Enhance classic Matrix Cryptography using Three-Pass Protocol

Syed Tariq Shah Waqif[1], Co Author: Assistant Professor Sayed Najmuddin Sadaat[2]
[1] MSCS Faculty of Computer Science Bakhtar University Maiwand169@gmail.com
[2] Faculty of Computer Science Bakhtar University, Kabul, Afghanistan.

Abstract: This reading merge modern and classic cryptographic algorithms then the data security of information become much wakeful authenticity. One of the modern method of cryptography algorithm is Three-Pass Protocol which the sender of message does not distribute the encryption key to the recipient for decryption so each party sender and receiver of the message used their own keys for encryption and decryption so the key doesn’t need to share between them. One of the oldest classical cryptography is Matrix Cipher which use a symmetric key method for message ciphering so in this method the same key used for encryption as well as for decryption process. In this composition the delivery process of sending and receiving messages using the Three-Pass Protocol, while Matrix Cipher algorithm used for encryption and decryption messages process. The outputs from this composition helps the two algorithms to deliver and encrypt plus decrypt the information in safe method.

Keywords: Security, Three-Pass protocol, Matrix Cipher, Encryption, Decryption.

1. Introduction

Securing the information which is transmitting over the internet and there is possibility that attacker steal the information during transmission, so how to make the information secure from unauthorized parties. In the era of modern technology message encryption is the necessity part to ensure that the channels used for communication are protected and decryption become difficult to unauthorized users [10]. Securing the rights of information producer owners by cryptographic technology which execute outstanding roles [13]. Transforming the actual data into scrambled code and all types of data such as text data, photograph data and / or Video data using encryption technique to be secure over a network [11]. Cryptography used key generation method to produce keys for data encryption and decryption [12]. The message which is sending over the internet is needed to be secure during transmission from the attacker in meddle [1]: Data is regularly used cryptographic security method to avoid unauthorized access and integrity. Cryptography has broken into main two sections modern and classic cryptography [4]. One of the modern method of cryptography which is used to provide security for data is Three-Pass Protocol the initial idea of Three-Pass Protocol is that the sender and the receiver used their own private key for encryption as well as decryption, Three-Pass Protocol is encrypts the message by two different private keys and the keys are not distributed between the sender and recipient [2]. There is no necessity for encryption key distribution by transmitter and give access to the receiver. The Classical cryptographic algorithm is using to convert message from readable form to unreadable form and the implementation of classical cryptography is very easy [7]. Anyway, it is painstaking for the old version and weak method in data security process.

Caesar Cipher is one of the oldest classical cryptography, in which the position of letters is changed in alphabetic set according to the size of key or also called ROT algorithm [3]. The problems which still in this classical cryptographic algorithm are utilize single key for all plaintext, Key repetition in cipher text, Very weak against brute force attack and frequency analysis attack. For these current problems, the principle purpose is to provide the strongest security for the data by modern and classical cryptography where Three-Pass Protocol is used to transport the message while Classical cryptographic is executing for encryption and decryption algorithms. The main advantages of my research are to provide the powerful security for data while running in the global network through utilizing classical matrix substitution cryptography for encryption and decryption without giving access to private encryption key to the recipient by help of Three-Pass Protocol process.

2. Related Works

Caesar cipher, which is famous as the shift cipher, is the simplest and most greatly known classical encryption techniques. One of the substitution cipher is Caesar cipher which replaced letters of plaintext in the position of fixed letters of alphabet. For instance, the shift key is 3, D will take the position of A, E hold the position of B and F replaced C and others. The complex schemes of classical encryption is Vigenere cipher which is till used in modern application in the ROT13 system [14]. One of the polyalphabetic substitution form is Vigenere cipher [15] [16]. The encryption scheme of Vigenere cipher was invented by French Blaise De Vigenere in 16th century [17]. The birth of cryptography was to claims related data security issues [18].

a) **Confidentiality**. The data should be accessed only by certain parties.

b) **Authentication**. Sender and receiver of the message need to know that the transmitter of the message is the actual party as we claimed.

c) **Integrity**. The message which sent is guaranteed that the message delivered to the specific recipient without a bit changes occurred. These demands relate to guarantee every message sent definitely reaching the recipient without any part of the message is changed, duplicated, tampered with, altered the order, and added.

The sender and receiver use their own private keys and there is no need of exchanging key between parties by the help of Three-Pass protocol process [18].

3. Theories

The envelopment of these two encryption algorithms theories, such as Matrix cipher and Three-Pass Protocol. However the technique on how to make the single algorithm executes two times in encryption and decryption process is Three-Pass Protocol. The Three-Pass Protocol avoid the sender and recipient to distribute the password in the encryption as well as decryption process.

3.1 Matrix Cipher

Caesar Cipher is one the oldest and most known in the development of cryptography [6]. Matrix cipher is a substitution cipher which is enhance of Caesar cipher cryptography method, Matrix cipher working through matrix of table and hold the characters in the Matrix table for encryption. This technique is also known as a classical cryptography. Matrix cipher cryptography algorithm is much easy to utilize then other cryptography methods. The principal of these classical and modern cryptographic algorithms are changing the characters in the plaintext with specific value assign. Matrix cipher takes some steps to establish cipher text:

- Specify the esteem of the replace letters in the plaintext to convert in the cipher text form.
- Releasing the character from predetermined shift cipher text into plaintext.
- A key is assigned for encryption and key is changing for every rows and columns.
- Key has formula and the formula is (key =k+1) for every rows and columns.
- Matrix is design according to the characters size.

3.2 Three-Pass Protocol

The Framework of a three-pass protocol that allows one party to send message securely to a second party without having to exchange or distribute encryption keys. It is called a three-pass protocol for the exchange three times to authenticate the sender and recipient of the first protocol. This protocol may be realized by utilizing exclusive-OR (XOR) operations [5]. It is developed by Adi Shamir developed around 1980, the basic concept of the three-pass protocol is that each party has the encryption key or a private key and a private decryption. Both sides independently using the key, to encrypt messages first and then to decrypt the message. This protocol works in commutative cipher or LIFO method. Commutative means that the order of encryption and decryption is interchangeable (Encryption A – Encryption B – Decryption A – Decryption) [8].

Figure 1 illustrates the Three-Pass Protocol scheme.

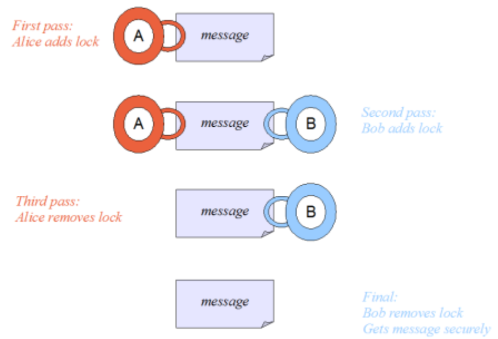


Figure. 1: The Three-Pass Protocol scheme

4. Proposed Work

The objective of this reading, which provide security to the message by using different algorithms where both parties don't need to know the encryption key of each other. Matrix cipher is used for encryption and decryption process. The outputs in the form of cipher text is received by coding process. Matrix Cipher algorithm used for message encryption process where Encryption will be done by sender as well as by receiver in a row consecutively to the message and for the decryption message process the same method performed twice in succession by the receiver and sender of the message.

The text message processed through encryption and decryption process, there are two plus one steps in the process of ciphering and deciphering to the message. The memo which is used in this reading include of numbers from 0 to 9, lowercase, uppercase of English language and also include the Arabic, Pashto, Dari, Urdu languages letters plus numbers for better security the proposed work memo consisted of ASCII table and Extended ASCII table characters to increase the security of proposed work against brute-force attack and Frequency analysis attack which is the big whole in previous research of (Three-Pass Protocol Implementation in Caesar Cipher Classic Cryptography) by Boni Oktaviana in 2016 (IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. III (Jul.-Aug. 2016), PP 26-29 www.iosrjournals.org)[9]. The composition of Three-Pass protocol and Matrix cipher algorithm processes make this opportunity to utilize Modern and Classic cryptography in a time. Three-Pass protocol is using for delivering the messages, while for encryption and decryption processes using Matrix cipher. The user interface flowchart is explaining in Figure1, key generation process, encryption and decryption process in a simulation program.

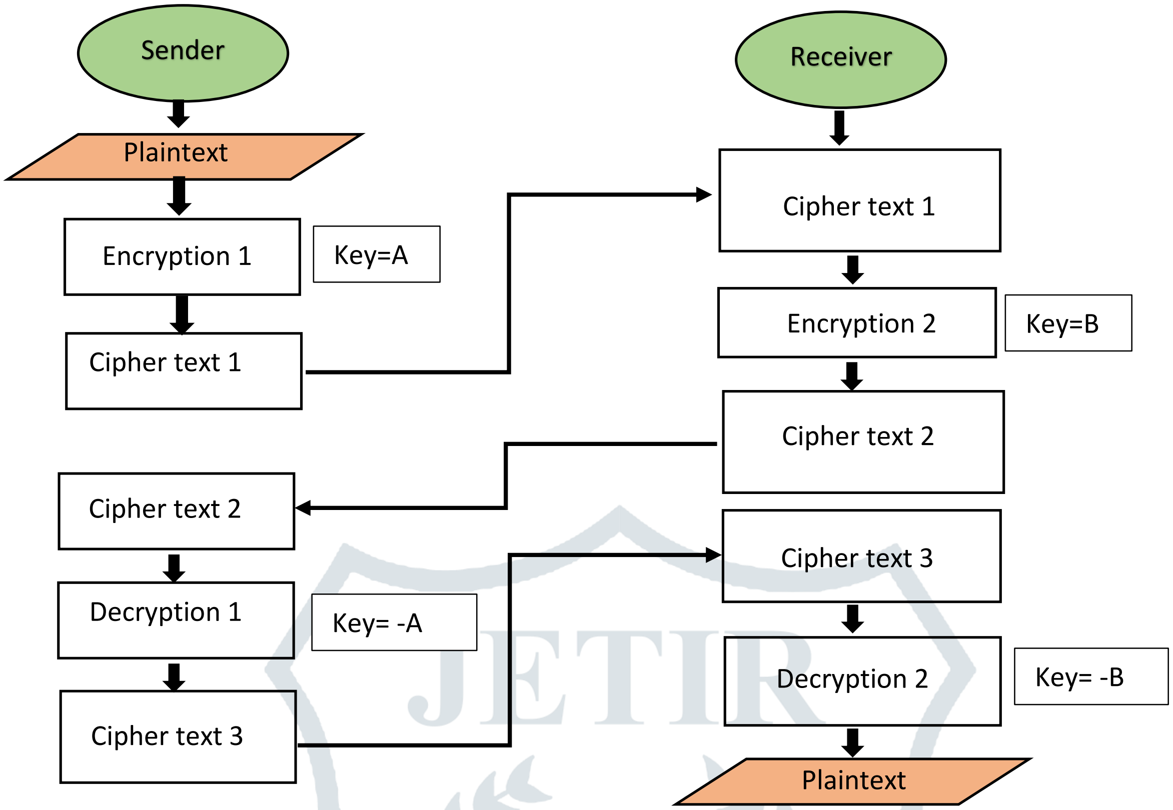
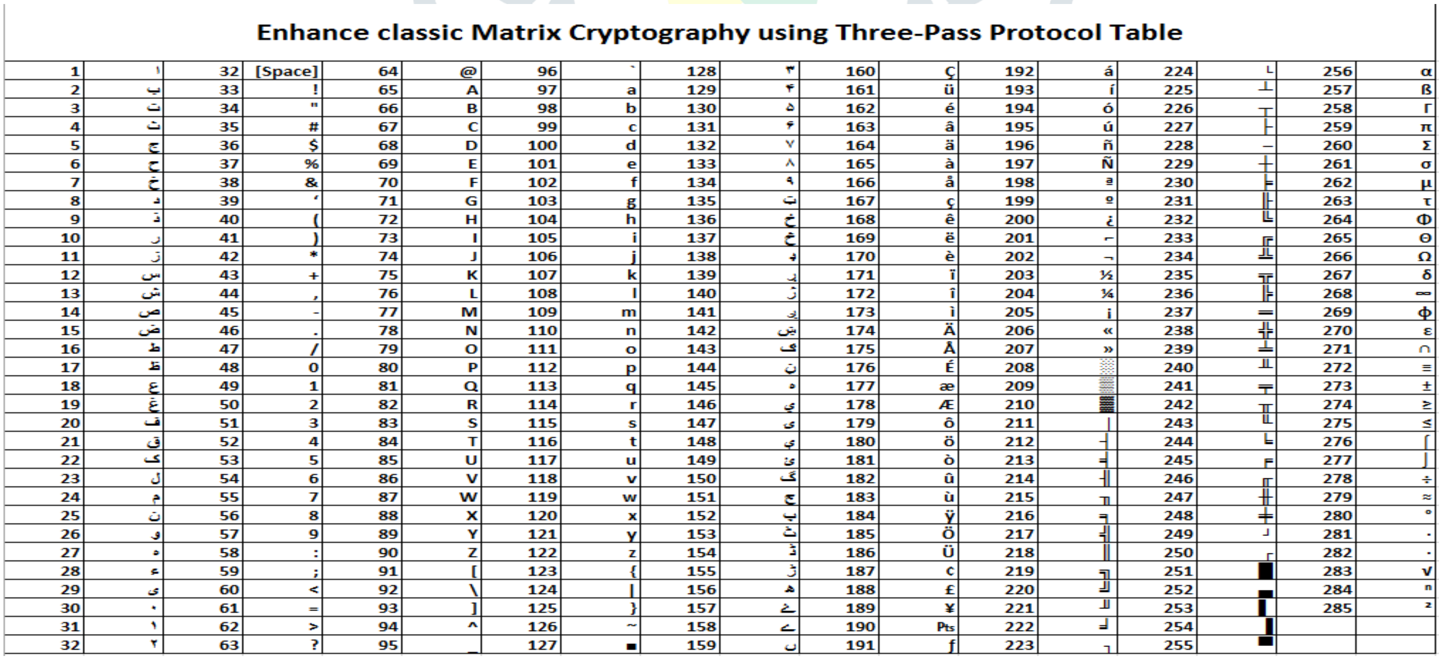


Figure. 2: Three-Pass Protocol Flow Chart

The plaintext is encrypted into cipher text in the first phase of coding. Unauthorized people can't read the cipher text since to decrypt the message by the encrypted key. The encryption procedure result is sent to destination without sharing the cipher key. When the sender sent the message to the recipient in the form of cipher text the receiver encrypt the same message by its private encryption key and send it back to sender of the message after the second encryption process the message reached to sender and the sender decrypt the message by its private key and send it to the catcher while the receiver got the message in the form of cipher text and want to bring the message in the original form the receiver decrypt the cipher text by its own private key.

Table 1. The ordinary character associations with their numerical equivalent



Enhance classic Matrix Cryptography using Three-Pass Protocol Table

1	ا	32	[Space]	64	@	96	`	128	٣	160	Ç	192	á	224	└	256	α
2	ب	33	!	65	A	97	a	129	۴	161	ü	193	í	225	┴	257	ß
3	ت	34	"	66	B	98	b	130	۵	162	é	194	ó	226	┬	258	Γ
4	ث	35	#	67	C	99	c	131	۶	163	â	195	ú	227	├	259	π
5	ج	36	$	68	D	100	d	132	۷	164	ä	196	ñ	228	─	260	Σ
6	ح	37	%	69	E	101	e	133	٨	165	à	197	Ñ	229	┼	261	σ
7	خ	38	&	70	F	102	f	134	٩	166	å	198	ª	230	╞	262	µ
8	د	39	‘	71	G	103	g	135	ٹ	167	ç	199	º	231	╟	263	τ
9	ذ	40	(	72	H	104	h	136	څ	168	ê	200	¿	232	╚	264	Φ
10	ر	41	)	73	I	105	i	137	ځ	169	ë	201	⌐	233	╔	265	Θ
11	ز	42	*	74	J	106	j	138	ډ	170	è	202	¬	234	╩	266	Ω
12	س	43	+	75	K	107	k	139	ړ	171	ï	203	½	235	╦	267	δ
13	ش	44	,	76	L	108	l	140	ژ	172	î	204	¼	236	╠	268	∞
14	ص	45	-	77	M	109	m	141	ږ	173	ì	205	¡	237	═	269	φ
15	ض	46	.	78	N	110	n	142	ښ	174	Ä	206	«	238	╬	270	ε
16	ط	47	/	79	O	111	o	143	ک	175	Å	207	»	239	╧	271	∩
17	ظ	48	0	80	P	112	p	144	ڼ	176	É	208	░	240	╨	272	≡
18	ع	49	1	81	Q	113	q	145	ه	177	æ	209	▒	241	╤	273	±
19	غ	50	2	82	R	114	r	146	ې	178	Æ	210	▓	242	╥	274	≥
20	ف	51	3	83	S	115	s	147	ی	179	ô	211	│	243	╙	275	≤
21	ق	52	4	84	T	116	t	148	ي	180	ö	212	┤	244	╘	276	⌠
22	ک	53	5	85	U	117	u	149	ئ	181	ò	213	╡	245	╒	277	⌡
23	ل	54	6	86	V	118	v	150	گ	182	û	214	╢	246	╓	278	÷
24	م	55	7	87	W	119	w	151	چ	183	ù	215	╖	247	╫	279	≈
25	ن	56	8	88	X	120	x	152	پ	184	ÿ	216	╕	248	╪	280	°
26	و	57	9	89	Y	121	y	153	ټ	185	Ö	217	╣	249	┘	281	∙
27	ه	58	:	90	Z	122	z	154	ڈ	186	Ü	218	║	250	┌	282	·
28	ء	59	;	91	[	123	{	155	ژ	187	¢	219	╗	251	█	283	√
29	ی	60	<	92	\	124	|	156	ھ	188	£	220	╝	252	▄	284	ⁿ
30	٠	61	=	93	]	125	}	157	ۓ	189	¥	221	╜	253	▌	285	²
31	١	62	>	94	^	126	~	158	ے	190	₧	222	╛	254	▐		
32	٢	63	?	95	_	127	■	159	ں	191	ƒ	223	┐	255	▀		

This is the table which is used in Enhance Classic Matrix cryptography using Three-Pass Protocol algorithm by combining modern and classic algorithms to reduce the available risk in classic cryptography.

5. Testing and Implementation

Demonstration of the Three-Pass protocol implementation on Matrix cipher. Let's take the incoming text "**We Trust on One ALLAH**" as a plaintext. The first alteration value is 3. The encryption procedure execute twice. First, the forwarder should cryptograph the message and send it to the receiver. Once the recipient received the message, receiver should cryptograph the message for second times. Let's have a look the illustration.

Key =3 for the first row and for the second row the key will increase with one according to key formula Key = k+1, so for first row key =3 and for second row the key is change from 3 to 4 and for third row key is change from 4 to 5 and so on when the rows are completed then the columns encryption will start and the key will takes from the last row key.

The plaintext to be encrypted is **"We Trust on One ALLAH ".**

The size of characters and spaces are 21 according to the size of characters the matrix will be 5*5 which can hold 25 characters in the extra positions we add lowercase alphabets a b c in sequence as we need.

Let's have a look the illustration.

Table 2.1 The first phase of encryption

Key = k+1	Encryption				
	8	9	10	11	12
3	W	e	T	r	u
4	s	t	o	n	O
5	n	e	A	L	L
6	A	H	a	b	c
7	d	e	f	g	h

First row base encryption in **Table 2.2** the first phase of encryption

Key = k+1	Encryption				
	8	9	10	11	12
3	Z	h	W	u	x
4	w	x	s	r	S
5	s	j	F	Q	Q
6	G	N	g	h	i
7	k	l	m	n	o

In Table 2.2 we see the incoming text will be encrypted using Matrix Cipher. And the encryption process produces "Z h W u x w x s r S s j F Q Q G N g h I k l m n o" as the cipher text but the column base encryption in not done yet.

Table 3.1 The first phase of encryption in column base

Key = k+1	Encryption				
	8	9	10	11	12
3	b	q	a	٣	٧
4	■	۴	}	}	_
5	{	s	P	\	]
6	O	W	q	s	u
7	s	u	w	y	{

In Table 3.1 we see the incoming text will be encrypted using Matrix Cipher. And the encryption process produces "b q a ٣ ٧ ■ ۴ } } _ { s P \ ] O W q s u s u w y {" as the cipher text.

Table 4. The last phase of encryption

Key = k+1	Encryption				
	10	11	12	13	14
5	b	q	a	٣	٧
6	■	۴	}	}	_
7	{	s	P	\	]
8	O	W	q	s	u
9	s	u	w	y	{

First row base encryption in **Table 4.1** the last phase of encryption

Key = k+1	Encryption				
	10	11	12	13	14
5	g	v	f	٨	څ
6	٨	ٿ	۶	۶	e
7	٥	z	W	c	d
8	W	_	y	{	}
9	|	~	٣	٥	٧

In Table 4.1 we see the incoming text will be encrypted using Matrix Cipher. And the encryption process produces "g v f ٨ څ ٨ ٿ ۶ ۶ e ٥ z W e d W _ y { } | ~ ٣ ٥ ٧" as the cipher text but the column base encryption in not done yet.

Table 4.2 The last phase of encryption in column base

Key = k+1	Encryption				
	10	11	12	13	14
5	g	v	f	٨	څ
6	٨	ٿ	۶	۶	e
7	٥	z	W	c	d
8	W	_	y	{	}
9	|	~	٣	٥	٧

Table 4.3 The last phase of encryption in column base

Key = k+1	Encryption				
	10	11	12	13	14
5	q	۴	r	ي	ڇ
6	ڪ	ي	ڪ	ڽ	s
7	ژ	٨	c	p	r
8	a	j	٨	ځ	ڔ
9	٩	څ	ژ	ڪ	ي

Table 4.3 shows the second round of the encryption using shift value 5 in start. The final cipher text would be "q ۴ r ي ڇ ڪ ي ڪ ڽ s ژ ٨ c p r a j ٨ ځ ڔ ٩ څ ژ ڪ ي". It is the last set of the encryption process. To read the message, the participants must decrypt the final cipher text twice.

Table 5 The first phase of decryption

Key = k-1	Decryption				
	- 8	- 9	- 10	- 11	- 12
- 3	q	۴	r	ي	ڇ
- 4	ڪ	ي	ڪ	ڽ	s
- 5	ژ	٨	c	p	r
- 6	a	j	٨	ځ	ڔ
- 7	٩	څ	ژ	ڪ	ي

First row base decryption in **Table 5.1** the first phase of decryption

Key = k-1	Decryption				
	- 8	- 9	- 10	- 11	- 12
- 3	n	~	o	ڪ	ي
- 4	ڔ	ښ	ڔ	ژ	o
- 5	ٿ	٣	^	k	m
- 6	[	d	■	٥	٨
- 7	■	٥	٨	ځ	ڔ

In Table 5.1 we see the incoming text will be decrypted using Matrix Cipher. And the decryption process produces "n ~ o ڪ ي ڔ ښ ڔ ژ o ٿ ٣ ^ k m [d ■ ٥ ٨ ■ ٥ ٨ ځ ڔ" as the cipher text but the column base decryption in not done yet.

Table 5.2 The first phase of decryption in column base

Key = k-1	Decryption				
	- 8	- 9	- 10	- 11	- 12
- 3	f	u	e	۷	خ
- 4	۶	۸	۴	۴	c
- 5	■	w	T	`	a
- 6	S	[	u	w	y
- 7	w	y	{	}	■

In Table 5.2 we see the incoming text will be decrypted using Matrix Cipher. And the decryption process produces “f u e ۷ خ ۶ ۸ ۴ ۴ c ■ w T ` a S [u w y W y { } ■” as the cipher text.

Table 6 The first phase of decryption

Key = k-1	Decryption				
	- 10	- 11	- 12	- 13	- 14
- 5	f	u	e	۷	خ
- 6	۶	۸	۴	۴	c
- 7	■	w	T	`	a
- 8	S	[	u	w	y
- 9	w	y	{	}	■

First row base decryption in **Table 6.1** the last phase of decryption

Key = k-1	Decryption				
	- 10	- 11	- 12	- 13	- 14
- 5	a	p	`	■	۶
- 6	}	■	{	{	]
- 7	x	p	M	Y	Z
- 8	K	S	m	o	q
- 9	n	p	r	t	v

In Table 6.1 we see the incoming text will be decrypted using Matrix Cipher. And the decryption process produces “a p ` ■ ۶ } ■ { {] x p M Y Z K S **m** o q **n** p r t v” as the cipher text but the column base decryption in not done yet.

Table 7 The last phase of decryption in column base

Key = k-1	Decryption				
	- 10	- 11	- 12	- 13	- 14
- 5	a	p	`	■	۶
- 6	}	■	{	{	]
- 7	x	p	M	Y	Z
- 8	K	S	m	o	q
- 9	n	p	r	t	v

Table 7.1 The very last phase of decryption in column base

Key = k-1	Decryption				
	- 10	- 11	- 12	- 13	- 14
- 5	W	e	T	r	u
- 6	s	t	o	n	O
- 7	n	e	A	L	L
- 8	A	H	a	b	c
- 9	d	e	f	g	h

At the end of decryption from both parties’ sender and receiver we got our original plaintext.
“We Trust on One ALLAH abcdefgh” just remove the last sequence of alphabets. ”We Trust on One ALLAH”.

6. Conclusion

The very first generation of encryption to make text message unreadable is Caesar cipher also known as classical cryptography which has many versions and lots of them the techniques till vulnerable against brute-force attack and frequency analysis attacks. Through merging Three-Pass Protocol and one of the classical cryptography Matrix Cipher algorithm secure the classical cryptography and avoid the sender and receiver to distribute the encryption key between each other. Classical cryptography is still vulnerable in some phases.

References

[1]. A. P. U. Siahaan, "Factorization Hack of RSA Secret Numbers," International Journal of Engineering Trends and Technology, vol 37, no.1,pp.15-18,2016

[2]. M. Reza dan M. A. Budiman, "Simulasi Pengamanan File Teks Menggunakan Algoritma Massey-Omura," Jurnal Dunia Teknologi Informase, vol. 1, no. 1, pp. 20-27,2012.

[3]. A. Dony, Pengantar llmu Kriptogafi Teori Analisis dan implementasi, Yogyakarta: Andi Offset, 2008.

[4]. Mollin, An Introduction to Cryptography. Second Edition, Taylor & Francis Group, 2007.

[5]. Y. Kanamori dan S. –M. Yoo, "Quantum Three-pass protocol: key Distribution Using Quantum Super Position States," International Journal of Network Security & Its Applications, vol, 1, no. 2, pp. 64-70,2009.

[6]. B. Oktaviana, "Komvinasi Vigenere Cipher Dengan Caesar Cipher Dalam Three-Pass Protocol," Tesis. Pasca Sarjana Teknik Informatika USU, Medan, 2012.

[7]. A. P. U. Siahaan, "RC4 Technique in Visual Cryptography RGB Image Encryption," International Journal of Computer Science and Engineering, vol. 3, no. 7, pp. 1-6, 2016.

[8]. A. P. U. Siahaan, "Three-Pass Protocol Concept in Hill Cipher Encryption Technique," International Journal of Science and Research, vol, 5, no. 3, 2016.

[9]. *IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. III (Jul.-Aug. 2016), PP 26-29.*

[10]. Kester, Quist-Aphetse. "A cryptosystem based on Vigenere cipher with varying key." International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) [Online], 1.10 (2012): pp: 108-113. Web. 16 Jan. 2013.

[11]. Aniket Kesharwani, Hemant Gupta, Survey on Data Hiding in Encrypted Images, International Research Journal of Engineering and Technology (IRJET). 2015; 2(3): 144 – 150.

[12]. Harshala B. Pethe, Dr. S. R. Pandi. A Survey on Different Secret Key Cryptographic Algorithms.
IMBRD's Journal of Management and Research. 2014; 3(1): 142 – 150.

[13]. Dr. S. Arul Jothi, "Evaluation of Symmetric Key Cryptosystem Based On Randomized Key Block Cipher Algorithm to Cryptanalytic Attacks." IOSR Journal of Engineering (IOSRJEN), vol.09, no. 02 2019, pp. 01-04.

[14]. Quist-Aphetsi Kester, "A hybrid Cryptosystem Based on Vigenere Cipher and Columnar Transposition Cipher" International Journal of Advanced Technology & Engineering Research (IJATER), ISSN No: 2250-3536, vol.3, 1, Jan. 2013.

[15]. Bruen, Aiden A. & Forcinito, Mario A. (2011). Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century jobn Wiley & Sons. P. 21. ISBN 978-1-118-03138-4.http://books.google.com/boks?id=fd2LtVgFzoMC&pg=PA21.

[16]. Martin, Keith M. (2012). Everyday Cryptography. Oxford University Press. P. 142. ISBN 978-0-19-162588-6.http://books.google.com/books?id=1NHli2uzt_EC&pg=PT142.

[17]. Sanjeev Kumar Mandal et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (4), 2016, 2096-2099.

[18]. Robbi Rahim, "Study of Three Pass Protocol on Data Security" international journal of science and research (IJSR), ISSN(Online): 2319-7064, index Copernicus value (2013): 6.14, impact factor (2015): 6.391.