International Journal of Computer Science & Communication (ISSN: 0973-7391)
Volume 10 • Issue 2 pp. 201-210 March 2019 - Sept 2019 www.csjournals.com

Play-Fair Encryption Algorithm – A Review

Sakshi Agarwal[1], Dr. Gaurav Agarwal[2]
M.tech Scholar[1], Head of Deptt[2]
Department of Computer Science, Invertis University, Bareilly, INDIA

Abstract: Cryptography is an art of secure information that deals with the encoding and decoding of messages which enhances the security of the data at both ends. In cryptography there are so many algorithms that can encode the plain text into cipher text which can be decode to get the plain text again. The various algorithms are RSA(Rivest, Shamir, Aldeman), DES (Data Encryption Standard), Play-fair cipher and Vignere cipher and Hill Cipher. The traditional Play fair cipher has 5*5 matrix in which the position of I/J is same and only the 26 alphabets of English they used. In this paper, we deal with the enhancement of traditional play-fair as by using some more special characters, numbers and small letters of English alphabet.

1.INTRODUCTION

As the development in the modern world the security of the data is the major concern in communication devices and the Internet. Encryption is a process ofconverting messages, information or data into a form unreadable by anyone except the intended recipient.The root of the word encryption—crypt—comes from the Greek word kryptos, meaning hidden or secret[5].

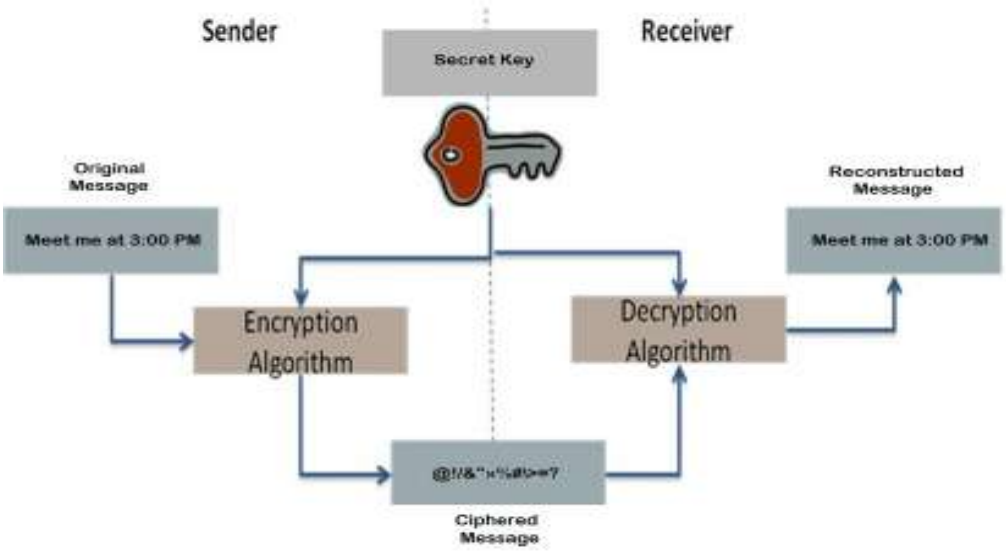


Fig 1: Encryption And Decryption Process Of A Cipher[7]

In order to provide a safety, security and privacy, we bound 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, Symmetric Key Cryptography and Asymmetric Key Cryptography. InSymmetric Key Cryptography a single key is shared between sender and receiver. The sender and the receiver uses' the same shared key and encryption algorithm to encrypt the message and decryption algorithm to decrypt the message. In Asymmetric Key Cryptography each user is having own pair of keys, public key and private key. The public key is shared among 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 while the receiver use his own private key to decrypt the message.

International Journal of Computer Science & Communication (ISSN: 0973-7391)
Volume 10 • Issue 2 pp. 201-210 March 2019 - Sept 2019 www.csjournals.com

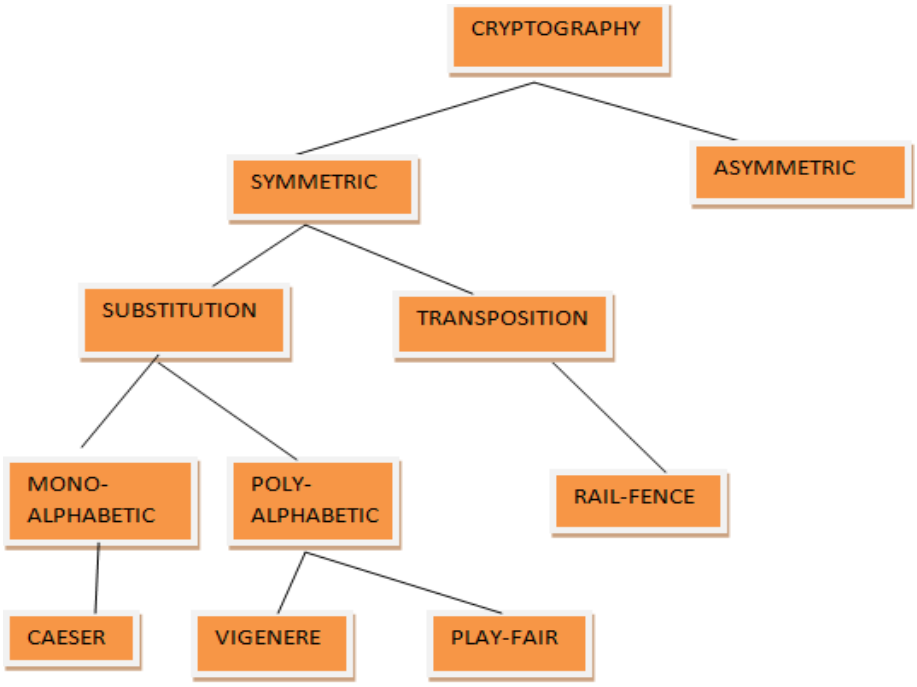


Fig2: Classification of Cryptography Techniques

Mono-alphabetic substitution is a cipher in which a character inthe plaintext is always changed to the same character in the cipher-text. The well-known example of Mono-alphabetic substitution cipher is the CAESAR cipher. In polyalphabetic substitution cipher a single character in the plaintext is changed to many characters in the cipher-text. The well-known example of polyalphabetic substitution cipher is VIGENERE cipher& PLAY-FAIR cipher which changes a single character in the plaintext into many characters in the cipher-text by considering the position of character in the plaintext. In transposition cipher the characters in the plaintext are swapped to get the cipher-text i.e. the characters retain their plaintext form but their position is changed. The plaintext is organized into two dimensional table and columns are interchanged according to a predefined key[1].The well-known example of transposition cipher is RAIL-FENCE cipher.

2. TRADITIONAL PLAY-FAIR CIPHER

Play-fair is a poly-alphabetic substitution cipher. Play-fair is digraph substitution cipher which uses a 5×5 matrix, in which the key word 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[1].The matrix of the play-fair is:

A	B	C	D	E
F	G	H	I/J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

FIG 3: ORIGINAL MATRIX OF PLAY-FAIR CIPHER

The process of encrypting the plain text into cipher text begins after the construction of key matrix. While encrypting the text in Play-fair cipher algorithm following rules are used:

1. Convert the given plaintext into digraphs ensuring that any repetitive plaintext letters that are in the same pair are separated with a filler letter, "X". Also for any standalone letter at the end would be paired by "X".
2. Each plaintext letters are replaced by the character lying on their right if the letters of diagraph being encrypted lay in the same row of key matrix.
3. Each plaintext letters are replaced by the character lying below them if the letters of diagraph being encrypted lay in the same column of key matrix.
4. Each plaintext letters are replaced by character lying in its row and the in the column of the other character if the letters of diagraph being encrypted lay in the different row and column of key matrix.

The process of decrypting cipher text into plain text in Play-fair cipher algorithm follows the same rules but it substitutes with the letter on the left or above instead of right and below as done during encryption[3].

3. LITERATURE SURVEY

3.1A Survey Paper on Play-fair Cipher and its Variants

This paper deals with the fact that all the encryption algorithm tested by the different attacks which define their strength, security and safety of data at both ends. The some attacks are Brute Force Attack, Avalanche Effect and Cipher-text Solely Attack.The parameters on which these attacks are tested:
(a)Key domain size for brute force attack
(b)Number of diagrams need to be searched for cipher-text only attack and
(c)The probability of occurrence of an element for frequency analysis attack.

TABLE 1: COMPARISON ON DIFFERENT FACTORS

Authors / Parameters	Key Domain Size	Number of diagrams for cipher text	Probabilityof occurrence of letters
1.Srivastava & Gupta	64!	4096	0.016
2.Verma et.al	64!	4096	0.016
3.Chand Bhattacharya	36!	1296	0.028
4.Dhenakaran & Ilayaraja	256!	65536	0.004
5.Hans et.al	26!*24*24	Difficult	Difficult

3.2Genetic Extension of Play-fair Cipher Using Modified Matrix

In this paper they describe about the modification in the traditional play-fair matrix, as it was of 5*5 matrix in which the alphabet of I/J uses the same place but they modified by separating the place of I&J along with it they add the smallletters of alphabet, the symbol & and numbers(0-9) as a matrix of 9*7 over them they applied the three basic operations of genetic algorithm i.e; population generation,cross-over mutation. Their proposed matrix is

TABLE 2: PROPOSED MATRIX

&	0	1	2	3	4	5	6	7
8	9	A	B	C	D	E	F	G
H	I	J	K	L	M	N	O	P
Q	R	S	T	U	V	W	X	Y
Z	a	b	c	d	e	f	g	H
i	j	k	l	m	n	o	p	Q
r	s	T	u	v	w	x	y	Z

3.2.1 Encryption algorithm

The process of encrypting plain text into cipher text according to proposed Play-fair cipher algorithm:

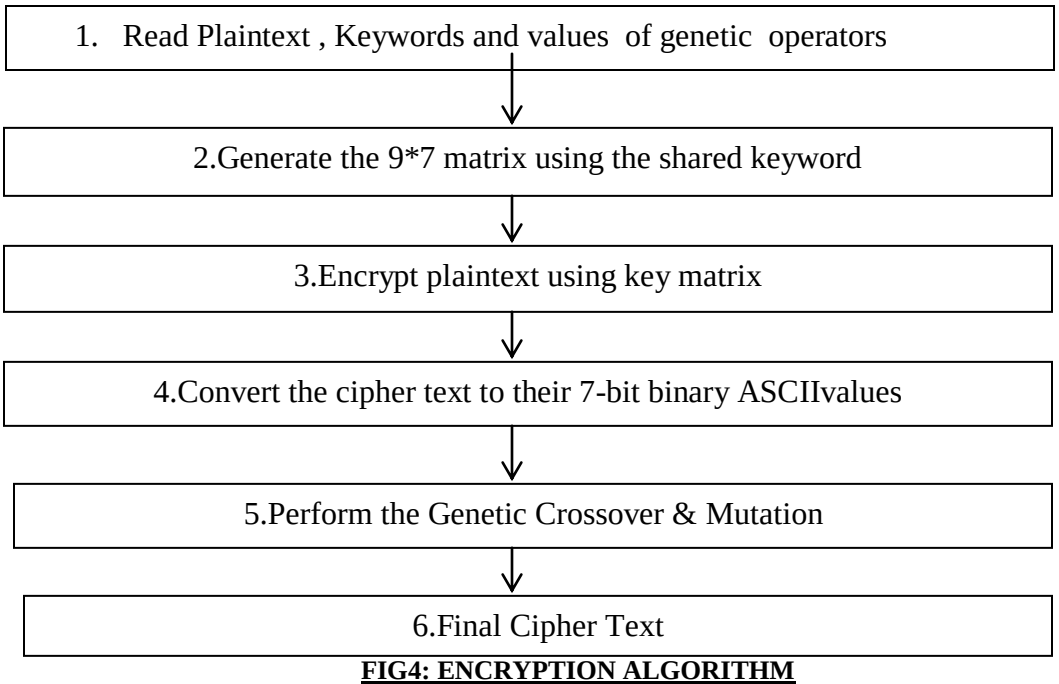


FIG4: ENCRYPTION ALGORITHM

3.2.2Decryption algorithm

The process of decrypting cipher text into plain text according to proposed Play-fair cipher algorithm.

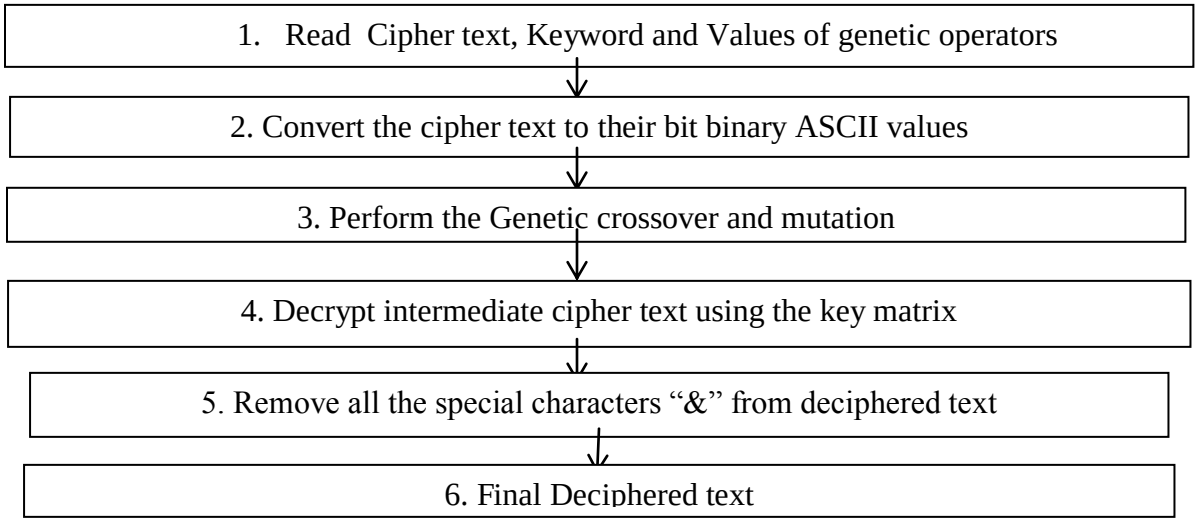


FIG5: DECRYPTION ALGORITHM

International Journal of Computer Science & Communication (ISSN: 0973-7391)
Volume 10 • Issue 2 pp. 201-210 March 2019 - Sept 2019 www.csjournals.com

3.2.3 Illustration of the Cipher

Let the keyword be "S69MftJrwAnqBJ" then the key matrix for keyword.

S	6	9	M	f	t	J	r	w
A	N	Q	B	&	0	1	2	3
4	5	7	8	C	D	E	F	G
H	I	K	L	N	O	P	Q	R
T	U	V	W	X	Y	Z	a	b
c	d	e	g	h	i	J	k	l
m	o	p	s	u	v	X	y	z

Now we encrypt and decrypt the message "Sadiq Nisar 7" using proposed play-fair cipher.
Encryption process:
Plaintext: Sadiq Nisar 7
Diagraphs Formation:Sa di qN is ar 7&
Intermediate Cipher text: rT ej &K gv k2 Cq

Sa	di	qN	is	ar	7&
⬇	⬇	⬇	⬇	⬇	⬇
rT	ej	&K	gv	k2	Cq

Now the first digraph is rT, Hence
r-114- 1110010
T- 84- 1010100
Here the crossover point is 3rd bit and the mutation point is 6th bit so after performing genetic operations we get,
r->1110110-118-v
T->1010000-80-P
Similarly we perform genetic operation on the remaining intermediate cipher text.
Final Cipher text: vPhg)Ddu`9Cq
Decryption process:
Cipher text: vP hg) Ddu `9 Cq
Converting to 7 bit binary ASCII value and performing genetic operations
v -118-1110110->1110010-114- r
P - 80-1010000->1010100- 84- T
Similarly we get,
Intermediate deciphered text: rT ej &K gv k2 Cq
Now we decipher it using ke matrix
Deciphered text:Sa di qN is ar 7&

rT	ej	&K	gv	k2	Cq
⬇	⬇	⬇	⬇	⬇	⬇
Sa	di	qN	is	ar	7&

3.3 Suggested Approach to Embedded Play-fair Cipher Message in Digital Image

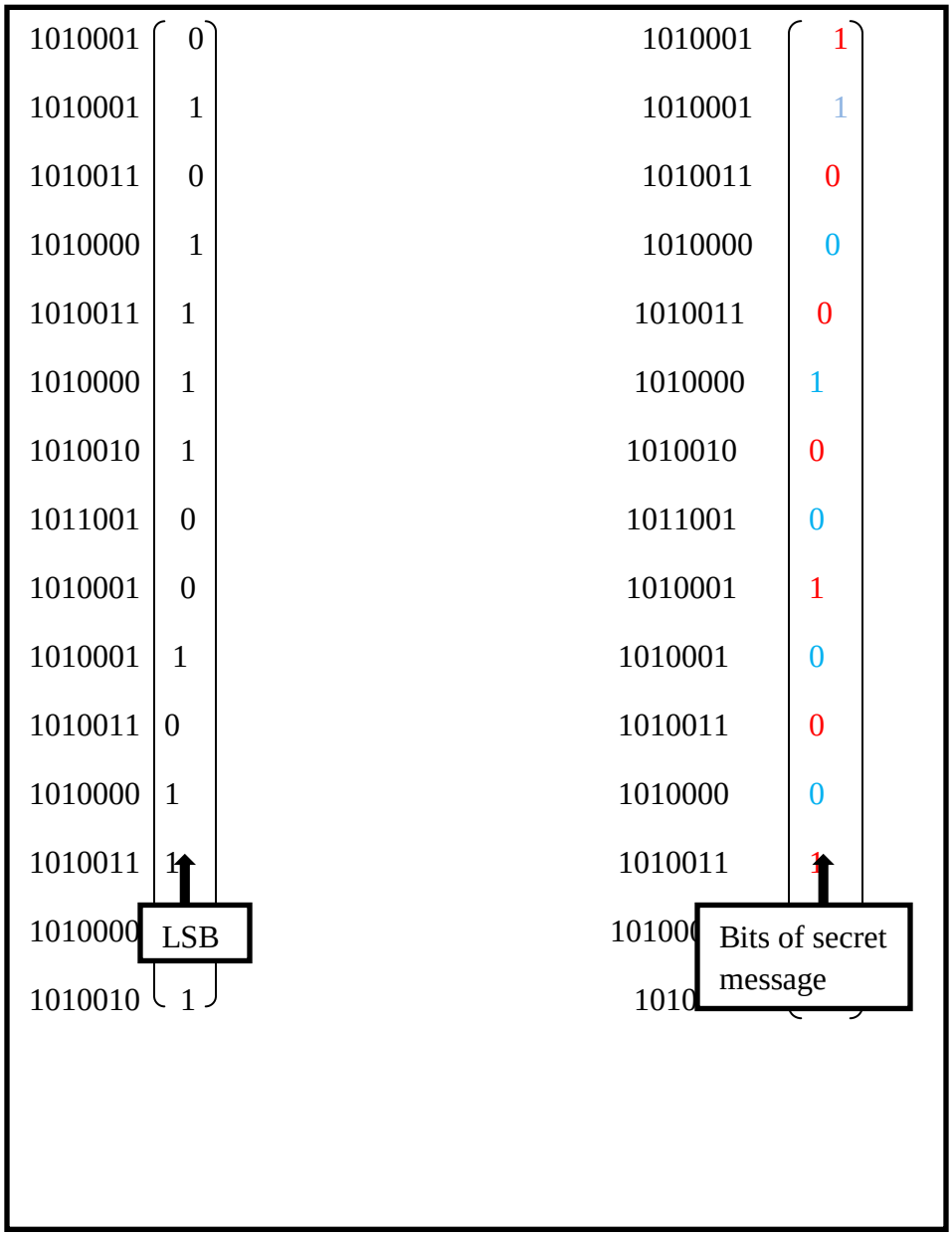
In this paper they deal with the term cyptography and stegnography over the image, by using two layers of security to maintain the privacy, confidentiality and accuracy of the data. First layer is cryptography where the message is encode in play-fair method and second layer is steganography where the encoded message is embedded in cover image. The steps of proposed algorithm are:
1- Enter the secret key for play-fair method.
2- Select the cover image.
3- Enter the message.
4- Encode the message in play-fair using the entered secret key.

5- Convert the message characters to the ASCII code.
6- Convert the ASCII code to the binary system (series of zeros and ones) and find the row and Column of the binary array.
7- Convert the cover image to binary system.
8- Embedded the encoded message bits in the pixels bits of cover image.
9- Return the cover image to decimal system.
10- Send stegno image in unsecure channel.

3.3.1APPLYING THE ALGORITHM'S STEPS IN MATLAP R2010a

The secret key will be "CIPHER". The enciphering diagram becomes
- The cover image will be "img.jpg"
- the secret message will be "HI" the Play-Fair = EP.
- ASCII code = (69 80)
- Binary system "1000101 ","1010000".

-insert the bits of secret message in the cover image



3.4An Approach for Enhancing theSecurity of Play-fair Cipher

In this paper they define the security of data in two steps at both ends by using 6*6 matrix instead of 5*5 matrix .They used the double encryption and the decryption over the data by applying play-fair and vigenere cipher along with random number generator which enhances the complexity of algorithm and the security of data.

Steps for Encryption

1. The alphabets and numbers are arranged in 6x6 Play-fair key matrix based on keyword.
2. Generate 6x6 unique random number matrix using the linear congruential generator methods.
3. Map the Play-fair key matrix with the random number matrix.
4. Encrypt the plain text P using Vigenere cipher with key k1 and get immediate result X
5. Then this result encrypt using Play-fair cipher with keyword k2 and get cipher-text C
6. Find the corresponding number to cipher-text C, the sequence of these number is transmit to receiver.

Steps for Decryption

1. Receiver receive the sequence of numbers.
2. Find the cipher-text C corresponding to sequence of number.
3. Decrypt the ciphertext C using the Play-fair cipher with keyword k2 and get intermediate result X.
4. And then X is decrypted by vigenere cipher with key k1 and get plaintext P.

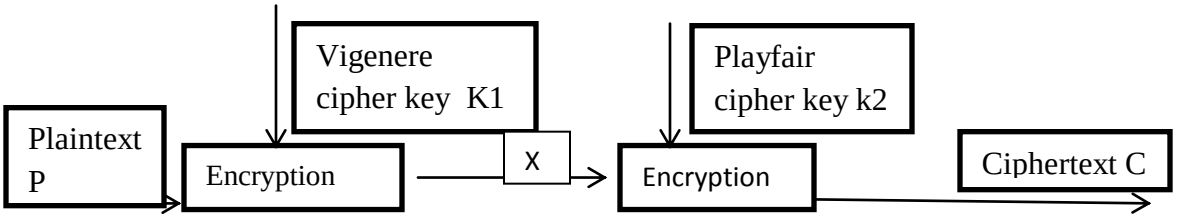


FIG6: ENCRYPTION USING PLAY-FAIR & VIGENERE CIPHER

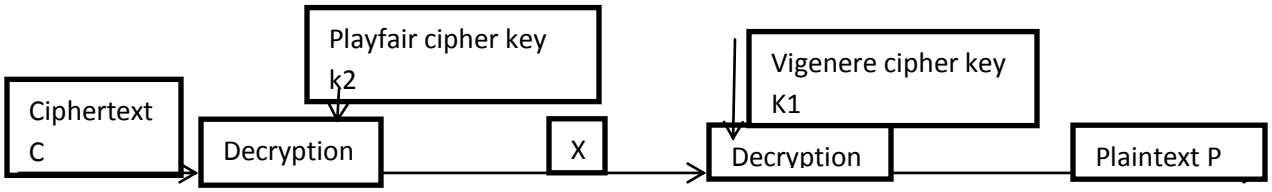


FIG7: DECRYPTION USING PLAY-FAIR & VIGENERE CIPHER

3.5 3D (6 X 6 X 3) – Play-fair Cipher

In this paper they modified the traditional digraph of 5*5play-fair matrix as a tri-graphof 6*6*3 in which they separate the place of I/J ,the small letters of alphabet(a-z) ,special case letters(46) and numbers(0-9).They proposed the 3 different floor for the encryption and the decryption of text.

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

Floor-2					
a	b	c	d	e	f
g	h	i	j	k	l
m	n	o	p	q	r
s	t	u	v	w	x
y	z	!	@	#	$
%	^	&	*	(	)

Floor-3					
_	-	=	[	]	\
{	}	|	;	:	‘
“	<	>	,	£	/
?	~	¬	¡	«	»
|	°	·	¥	€	„
…	¨	©	®	¸	÷

Algorithm for Encryption

Plain Text Tri-graph	Plain Text Tri-graph			Cipher Text Tri-graph
	1st Letter	2nd Letter	3rd letter	
1st Letter	Row	Column	Floor	1st Letter
2nd Letter	Floor	Row	Column	2nd Letter
3rd letter	Column	Floor	Row	3rd letter

Algorithm for Decryption

Cipher Text Tri-graph	Cipher Text Tri-graph			Plain Text Tri-graph
	1st Letter	2nd Letter	3rd letter	
1st Letter	Row	Floor	Column	1st Letter
2nd Letter	Column	Row	Floor	2nd Letter
3rd letter	Floor	Column	Row	3rd letter

4. Proposed Work

On the basis of the study of different play-fair cipher encryption by the different authors gives the result as:

Authors	Result
1.A Survey Paper on Play-fair Cipher and its Variants	It describes about the various factors on which the play-fair encryption can be tested as the key domain size, no. of diagram and the probability of occurence of letter along it we can test the play fair encryption on avalanche effect.
2.Genetic Extension of Play-fair Cipher Using Modified Matrix	It describes about the updated version of the play-fair cipher encryption by drawing 9*7 matrix by applying the operation of genetic mutation and crossover for both the encryption and decryption.
3.Suggested Approach to Embedded Play-fair Cipher Message in Digital Image	It presents a technique for protect the data through using cryptography and steganography. The cryptography stage is using Play fair cipher to encrypted the secret message. In steganography stage convert Play-fair cipher text to binary and store the first bit in every letter in secret message in the LSB of pixel in the image and then the second bit in every letter embedded in the LSB of pixel and continue so until the last bit in last letter in the secret message.
4.An Approach for Enhancing the Security of Play-fair Cipher	It present securetransmission of message by modified version of Playfair cipher with Random number generator methods combining with Vigenere cipher.For the encryption, first encrypt the plaintext by vigenere cipher, and then result encrypt by playfair cipher. And result is called ciphertext. After that we are mapping random numbers to ciphertext and corresponding numbers will be transmitted to the recipient instead of alphabetical letter.
5.3D (6 X 6 X 3) – Play-fair Cipher	It deal with the development of 3D(6*6*3) matrix by designing different floor with the different letter and alphabet in each floor for the encryption and decryption.
6.SURVEY PAPER ON THE PLAY-FAIR ENCRYPTION ALGORITHM	We analyze the performance of the playfair encryption by comparing the existing technique on the different parameters as space complexity ,time complexity etc.

5. Conclusion

The play-fair cipher encryption is a substitution technique in which message encrypted in the form that the intruder cannot retrieve the message .In the traditional play-fair cipher technique the matrix of 5*5 is given in that the only 25 letters placed where the J/I occupied the same place, which degrade the message form .So to overcome the problem off traditional matrix ,the various authors used the different matrices in that all the special letters ,small alphabets and the numerical values inserted so that the all information can get retrieved.

6. References

[1]A. Aftab Alam, B. Shah Khalid, and C. Muhammad Salam," A Modified Version of Play-fair Cipher Using 7×4 Matrix International Journal of Computer Theory and Engineering, Vol. 5, No. 4, August 2013.

[2] Lecture Hadab Khalid Obayes," Suggested Approach to Embedded Play-fair Cipher Message in Digital Image", Hadab Khalid Obayes, Int. Journal of Engineering Research and Applications www.ijera.com ISSN: 2248-9622, Vol. 3, Issue 5, Sep-Oct 2013, pp.710-714

[3]Mohammad Sadiq Nisar Siddiqui,Siddhartha Sankar Biswas,Parul Agarwal"Genetic Extension of Play-fair Cipher Using Modified Matrix",International Journal of Computer & Mathematical Sciences IJCMS ISSN 2347 – 8527 Volume 6, Issue 6 June 2017

[4]R.Deepthi,"A Survey Paper on Play-fair Cipher and its Variants "International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 04 Issue: 04 | Apr -2017 www.irjet.net

[5] Sarita Singh & Abhishek Dixit," An Approach for Enhancing the Security of Play-fair Cipher" Imperial Journal of Interdisciplinary Research (IJIR) Vol-3, Issue-6, 2017 ISSN: 2454-1362, http://www.onlinejournal.in.

[6]"Safwat Hamad _ Amal Khalifa _ Ahmed Elhadad _ S. Z. Rida" A Modified Play-fair Cipher for Encrypting Digital Images J. of Communication & Computer. Eng. Copyright©Modern Science PublishersISSN 2090-6234 www.m-sciences.comVolume 3, Issue 2, 2013, Pages 1:9

[7] "Ashish, Fariya", "Naz 3D (6 X 6 X 3) - Playfair Cipher",International Conference of Advanced Research & Innovation 2016.