International Journal of Latest Engineering Research and Applications (IJLERA) ISSN: 2455-7137

Volume – 02, Issue – 08, August – 2017, PP – 61-66

A method for encryption and decryption of large messages by using matrices

Dr. JyotiShinde[1], Mr. Ravikumar[2],Prof. P Madar Valli[3]

[1]*Professor, Al Habeeb College of Engineering and Technology,Telangana India*

[2]*Assistant Professor, Al Habeeb College of Engineering and Technology, Telangana India*

[3]*Principal, Al Habeeb College of Engineering and Technology, Telangana India*

Abstract: This paper aims to provide broad view about security for large messages. In this, we are using 400 characters for encryption and decryption, characters are easily encrypted and decrypted by using a open software called geogebra, that helps in multiplying matrices for decryption and getting inverse for encryption, encrypting and decrypting large message with less time, estimated less than one minute. This paper reviews sending large messages with encryption and decryption with less time. Encrypted and decrypted for 400 characters.

Key words: Geogebra, Matrices Encryption, Decryption.

I. Introduction

Transmission and storage of multimedia data like audio, video, and images over the Internet has increased in today's digital communication. Among the different multimedia data, messages are transmitted and used very often. It is essential to protect the multimedia data from unauthorized disclosure during transmit. Information security has become a very critical aspect of modern computing systems to protect data from unauthorized access.Etymologicallyspeaking, the word cryptography comes fromthe Greek origin. It is a combination of two words Crypto and Graphy. Crypto means Secret and Graphy means Writing [1]. Cryptography deals with creating documents that can be shared secretly over public communication channels. The present Scenario, everyone needs to encrypt the message at the sender side and decrypt it at the receiver side to preserve security and privacy. So cryptography is the study of creating and using encryption and decryption techniques. In cryptography the term plaintext is used for the original message that is to be transformed. The message which has been transformed is called Cipher text. An encryption algorithm works with a key to transform the plain text into cipher text. Decryption algorithm works in the reverse order and converts the cipher text into plain text [2]. Today this term refers to the science and art of transforming messages to make them secure and immune to attacks. For the purpose of security and privacy, we need to encrypt the message at the sender side and decrypt it at the receiver side. So cryptography is the study of creating and using encryption and decryption techniques. Cryptography is divided into two types [3]. Symmetric Key, Symmetric Key Cryptography a single key is shared between sender and receiver. The sender uses the shared key and encryption algorithm to encrypt the message. The receiver uses the shared key and decryption algorithm to decrypt the message. In Asymmetric Key Cryptography each user is assigned a pair of keys, public key and private key. The public key is announced to all members while the private key is kept secret by the user. The sender uses the public key of the receiver to encrypt the message. The receiver uses his own private key to decrypt the message [4]. As shown in fig1. Computer and network security is both fascinating and complex. Some of the reasons follow:

1. Security is not as simple as it might first appear to the novice. The requirements seem to be straight forward indeed, most of the major requirements for security services can be given self-explanatory, one-word labels: confidentiality, authentication, nonrepudiation, or integrity. But the mechanisms used to meet those requirements can be quite complex, and understanding them may involve rather for reasoning.

2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features. In many cases, successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism.

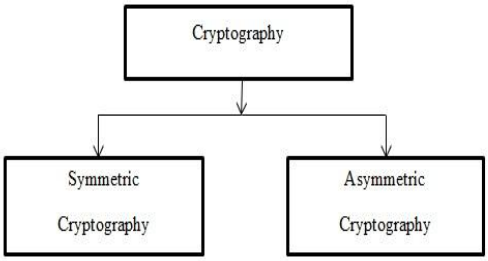

Fig 1. Types of Cryptography

3. Because of point 2, the procedures used to provide particular services are often counter intuitive. Typically, a security mechanism is complex, and it is notobvious from the statement of a particular requirement that such elaborate measures are needed. It is only when the various aspects of the threat are considered that elaborate security mechanisms make sense.
4. Having designed various security mechanisms, it is necessary to decide where to use them. This is true both in terms of physical placement (e.g., at what points in a network are certain security mechanisms needed) and in a logical sense [e.g., at what layer or layers of an architecture such as TCP/IP(Transmission Control Protocol/Internet Protocol) should mechanisms be placed].
5. Security mechanisms typically involve more than a particular algorithm orprotocol. They also require that participants be in possession of some secret information (e.g., an encryption key), which raises questions about the creation, distribution, and protection of that secret information. There also may be a reliance on communications protocols whose behaviour may complicate the task of developing the security mechanism. For example, if the proper functioning of the security mechanism requires setting time limits on the transit time of a message from sender to receiver, then any protocol or network that introduces variable, unpredictable delays may render such time limits meaningless.
6. Computer and network security is essentially a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them. The great advantage that the attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security.
7. There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs.
8. Security requires regular, even constant, monitoring, and this is difficult in today's short-term, overloaded environment.
9. Security is still too often an afterthought to be incorporated into a system after the design is complete rather than being an integral part of the design process.
10. Many users and even security administrators view strong security as an impedimentto efficient and user-friendly operation of an information system or useof information. It secures information mathematically by mangling message with key.

Cryptography principles

Cryptographic Principle 1:

The first principle is that all encrypted messages must contain some redundancy, that is, information not needed to understand the message. Messages must contain some redundancy.

Cryptographic Principle 2:

Some method is needed to foil replay attacks. One such measure is including in every message a time stamp valid only for, say, 10 seconds. The receiver can then just keep messages around for 10 seconds, to compare newly arrived messages to previous ones to filter out duplicates.
The privacy of intended sender and receiver information is protected from eavesdropper [5].The development of the worldwide web resulted in broad use of cryptography for e-commerce and business applications. The underlying enabling technologies are inexpensive fast software cryptography and open security protocols such as TLS (SSL), SSH and IPsec as introduced in the second half of the 1990s. In spite of this development, only a small fraction of the Internet is encrypted. Most of this encryption is situated at the network or transport layer; the communication is protected end-to-end (e.g., from the browser in the client to the web server), from gateway

to gateway (for a VPN based on IPsec using tunnel mode) or from client to gateway (e.g., a VPN for remote access to company networks). In the last decade we have witnessed an explosion of data between sender and receiver [6].According to the above introduction all research work showing that encryption is applied for only small messages. Now, we propose a Novel Method that encrypts and decrypts In this paper we proposed a novel method that encrypts and decrypts 20X20 rank matrix, approximately 400 character message.

II. Literature Review

In network security, we are having attacks like Passive attack and Active attack; Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Active attacks involve some modification of the data stream or the creation of a false stream. According to Cryptography and network security; the existing systems are discussed as fallows.

Dr. James H. Yu [7] concluded that most people do not know they are at risk until an attack occurs. The general rule is that as network security increases, cost increases, and the overall system network performance decreases. Network security consists of authentication, access control, integrity, and confidentiality. It must be addressed at three levels:

(1) user-internal security policies,

(2) Application – firewalls, proxies, and software, and

(3) hardware – intelligent hubs, switches, and routers. A network security policy, an auditing procedure, and a violation response plan must all be in place to deal with any breach or breakdown of network security before it occurs. Kyung Jun Choi et.al [8] investigated various cryptographic algorithms suitable for wireless sensor network based on MICAz-type motes in which MD5 and RC4 showed best performance in terms of power dissipation and in terms of cryptographic processing time used.Play fair is digraph substitution cipher which uses a 5×5 matrix, in which the keyword is written first and the remaining cells of the matrix are filled with other letter of alphabets with I and J taken in the same cell. The message is divided into digraphs, in which repeating letters in the same pair are separated by filler letter X. In case of odd number of letters in the message a spare letter X is padded with the word to complete the pair. Then the plaintext is encoded according to the four rules presented in [9].The security of RSA is based on the fact that it is relatively easy and two large prime numbers p and q, but no efficient methods are known to factor their product N. Note that the security of RSA is based on the fact that extracting random modular roots mod N is hard. This problem could be easier than factoring N (it cannotbe harder); surprisingly, whether or not it is easier is still an open problem[10].In 2010 Dunkelman et al. [11] have published a related key attack on the 64-bit block cipher KASUMI (that is standardized for GSM under the name A5/3 and that is also used for encryption in 3GPP); the attack requires 4 related keys, 226 plaintexts, 230 bytes of memory and time 232; while these complexities are rather low, the attack cannot be applied to KASUMI as deployed in current mobile networks.

III. Proposed Method For Encryption and Decryption by Using Matrices

In this paper we proposed a novel method that encrypts and decrypts the large messages by using a open software called Geogebra, here GeoGebra (from Geometry and Algebra) is one of the mostinnovative, open -code math software (GNU General Public License) which can be freely downloaded from www.geogebra.org. GeoGebra works on a wide spectrum of operating system platforms which have Java virtual machine installed on. Markus Hohenwarter created free open-source dynamic mathematics software GeoGebra, which is used for bothteaching and learning mathematics from middle school through college to the University level and also in industry (*seeHohenwarter&Preiner,2007*). GeoGebra offers geometry, algebra and Calculus features in a fully connected, compacted and easy-to-use software environment. In other words, this tool extends the concepts of dynamic geometry to the fields of algebra and mathematical analysis. Designed specifically for educational purposes, GeoGebra can help students grasp experimental, problem-oriented and research-oriented learning of mathematics, both in the classroom and at home. By using this geogebra open software we created a mathematical model that enables to multiply matrices of 20X20 matrices and even for more order of matrices. We executed for 20X20 matrices, the geogebra instantly gives a resultant matrix, and the geogebra is one of the best open software for matrix multiplication of any order matrices. In the above flow chart we use geogebra open software then we enter a Matrix that is formed by a message by assigning a number into text like A=1 B=2…..Z=26 likewise, then randomly choose a key matrix on our own. Multiply key matrix and first matrix by geogebra open software, get a resultant matrix, this process is called encryption process. Next the key matrix is inverted and multiplied with the resultant matrix of first matrix and key matrix, then get a matrix same as first matrix. This process is called as decryption process.

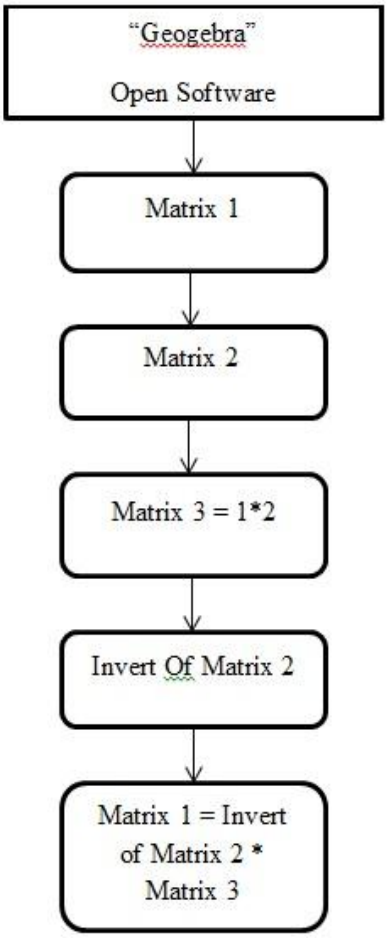

Fig 2. Flowchart

IV. Experimental Results

In this paper we choose the message to encrypt and decrypt is

"Alhabeebcollege of engineering and technology is a premier institution is established by Alhabeeb charitable trust in the year 2002. The college is affiliated to JNTU Hyderabad, Approved by AICTE and accredited by NNBA. In addition to this, the institution is also being certified ISO 9001:2008. The college is situated at Damerigadda, Chevella, Hyderabad. The Hyderabad is a pearl city of India"

The above message is coded as shown in below table.

Table 1. Coding Table for chosen text

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
-	A	B	C	D	E	F	G	H
9	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**
I	J	K	L	M	N	O	P	Q
18	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**
R	S	T	U	V	W	X	Y	Z
27	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**
0	.	,	:	1	2	8	9	;

The above table is coded as according to text to be encrypted.

Matrix 1 represents the message to be encrypted formed by using coding table.

Matrix 2 is key matrix selected randomly for multiplication with matrix 1.

Fig 5 shows the decrypted matrix.

Fig 7 shows the encrypted matrix, which is same as matrix 1.

matrix1 =

1	12	8	1	2	5	5	2	0	3	15	12	12	5
7	5	0	15	6	0	5	14	7	9	14	5	5	18
9	14	7	0	1	14	4	0	20	5	3	8	14	15
12	15	7	25	0	9	19	0	1	0	16	18	5	13
9	5	18	0	9	14	19	20	9	20	21	20	9	15
14	0	9	19	0	5	19	20	1	2	12	9	19	8
5	4	0	2	25	0	1	12	8	1	2	5	5	2
0	3	8	1	18	9	20	1	2	12	5	0	20	18
21	19	20	0	9	14	0	20	8	5	0	25	5	1
18	0	32	27	27	32	28	0	20	8	5	0	3	15
12	12	5	7	5	0	9	19	0	1	6	6	9	12
9	1	20	5	4	0	20	15	0	10	14	20	21	0
8	25	4	5	18	1	2	1	4	29	1	16	16	18
15	12	5	4	0	2	25	0	1	9	3	20	5	0
1	14	4	0	1	3	3	18	5	4	9	20	5	4
0	2	25	0	14	2	1	28	0	9	14	0	1	4
4	9	20	9	15	14	0	20	15	0	20	8	9	19
29	20	8	5	0	9	14	19	20	9	20	21	20	9
15	14	0	9	19	0	1	12	19	15	0	2	5	9
14	7	0	3	5	18	20	9	6	9	5	4	0	9
19	15	0	34	27	27	31	30	32	27	27	33	28	0
20	8	5	0	3	15	12	12	5	7	5	0	9	19
0	19	9	20	21	1	20	5	4	0	1	20	0	4
1	13	5	18	9	7	1	4	4	1	29	3	8	5
22	5	12	12	1	29	8	25	4	5	18	1	2	1
4	28	0	20	8	5	0	8	25	4	5	18	1	2
1	4	0	9	19	0	1	0	16	5	1	18	12	0
3	9	20	25	0	15	6	0	9	14	4	9	1	2

Fig 3.Message into matrix

matrix2 =

1	2	1	3	−4	5	3	6	7	8	−2	3	−6	7
9	1	7	6	4	3	2	1	8	1	2	−3	6	4
2	3	4	−5	6	3	1	4	5	2	7	8	−5	0
0	2	4	6	−8	1	−2	3	4	−5	6	7	8	9
1	2	0	3	5	4	3	7	8	−9	2	−1	2	3
0	1	5	7	8	2	6	1	−2	3	4	5	8	7
−1	2	3	4	6	7	8	1	2	3	−7	1	2	3
2	3	−4	5	6	7	1	8	6	4	3	2	−3	4
1	7	8	6	−7	1	2	−3	4	−5	6	7	1	2
4	5	−6	1	2	3	4	5	6	7	−1	2	0	1
1	2	0	3	4	5	0	6	7	−8	1	2	3	4
3	4	6	7	−5	0	1	2	3	0	−2	1	3	4
2	0	1	2	−3	1	2	3	4	0	1	−2	1	2
−1	2	−3	4	5	6	7	9	2	3	−1	0	2	3

Fig 4. Key matrix

=

208	168	204	288	171	259	194	303	392	−33	74	94	185	278
145	291	44	459	91	439	264	546	542	−27	129	228	193	456
226	310	364	471	78	322	382	297	439	101	190	250	214	394
210	294	429	622	57	466	350	479	575	−10	86	333	427	676
293	522	199	623	492	724	579	788	824	183	128	423	165	610
131	289	173	499	103	533	328	587	586	124	105	337	140	591
126	195	83	298	107	268	163	348	440	−183	131	74	64	256
120	237	68	337	400	462	499	507	471	31	10	119	204	332
393	396	410	544	208	460	330	537	722	266	267	348	48	562
129	548	568	682	425	743	712	720	807	−29	441	820	382	877
198	215	98	398	196	448	269	509	531	136	71	133	71	416
228	340	197	364	191	495	328	555	655	130	52	291	18	432
442	382	142	530	164	447	443	622	793	152	83	79	274	463
218	255	299	404	60	357	346	276	447	237	−149	153	130	391
265	254	196	420	145	307	182	343	450	54	97	117	141	320
185	274	−50	156	509	466	185	595	583	10	294	291	−100	258
238	414	293	563	378	582	370	708	746	−155	434	438	230	585
419	533	457	823	80	704	510	704	982	218	163	402	170	789
269	372	156	493	14	416	305	479	689	6	210	227	118	448
130	267	180	492	312	465	457	391	407	229	−12	239	200	474
532	899	688	1482	118	1039	801	1069	1483	−139	385	758	730	1369
154	262	109	451	328	523	477	540	490	321	47	225	84	482
261	302	434	547	129	398	297	393	604	−185	123	219	379	510
201	218	243	433	141	352	145	438	568	−330	267	240	373	484
182	326	229	569	391	583	370	603	603	221	295	504	174	708
380	402	552	704	−166	297	190	269	655	−196	342	310	435	565
170	275	286	396	−183	157	152	226	432	−254	159	154	215	301
214	333	376	395	43	283	234	309	458	38	345	504	321	497

Fig 5.Decryption matrix

0.61	0.37	−0.27	−0.6	−0.74	0.22	−0.79	−0.72	0.41	0.01	1.23	−0.34	−0.5	0.7
0.56	0.77	−0.19	0.32	0.66	−0.44	−0.43	−0.52	0.22	−0.04	−0.73	−0.31	−2.29	0.98
−0.11	−0.01	0.11	0.13	0.16	−0.09	0.16	0.11	−0.09	−0.07	−0.3	0.12	0.01	−0.07
−0.55	−0.61	0.14	−0.12	−0.26	0.26	0.44	0.6	−0.19	0.04	0.19	0.38	1.58	−0.82
−0.1	−0.06	0.05	0.06	0.16	0.01	0.12	0.13	−0.09	0.01	−0.18	0.08	0.03	−0.16
0.36	0.44	−0.15	−0.03	−0.17	−0.17	−0.32	−0.36	0.25	−0.11	0.22	−0.35	−0.9	0.66
0.16	−0.02	−0.08	−0.27	−0.25	0.18	−0.19	−0.23	0.15	0.04	0.44	−0.12	0.2	0.11
−0.13	−0.15	0.09	−0.04	−0.1	0.04	0.04	0.09	−0.09	−0.02	0.1	0.17	0.38	−0.07
−0.72	−0.61	0.3	0.31	0.32	0.01	0.81	0.78	−0.41	0.11	−0.63	0.42	1.41	−1.06
−0.28	−0.15	0.14	0.25	0.23	−0.09	0.34	0.34	−0.2	0.02	−0.52	0.17	0.29	−0.31
0.07	0.16	−0.02	0.1	0.16	−0.08	−0.09	−0.04	0.06	−0.04	−0.23	−0.13	−0.35	0.19
−0.37	−0.57	0.14	−0.28	−0.56	0.35	0.25	0.3	−0.1	0.1	0.68	0.25	1.53	−0.66
−0.26	−0.07	0.1	0.25	0.17	−0.1	0.27	0.2	−0.16	0.04	−0.37	0.1	0.16	−0.17
0.88	0.78	−0.33	0	0.25	−0.16	−0.73	−0.8	0.33	−0.07	0	−0.51	−2.07	1.04

Fig 6. Inverse matrix

0.61	0.37	−0.27	−0.6	−0.74	0.22	−0.79	−0.72	0.41	0.01	1.23	−0.34	−0.5	0.7
0.56	0.77	−0.19	0.32	0.66	−0.44	−0.43	−0.52	0.22	−0.04	−0.73	−0.31	−2.29	0.98
−0.11	−0.01	0.11	0.13	0.16	−0.09	0.16	0.11	−0.09	−0.07	−0.3	0.12	0.01	−0.07
−0.55	−0.61	0.14	−0.12	−0.26	0.26	0.44	0.6	−0.19	0.04	0.19	0.38	1.58	−0.82
−0.1	−0.06	0.05	0.06	0.16	0.01	0.12	0.13	−0.09	0.01	−0.18	0.08	0.03	−0.16
0.36	0.44	−0.15	−0.03	−0.17	−0.17	−0.32	−0.36	0.25	−0.11	0.22	−0.35	−0.9	0.66
0.16	−0.02	−0.08	−0.27	−0.25	0.18	−0.19	−0.23	0.15	0.04	0.44	−0.12	0.2	0.11
−0.13	−0.15	0.09	−0.04	−0.1	0.04	0.04	0.09	−0.09	−0.02	0.1	0.17	0.38	−0.07
−0.72	−0.61	0.3	0.31	0.32	0.01	0.81	0.78	−0.41	0.11	−0.63	0.42	1.41	−1.06
−0.28	−0.15	0.14	0.25	0.23	−0.09	0.34	0.34	−0.2	0.02	−0.52	0.17	0.29	−0.31
0.07	0.16	−0.02	0.1	0.16	−0.08	−0.09	−0.04	0.06	−0.04	−0.23	−0.13	−0.35	0.19
−0.37	−0.57	0.14	−0.28	−0.56	0.35	0.25	0.3	−0.1	0.1	0.68	0.25	1.53	−0.66
−0.26	−0.07	0.1	0.25	0.17	−0.1	0.27	0.2	−0.16	0.04	−0.37	0.1	0.16	−0.17
0.88	0.78	−0.33	0	0.25	−0.16	−0.73	−0.8	0.33	−0.07	0	−0.51	−2.07	1.04

Fig 6. Inverse matrix

matrix1 =

1	12	8	1	2	5	5	2	0	3	15	12	12	5
7	5	0	15	6	0	5	14	7	9	14	5	5	18
9	14	7	0	1	14	4	0	20	5	3	8	14	15
12	15	7	25	0	9	19	0	1	0	16	18	5	13
9	5	18	0	9	14	19	20	9	20	21	20	9	15
14	0	9	19	0	5	19	20	1	2	12	9	19	8
5	4	0	2	25	0	1	12	8	1	2	5	5	2
0	3	8	1	18	9	20	1	2	12	5	0	20	18
21	19	20	0	9	14	0	20	8	5	0	25	5	1
18	0	32	27	27	32	28	0	20	8	5	0	3	15
12	12	5	7	5	0	9	19	0	1	6	6	9	12
9	1	20	5	4	0	20	15	0	10	14	20	21	0
8	25	4	5	18	1	2	1	4	29	1	16	16	18
15	12	5	4	0	2	25	0	1	9	3	20	5	0
1	14	4	0	1	3	3	18	5	4	9	20	5	4
0	2	25	0	14	2	1	28	0	9	14	0	1	4
4	9	20	9	15	14	0	20	15	0	20	8	9	19
29	20	8	5	0	9	14	19	20	9	20	21	20	9
15	14	0	9	19	0	1	12	19	15	0	2	5	9
14	7	0	3	5	18	20	9	6	9	5	4	0	9
19	15	0	34	27	27	31	30	32	27	27	33	28	0
20	8	5	0	3	15	12	12	5	7	5	0	9	19
0	19	9	20	21	1	20	5	4	0	1	20	0	4
1	13	5	18	9	7	1	4	4	1	29	3	8	5
22	5	12	12	1	29	8	25	4	5	18	1	2	1
4	28	0	20	8	5	0	8	25	4	5	18	1	2
1	4	0	9	19	0	1	0	16	5	1	18	12	0
3	9	20	25	0	15	6	0	9	14	4	9	1	2

Fig 7. Encryption Matrix

Table 2. Comparison Table

Matrix	Characters	Manual Time	Geogebra Time
3 X 3	16	20-25 min(avg)	<1 Min
20 X 20	400	Can't say	1 Min(avg)

The above comparison table shows that this method works efficiently for encryption and decryption with less time for large messages.

V. Conclusion

This paper concludes that the large messages are transferred by providing cryptography technique called encryption and decryption. We have succeeded setting 20X20 matrices in less time by using geogebra open software. Through this approximately 400 characters are encrypted and decrypted. There is a scope of expanding 20X20 matrices using our proposed novel method.

References

[1]. Andrew S. Tanenbaum, Networks Computer, 5th edition,Pearson Education, ISBN-10: 0132553171.

[2]. Muhammad Salam, Nasir Rashid, Shah Khalid,MuhammadRaees Khan, "A NXM Version of 5X5 Playfair Cipher for any Natural Language (Urdu as Special Case)". World Academy of Science, Engineering and Technology 73 2011.

[3]. A. Forouzan and G. Hill, *Data Communications and Networking*, 4th Edition by Behrouz, Feb 9, 2006.

[4]. A. AftabAlam, B. Shah Khalid, and C. Muhammad Salam, "A Modified Version of Playfair Cipher Using 7×4 Matrix" Vol. 5, No. 4, August 2013.

[5]. S.S.Dhenakaran, M. Ilayaraja, "Extension of Playfair Cipher using 16X16 Matrix*"* Volume 48– No.7, June 2012.

[6]. KatholiekeUniversiteit Leuven and IBBT, "Cryptography for Network Security:Failures, Successes and Challenges".

[7]. Dr. James H. Yu &Mr. Tom K. Le, "Internet and Network Security", "Journal of industrial technology",Volume 17, Number 1 - November 2000 to January 2001.

[8]. Kyung Jun Choi, John –In Song, "Investigation of feasible cryptographic Algorithm For wireles sensor network", International conference on ICACT Feb 20-22,2006.

[9]. *Cryptography and Network Security: Principles and Practice*, 4th Edition by William Stallings, Prentice Hall, Nov 26, 2005.

[10]. R.L. Rivest, The MD5 message-digest algorithm, RFC 1321, April 1992.

[11]. O. Dunkelman, N. Keller, A. Shamir, \A practical-time attack on the KASUMcryptosystem used in GSM and 3G telephony," Advances in Cryptology, Proceed- ings Crypto'10, LNCS, T. Rabin, Ed., Springer, Heidelberg, 2010, in print.

[12]. Na Qi Jing Pan Qun Ding, The Implementation of FPGA-based RSA Public-Key Algorithm and Its Application in Mobile-Phone SMS Encryption System, IEEE International Conference on Instrumentation, Measurement, Computer, Communication and Control, 2011, 700-703.

[13]. Ch. Rupa and P.S. Avadhani, Message Encryption Scheme Using Cheating Text, IEEE International Conference on Information Technology, 2009, 470-474.

[14]. Rishav Ray, JeeyanSanyal, Tripti Das, KaushikGoswami, Sankar Das and AsokeNath, A new Randomized Data Hiding Algorithm with Encrypted Secret Message using Modified Generalized Vernam Cipher Method: RAN-SEC algorithm, IEEE Information and Communication Technologies World Congress, 2011, 1211-1216.

[15]. Hongbo Zhou, Mutka and Lionel M. Ni, Multiple-key Cryptography-based Distributed Certificate Authority in Mobile Ad-hoc Networks, IEEE proceedings of GLOBECOM, 2005, 1681-1685.

[16]. http://en.wikipedia.org/wiki/Digital_signature.

[17]. http://searchsecurity.techtarget.com/definition/digital-signature.

