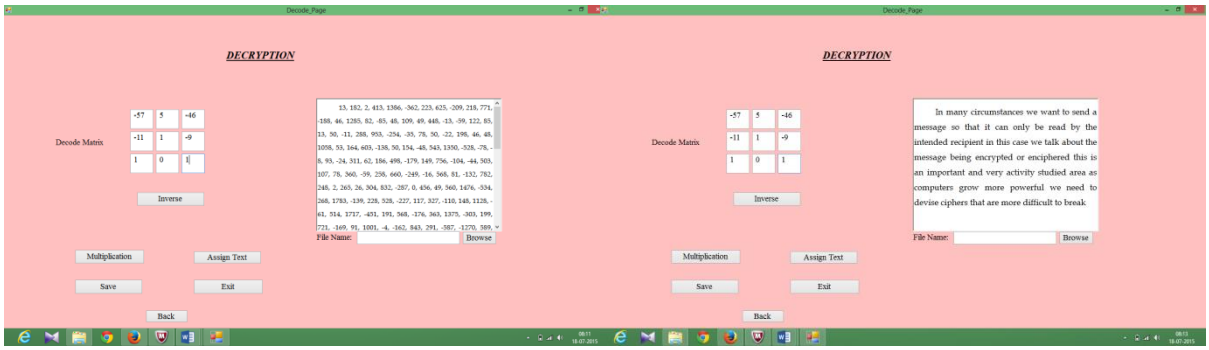
77, 21, 15, 41, 101, 51, 2, 53, 14, 77, 65, 30, 31, 41, 128, 71, 2, 24, 45, 26, 36, 63, 6, 26, 15, 6, 2, 33, 71, 34, 85, 13, 15, 128, 26, 24, 116, 53, 101, 15, 41, 26, 128, 36, 2, 87, 129, 15, 128, 13, 15, 71, 17, 38, 122, 63, 7, 71, 53, 45, 101, 24, 63, 68, 33, 19, 48, 63, 9, 26, 15, 65, 26, 2, 116, 15, 9, 28, 34, 71, 17, 26, 15, 49, 24, 122, 26, 33, 86, 129, 86, 63, 1, 26, 30, 7, 10, 49, 87, 33, 122, 63, 49, 51, 15, 122, 109, 60, 36, 53, 30, 2, 36, 87, 63, 6, 129, 15, -114, 2, 19, 120, 15, 101, 43, 68, 22, 71, 63, 71, 55, 26, 15, 62, 26, 36, 83, 2, 35, 129, 63, 43, 26, 7, 33, 69, 53, 129, 33, 30, 92, 28, 67, 122, 87, 40, 63, 13, 1, 63, 129, 33, 56, 77, 10, 17, 87, 1, 26, 40, 15, -114, 109, 49, 83, 53, 7, 36, 53, 2, 33, 15, 7, 41, 10, 13, 1, 71, 2, 51, 71, 63, 2, 86, 15, 12, 26, 81, 28, 15, 101, 45, 85, 7, 12, 26, 117, 28, 63, 36, 71, 22, 86, 49, 87, 116, 15, 2, 92, 26, 101, 63, 101, 36, 15, 30, 68, 41, 10, 113, 71, 26, 92, 36, 34, 93, 81, 13, 6, 15, 41, 13, 92, 26, 15, 10, 13, 6, 95, 81, 97, 5, 19, 15, 6, 26, 63, 24, 129, 95, 40, 63, 71, 13, 15, 116, 26, 12, 7, 36, 87, 63, 30, 49, 10, 17, 87, 81, 36, 34, 122, 109, 2, -114, 15, 82, 1, 87, 34, 41, 25, 1, 26, 34, 86, 7, 105, 97, 49, 30, 5, 19, -114, 53, 71, 13, 63, 9, 81, 26, 2, 29.

We get the original message

In many circumstances we want to send a message so that it can only be read by the intended recipient in this case we talk about the message being encrypted or enciphered this is an important and very activity studied area as computers grow more powerful we need to devise ciphers that are more difficult to break

Vb.net output window





Conclusion:

The matrix applied cryptography will go a long way to help the Defense, Secret Services, Police, Financial Services including Banking and Insurance, Business, inventions, Governments, Foreign Relations, Diplomacies, Strategies etc, to ensure confidentiality and integrity The new trends in matrix based cryptography saves the messages from the dangerous clutches of hackers. This paper has made an earnest attempt by adopting a simple matrix model to save the messages from being hacked by the unscrupulous elements.

References

1. Buchmann, Johannes, Introduction to cryptography, second edition 2004, ISBN 978-1-4419-9003-7
2. A. Abdul Salam, A. Prasanna, The Practical Application of Cryptography by Using A Matrix In Image Identification and Road Mapping, Proceedings of the International Conference on Mathematics –A Global Scenario, 2012, ISBN 978-81-925376-0-8
3. A. Abdul Salam, A. Prasanna, Decryption of Road Map By Two Different Persons Using Matrix, Proceedings of the International Conference on Discrete Mathematics and its Applications, 2013, ISBN 978-81-924767-5-9
4. BibhudendraAcharya, GirijaSankarRath, Sarat Kumar, Patra, Saroj Kumar Panigrahy. 2007. Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm, *International Journal of Security*, Vol 1, Issue1, 2007, pp. 14-21
5. P. Butkovic, *Max-linear systems: theory and algorithms*, Springer-Verlag London, 2010.
6. D. Grigoriev, I. Ponomarenko, *Constructions in public-key cryptography over matrix groups*, Contemp. Math., Amer. Math. Soc. 418 (2006), 103{119.
7. Strang, Gilbert. Introduction to Linear Algebra. Sellesley-Cambridge Press, 1998.