Table of Contents

Table of Figures

Abstract.

This report provides an in-depth review of cryptographic algorithms, with an emphasis on the Playfair Cipher and its modified equivalent. Beginning with an overview of the basic concepts of cryptography, the report digs into the historical and theoretical foundations that encourage secure communication. The second section focusses on the Playfair Cipher, describing its algorithmic operations, use of fragments, and its historical significance. The Playfair Cipher's merits and imperfections are evaluated critically. To address these identified flaws, the third section presents the Modified Playfair Cipher, which includes changes to the algorithm to enhance resistance against cryptographic attacks. The fourth section describes the thorough testing procedures used to evaluate both ciphers' performance and security features. Comparative examinations of the Playfair Cipher and its modified opposition demonstrate their unique advantages and flaws allowing for a deeper comprehension of their practical applications. The report wraps up by summarizing major findings and highlighting the significance of careful cryptographic decisions in guaranteeing secure communication.

1. Introduction.

Security can be defined as freedom from poverty or desire, as well as precautions to prevent theft and espionage. Fischer and Green define security as a safe and reliable environment that allows individuals or groups to pursue their goals without disruption or fear of harm. Traditional definitions of security include private services which protect people, information, and assets for personal or collaborative safety. (Brooks, 2010)

CIA Triad and its role in information security.

The CIA triad, which represents confidentiality, integrity, and availability, is a concept aimed to guide an organization's information security (infosec) policy. (Cameroan Hashemi-Pour, 2023)

Let's breakdown the components of the CIA triad:

Figure 1: CIA Triad. (Jussi Nikander, 2020)

- **Confidentiality:**
  Roughly equivalent to privacy, confidentiality measures are designed to prevent sensitive information from unauthorized access attempts. It ensures that only authorized individuals have access to the sensitive data.

- **Integrity:**
  Data must remain consistent, accurate, and trustworthy throughout its entire existence. Data must not be tampered, modified in transit, and precautions must be taken to ensure it cannot be altered by unauthorized individuals.
- **Availability:**
  Information should be consistent and easily available to authorized individuals in need. This includes correctly maintaining the hardware, technical infrastructure, and systems that store and show the data.

The CIA triangle is a core concept in information security, and it is frequently expanded to include other principles such as authenticity, non-repudiation, and accountability. Organizations that implement the CIA principles can develop a robust and comprehensive strategy to information security, minimizing risks and protecting their valuable assets from different attacks. This approach is also applicable to a variety of fields, including computer networks, cloud services, databases, and communication systems.

Introduction to Cryptographic Systems

Cryptography is the science of using mathematical algorithms to encrypt or decrypt a data. It enables you to store or transmit sensitive information across the insecure network so that it cannot be read just in case if someone gain the access to the information except the authorized recipient. In order to encrypt a plaintext, a cryptographic algorithm combines with a key which can be a word, integer or phrase. The durability of the encrypted data is dependent with the two factors i.e. strength of the cryptographic algorithm and key’s secrecy.

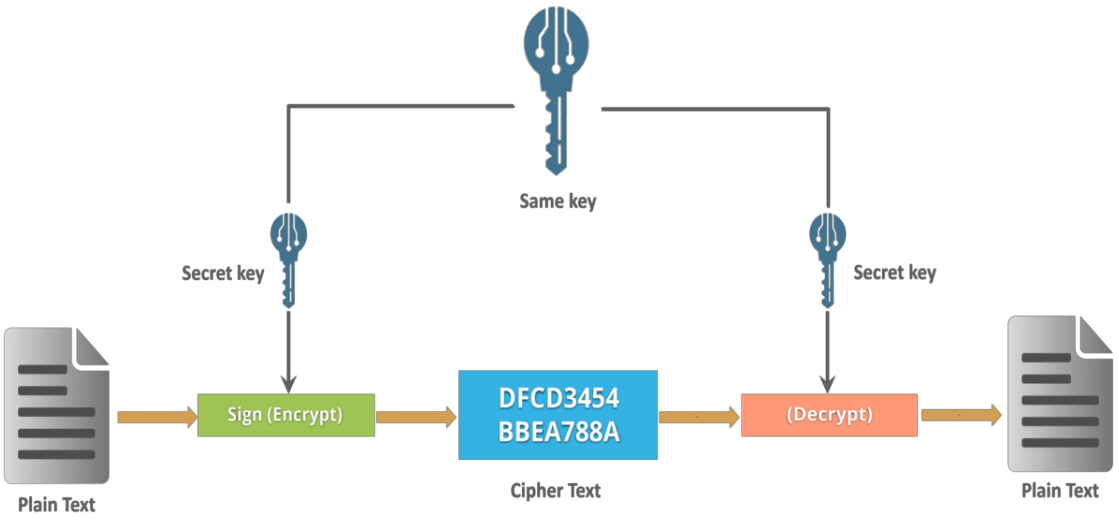


Figure 2: Cryptography Process. (Shashank, 2023)

Key terminologies in Cryptography.

Encryption: Process of converting plaintext into ciphertext through certain algorithm and a key.

Decryption: Reverse process of encryption, converting ciphertext into plaintext through certain algorithm and a key.

Key: A piece of information used by an algorithm inorder to perform encryption and decryption process.

Cipher: A specific algorithm that is used for encryption and decryption.

Plaintext: The original or unencrypted message.

Ciphertext: The encrypted message obtained by performing cryptographic algorithm.

History of Cryptography.

The word “Cryptography” is derived from the Greek word *kryptos* which mean hidden. The invention of cryptography is usually stated from about 2000 B.C., while the Egyptians started using hieroglyphic writing. These were made up of complicated pictograms that only a selected group of people only know in their entirety. (Richards, Kathleen, 2023)

The first known user of modern cipher was Julius Caesar (100 B.C. to 44 B.C.). He uses it when communicating with his officers and governors because he did not his messengers. Because of this, he invented a mechanism where each character in his communications was substituted with a character three positions forward of it in the Roman alphabet.

On the other hand, cryptanalysis is the science of identifying and breaking secure communication. It involves combination of mathematical tools, finding patterns and determination. Cryptanalysis are often referred as attackers. (Stony Brook Computer Science, 2023)

The two fundamental encryption method in the filed of cryptographic systems are:

Symmetric encryption:

In symmetric encryption the message is encrypted with a single key and same key is used for decrypting the message. Symmetric is also termed as secret key encryption. Due to its simplicity, it is commonly used encryption technique but also less secure. (javatpoint, 2023)

Asymmetric encryption:

It uses two keys for encryption and based on the technique of public and private key. Public key is used to encrypt the message whereas private key is used to decrypt the message. It takes more time to encrypt than the symmetric encrypting process. (Javatpoint, 2023)

2. Playfair Cipher

Background

Sir Charles Wheatstone, a British scientist invented Playfair Cipher in 1854. It was also the first diagraph substitution cipher ever created. It gained popularity during the late 19th century Boer War, when the British Army used it to communicate by sending secret messages. (Nagaraj, 2023)

The Playfair cipher encrypts *bigrams*, which are also called *pairs of letters*. This method of encryption provides more security and is easier in implementation. In order to decrypt the ciphertext encrypted with the Playfair cipher the receiver only needs paper and pencil, making the cipher suitable for telegraphy. Due to this fact, the British used the cipher extensively during *World War I and the Second Boer War*. And During World War II, Australis also use the cipher. (Rembert, 2022).

Mechanics of Playfair Cipher

To encrypt plaintext the Playfair cipher uses a **5 * 5 table** containing a keyword. The keyword is placed first in the table starting from top left to top right, down to the second row and across the row. *In case, if the keyword contains two instances of the same letter, then the second instance is eliminated.*

The remaining alphabet letters fill out the rest of the table. **I and J** are used together to make sure that all letters are included.

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

To use the Playfair cipher while encrypting the plaintext,

one must know the following rules: (Rembert, 2022)

Rule 1. If the two letters are same, then you need to add

any filler letter such as “X”

for an instance, **HELLO** would be changed as **HE LX LO**

Rule 2. If the letters are in same row in the table, then you

need to replace the plaintext letter directly by the right-side

letters. (DF = FH).

Rule 3. If the letters are in same column in the table, then you Need to replace the plaintext letter directly by the below letters and if the letters are at the end of the column, then directly replace it by uppermost letter in the column. (OW = BO).

Rule 4. And, If the letters are not in a row or a column, then they are replaced by the plaintext letters that are in the opposite corners. (RH = UB).

Strengths and Weaknesses of Playfair Cipher

- One of its major strengths is that it is simple to use, as it just only requires a *5 * 5 key table* and few simple steps and rules to encrypt and decrypt the plaintext messages. It also generates ciphertext that is somewhat resistant to frequency analysis, a common cryptanalysis method which includes evaluating the frequency of letters of pairs of letters in the ciphertext to predict the plaintext.

- One of its major flaws is that it is vulnerable to *known-plaintext attacks*, meaning that an attacker with knowledge of some of the plaintext along with ciphertext may obtain the key table and use it to decrypt next messages.

- It's also prone to *brute-force attacks,* in which an attacker tries every potential key table until they identify the ideal one.

Although, the Playfair Cipher may not be a secure technique used in encryption, but in the world of cryptography it has been able to left a lasting impact. Cryptographers have been inspired by its innovative nature and simplicity, and its application in historical conflicts demonstrates the essential role that encryption has played in securing confidential data.

3. Modified Playfair Cipher.

The new extended *10* 9* Playfair cipher contains almost all the printable characters. Lowercase and uppercase alphabets, numbers, punctuation marks and special characters are all included in this modified cipher. The matrix is created by filling in the letters, numbers, or specific characters of the keyword, then filling in the remaining letters in alphabetical order and digits in ascending order from 0 to 9 and special characters. The Upper-case alphabets are placed at first, and then lower-case alphabets following the digits 0 to 9 in ascending order, followed by cells of the lower-case alphabet z. Unlike, Traditional Playfair cipher we have not counted **I/J** as one letter. Instead, we have placed both I and J in separate cells to reduce confusion for the user during decryption process. Since this approach allows plain text including alpha numeric values, the user can simply encrypt alpha numeric data. This algorithm can also easily and quickly encrypt plain text that includes contact numbers, house numbers, dates of birth and other numerical values. (Subhajit Bhattacharya, 2014)

Some of the major changes and rules of this modified Cipher are explained below:

- **Alphanumeric keyword:** Instance of using normal letters as a keyword, we will be using alphanumeric keyword to enhance the complexity.
  For an instance,
  Keywords = “Caesar@14”
  Unique Characters = C,a,e,s,r,@,1,4

- **Modified Matrix Construction:** If the keyword starts with vowel letter, we will be arranging the keyword from top right to down & if the keyword starts with consonant letter, we will be arranging the keyword from top right to down following with remaining characters.

- **Alphanumeric keyword sensitivity:** If the keyword letter starts with alphanumeric letter, then while constructing the matrix we will be writing keyword from reverse order from top left to top right following with remaining characters. It's like flipping the word backwards.

  For an instance,

  Keyword = 2islington$

  Unique characters in reverse order = $,n,o,t,g,n,i,l,s,2

- **Variable Block Size:** Unless like traditional Playfair cipher, we will be taking 3 as a block size to encrypt and decrypt the messages. 1st letter will be replaced by right letter, 2nd letter will be replaced by below letter, 3rd letter will be replaced by left letter. And while decryption, will be reversing this rule.

The matrix that has the secret keyword as "**Original$1"** and a certain placement sequence is given in Table 1.

Unique characters = O,r,i,g,n,a,l,$,1

As the keyword starts with vowel letter, we will be arranging the keyword from top right to down following with remaining characters.

#	>	~	0	R	H	y	o	b	O
%	?	,	2	S	I	z	p	c	r
^	:	.	3	T	J	A	q	d	i
&	{	/	4	U	K	B	s	e	g
*	}	;	5	V	L	C	t	f	n
(	-	‘	6	W	M	D	u	h	a
)	=	[	7	X	N	E	v	j	l
_	!	]	8	Y	P	F	w	k	$
+	@	<	9	Z	Q	G	x	m	1

*Table 1: Modified Playfair cipher 10 * 9 matrix.*

Lowercase and uppercase alphabets, as well as numbers and other printable characters, can be handled. Single or multiple words can be encrypted and decrypted while maintaining punctuation marks, special characters, case and tilde symbol (~) as a white space. (White space is also considered as a character in this cipher which will be removed in the process of decryption) And during encryption we use ^ as the padding character, when there are duplicate letters in a diagram and an even number of characters. During decryption process, all instances of ^ are removed, and only original plain text are left. (Sanjay Basu, 2012)

The modification of the Playfair Cipher was necessary to overcome limitations in the original version. It increased the character set by introducing lowercase letters, digits, punctuation marks, and special characters. It additionally included an alphanumeric keyword, variable block size, and a bigger matrix to improve encryption performance. These changes enhanced the cipher's versatility and compatibility for encrypting a wide range of data types.

3.1 Algorithm for Encryption.

1. START
2. Select an alphanumeric keyword.
3. Construct a 10 * 9 matrix.
4. If Keyword starts with Vowel letter go to step 4.1 else go to step 5.
   - 4.1. Arrange the keyword from top right to down following with remaining characters.
   - 4.2. Take Block size = 3
   - 4.3. 1st letter of the block size will be replaced by its right letter, 2nd letter will be replaced by below letter and 3rd letter will be replaced by its left letter of the matrix.
   - 4.4. You will get the cipher text.
5. If keyword starts with Consonant letter go to step 5.1 else go to step 6.
   - 5.1. Arrange the keyword from top left to down following with remaining characters.
   - 5.2. Take Block size = 3
   - 5.3. 1st letter of the block size will be replaced by its right letter, 2nd letter will be replaced by below letter and 3rd letter will be replaced by its left letter of the matrix.
   - 5.4. You will get the cipher text.
6. If keyword starts with Alphanumeric letter.
   - 6.1. Arrange the keyword in reverse order from top left to top right following with remaining characters.
   - 6.2. Take Block size = 3
   - 6.3. 1st letter of the block size will be replaced by its right letter, 2nd letter will be replaced by below letter and 3rd letter will be replaced by its left letter of the matrix.
   - 6.4. You will get the cipher text.
7. STOP

3.2 Flowchart for Encryption.

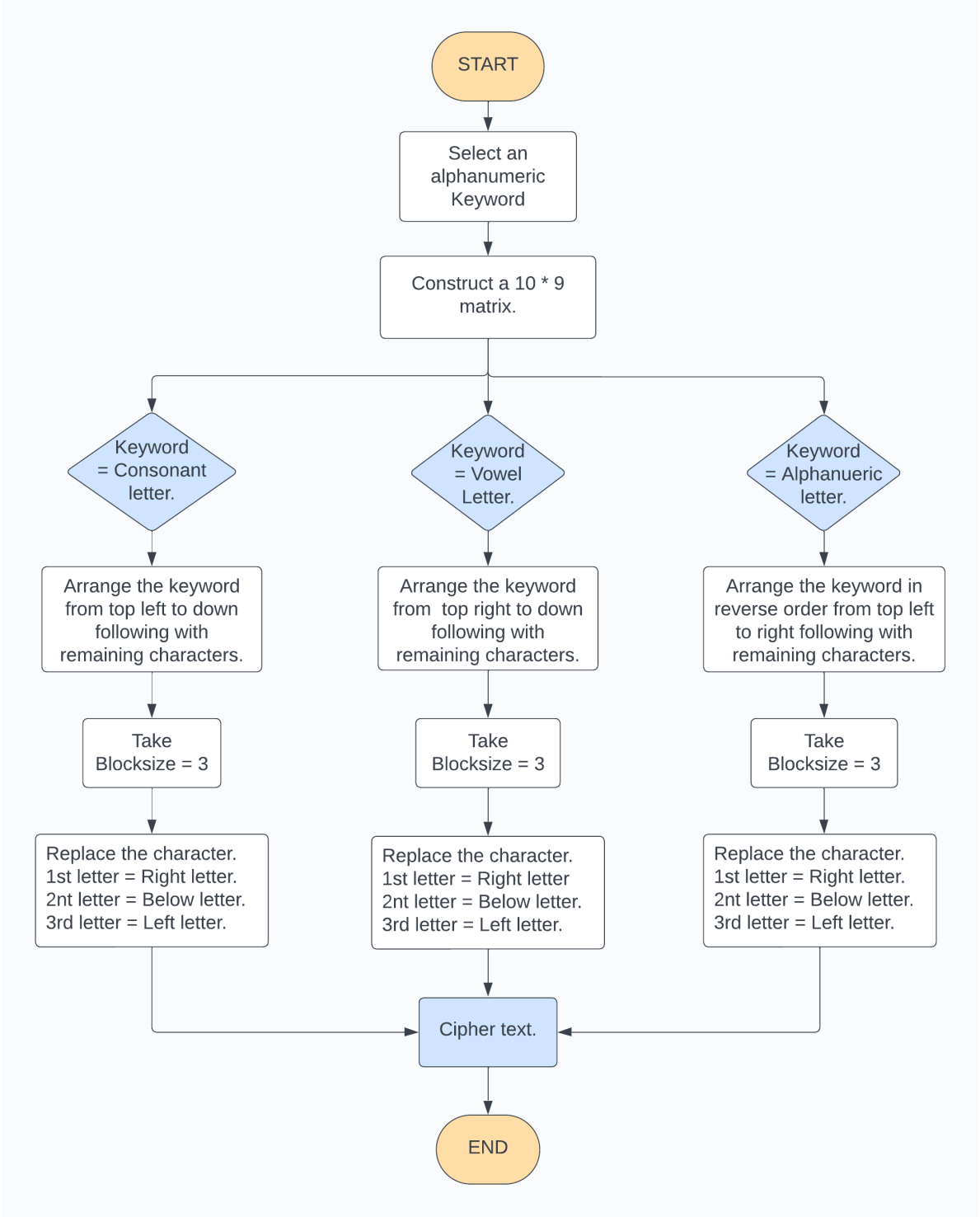


Figure 3: Flowchart for Encryption.

3.3 Algorithm for Decryption.

1. START
2. Give an alphanumeric keyword.
3. Construct a 10 * 9 matrix.
4. If Keyword starts with Vowel letter go to step 4.1 else go to step 5.
   - 4.1. Arrange the keyword from top right to down following with remaining characters.
   - 4.2. Take Block size = 3
   - 4.3. 1st letter of the block size will be replaced by its left letter, 2nd letter will be replaced by above letter and 3rd letter will be replaced by its right letter of the matrix.
   - 4.4. Remove any instance of ^ and you will get the plain text.
5. If keyword starts with Consonant letter go to step 5.1 else go to step 6.
   - 5.1. Arrange the keyword from top left to down following with remaining characters.
   - 5.2. Take Block size = 3
   - 5.3. 1st letter of the block size will be replaced by its left letter, 2nd letter will be replaced by above letter and 3rd letter will be replaced by its right letter of the matrix.
   - 5.4. Remove any instance of ^ and you will get the plain text.
6. If keyword starts with Alphanumeric letter.
   - 6.1. Arrange the keyword in reverse order from top left to top right following with remaining characters.
   - 6.2. Take Block size = 3
   - 6.3. 1st letter of the block size will be replaced by its left letter, 2nd letter will be replaced by above letter and 3rd letter will be replaced by its right letter of the matrix.
   - 6.4. Remove any instance of ^ and you will get the plain text.
7. STOP

3.4 Flowchart for Decryption.

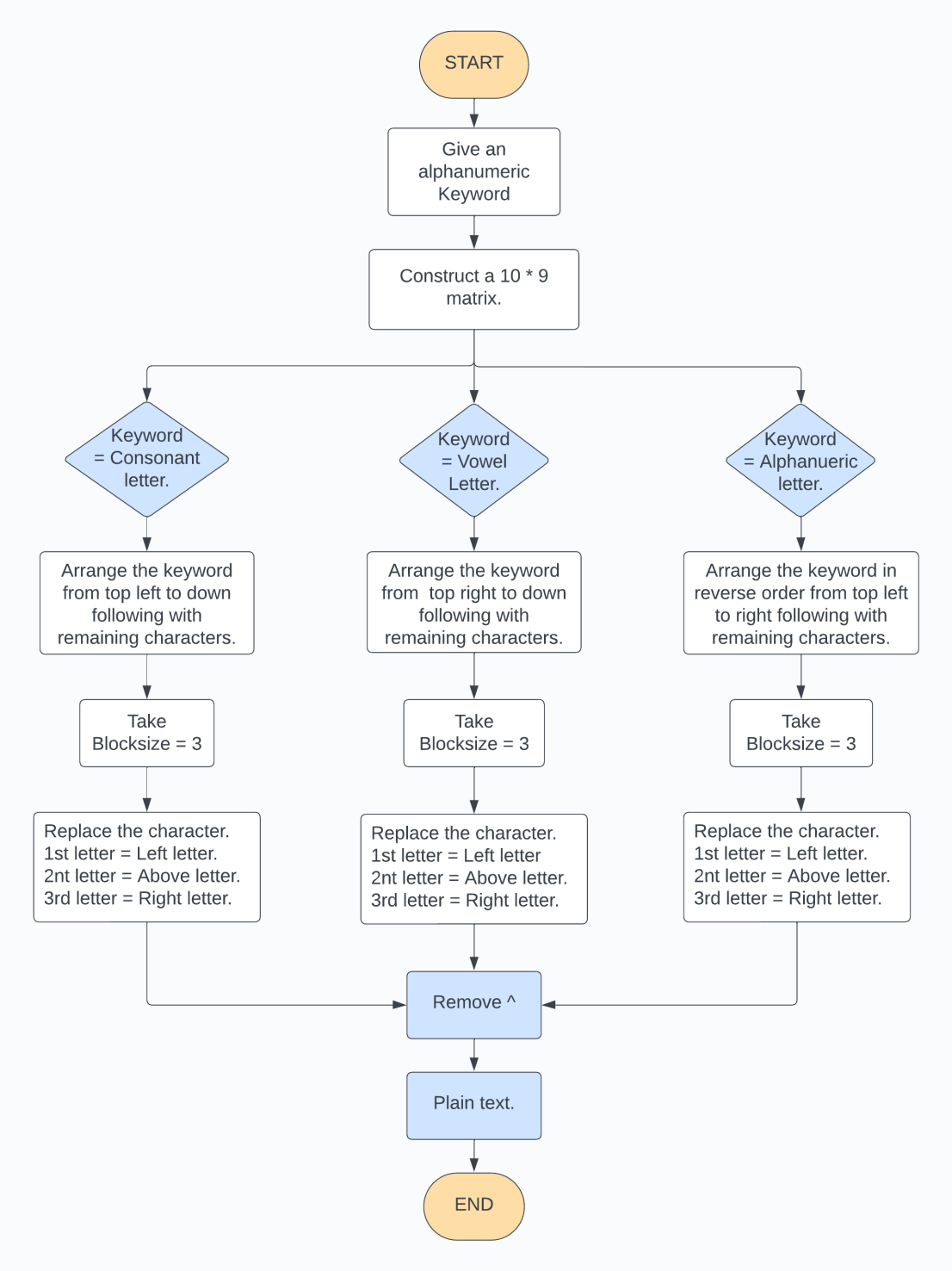


Figure 4: Flowchart for Decryption.

4. Testing

4.1. Test 1

- **Encryption**

Plaintext = **Amazing Race.**

Keyword = **#College2023**

Unique Characters = #,C,o,l,e,g,2,0,3

i. Constructing a *10 * 9* matrix.

ii. As the keyword starts with alphanumeric letter, we will be arranging the keyword in reverse order following with remaining characters.

i.e. Keyword = **3,0,2,g,e,l,o,C,#**

3	0	2	g	e	l	o	C	#	a
b	c	d	f	h	i	j	k	m	n
p	q	r	s	t	u	v	w	x	y
z	A	B	D	E	F	G	H	I	J
K	L	M	N	O	P	Q	R	S	T
U	V	W	X	Y	Z	1	4	5	6
7	8	9	~	,	.	/	;	‘	[
]	<	>	?	:	{	}	-	=	!
@	$	%	^	&	*	(	)	-	+

iii. Take Block size = 3

iv. Replace the 1st character with Right letter, 2nd character with Below letter, 3rd letter with Left letter.

Ama = Bx#

zin = Aum

g~^ = e?%

Rac = Snb

e.^ = l{%

Hence, The Cipher text is **Bx#Aume?%Snbl{%**

- **Decryption**

Cipher text = **Bx#Aume?%Snbl{%**

Keyword = **#College2023**

Unique Characters = #,C,o,l,e,g,2,0,3

i. Constructing a *10 * 9* matrix.

ii. As the keyword starts with alphanumeric letter, we will be arranging the keyword in reverse order following with remaining characters.

i.e. Keyword = **3,0,2,g,e,l,o,C,#**

3	0	2	g	e	l	o	C	#	a
b	c	d	f	h	i	j	k	m	n
p	q	r	s	t	u	v	w	x	y
z	A	B	D	E	F	G	H	I	J
K	L	M	N	O	P	Q	R	S	T
U	V	W	X	Y	Z	1	4	5	6
7	8	9	~	,	.	/	;	‘	[
]	<	>	?	:	{	}	-	=	!
@	$	%	^	&	*	(	)	_	+

iii. Take Block size = 3

iv. Replace the 1st character with Left letter, 2nd character with Above letter, 3rd letter with Right letter.

Bx# = Ama
Aum = zin
e?% = g~^
Snb = Rac
I{% = e.^

Hence, the Plain text is **Amazing Race.**

4.2. Test 2

- **Encryption**

Plain text = **This is fun.**

Keyword = **Origin@te$**

Unique Characters = O,r,i,g,n,@,t,e,$

i. Constructing a *10 * 9* matrix.
ii. As the keyword starts with vowel letter, we will be arranging the keyword from top right to down following with remaining characters.

#	<	9	0	R	H	y	m	a	O
%	>	~	1	S	I	z	o	b	r
^	?	,	2	T	J	A	p	c	i
&	:	.	3	U	K	B	q	d	g
*	{	/	4	V	L	C	s	f	n
(	}	;	5	W	M	D	u	h	@
)	-	‘	6	X	N	E	v	j	t
_	=	[	7	Y	P	F	w	k	e
+	!	]	8	Z	Q	G	x	l	$

iii. Take Block size = 3
iv. Replace the 1st character with Right letter, 2nd character with Below letter, 3rd letter with Left letter.

Thi = Jjc
s^i = f&c
s^f = f&s

un. = h@:

Hence, The Cipher text is **Jjcf&cf&sh@:**

- **Decryption**

Cipher text = **Jjcf&cf&sh@:**

Keyword = **Origin@te$**

Unique Characters = O,r,i,g,n,@,t,e,$

i. Constructing a *10 * 9* matrix.
ii. As the keyword starts with vowel letter, we will be arranging the keyword from top right to down following with remaining characters.

#	<	9	0	R	H	y	m	a	O
%	>	~	1	S	I	z	o	b	r
^	?	,	2	T	J	A	p	c	i
&	:	.	3	U	K	B	q	d	g
*	{	/	4	V	L	C	s	f	n
(	}	;	5	W	M	D	u	h	@
)	-	‘	6	X	N	E	v	j	t
_	=	[	7	Y	P	F	w	k	e
+	!	]	8	Z	Q	G	x	l	$

iii. Take Block size = 3
iv. Replace the 1st character with Left letter, 2nd character with Above letter, 3rd letter with Right letter.

Jjc = Thi
f&c = s^i

f&s = s^f

h@: = un.

Hence, The Plain text is **This is fun.**

4.3. Test 3

- **Encryption**

Plain text = **Happy New Year 2024.**

Keyword = **dec0de!**

Unique Characters = d,e,c,0,!

i. Constructing a *10 * 9* matrix.

ii. As the keyword starts with consonant letter, we will be arranging the keyword from top left to down following with remaining characters.

d	h	q	z	I	R	1	~	>	$
e	i	r	A	J	S	2	,	?	%
c	j	s	B	K	T	3	.	:	^
0	k	t	C	L	U	4	/	{	&
!	l	u	D	M	V	5	;	}	*
a	m	v	E	N	W	6	‘	-	(
b	n	w	F	O	X	7	[	=	)
f	o	x	G	P	Y	8	]	@	_
g	p	y	H	Q	Z	9	<	#	+

iii. Take Block size = 3

iv. Replace the 1st character with Right letter, 2nd character with Below letter, 3rd letter with Left letter.

Hap = Qbg
py~ = yq1
New = Wcn
~Ye = >Z%
ar~ = ms1
202 = ,!S
4.^ = //:

Hence, The Cipher text is **Qbgyq1Wcn>Z%ms1,!S//:**

- **Decryption**

Cipher text = **Qbgyq1Wcn>Z%ms1,!S//:**

Keyword = **dec0de!**

Unique Characters = d,e,c,0,!

i. Constructing a *10 * 9* matrix.
ii. As the keyword starts with consonant letter, we will be arranging the keyword from top left to down following with remaining characters.

d	h	q	z	I	R	1	~	>	$
e	i	r	A	J	S	2	,	?	%
c	j	s	B	K	T	3	.	:	^
0	k	t	C	L	U	4	/	{	&
!	l	u	D	M	V	5	;	}	*
a	m	v	E	N	W	6	‘	-	(
b	n	w	F	O	X	7	[	=	)
f	o	x	G	P	Y	8	]	@	_
g	p	y	H	Q	Z	9	<	#	+

iii. Take Block size = 3

iv. Replace the 1st character with Left letter, 2nd character with Above letter, 3rd letter with Right letter.

Qbg = Hap
yq1 = py~
Wcn = New
>Z% = ~Ye
ms1 = ar~
,!S = 202
//: = 4.^

Hence, The Plain text is **Happy New Year 2024.**

4.4. Test 4

- **Encryption**

Plaintext = **I am from Networking group (N7).**

Keyword = **@Cybersecur!ty**

Unique Characters = @,C,y,b,e,r,s,c,u,!,t

i. Constructing a *10 * 9* matrix.

ii. As the keyword starts with alphanumeric letter, we will be arranging the keyword in reverse order following with remaining characters.

i.e. Keyword = **t,!,u,c,s,r,e,b,y,C,@**

t	!	u	c	s	r	e	b	y	C
@	a	d	f	g	h	i	j	k	l
m	n	o	p	q	v	w	x	z	A
B	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	~	,	.	/	;	‘
[	]	<	>	?	:	{	}	-	=
#	$	%	^	&	*	(	)	_	+

iii. Take Block size = 3

iv. Replace the 1st character with Right letter, 2nd character with Below letter, 3rd letter with Left letter.

I~a = J?@
m~f = n?d
rom = eEA
~Ne = ,Xr
two = !In
rki = ezh
ng~ = oq9
gro = hhn
up~ = cF9
(N7 =)X6
).^ = _{%

Hence, The Cipher text is **J?@n?deEA,Xr!Inezhoq9hhncF9)X6_{%**

- **Decryption**

Cipher text = **J?@n?deEA,Xr!Inezhoq9hhncF9)X6_{%**

Keyword = **@Cybersecur!ty**

Unique Characters = @,C,y,b,e,r,s,c,u,!,t

i. Constructing a *10 * 9* matrix.
ii. As the keyword starts with alphanumeric letter, we will be arranging the keyword in reverse order following with remaining characters.

i.e. Keyword = **t,!,u,c,s,r,e,b,y,C,@**

t	!	u	c	s	r	e	b	y	C
@	a	d	f	g	h	i	j	k	l
m	n	o	p	q	v	w	x	z	A
B	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	~	,	.	/	;	‘
[	]	<	>	?	:	{	}	-	=
#	$	%	^	&	*	(	)	_	+

iii. Take Block size = 3

iv. Replace the 1st character with Left letter, 2nd character with Above letter, 3rd letter with Right letter.

J?@ = l~a
n?d = m~f
eEA = rom
,Xr = ~Ne
!In = two
Ezh = rki
oq9 = ng~
hhn = gro
cF9 = up~
)X6 = (N7
_{% =).^

Hence, The Plain text is **I am from Networking group (N7).**

4.5. Test 5

- **Encryption**

Plaintext = **This is the final test 5.**

Keyword = **AllGooD100%**

Unique Characters = A,l,G,o,D,1,0,%

i. Constructing a *10 * 9* matrix.

ii. As the keyword starts with vowel letter, we will be arranging the keyword from top right to down following with remaining characters.

#	>	~	Z	Q	H	v	k	b	A
$	?	,	2	R	I	w	m	c	l
^	:	.	3	S	J	x	n	d	G
&	{	/	4	T	K	y	p	e	o
*	}	;	5	U	L	z	q	f	D
(	-	‘	6	V	M	B	r	g	1
)	=	[	7	W	N	C	s	h	0
_	!	]	8	X	O	E	t	i	%
+	@	<	9	Y	P	F	u	j	a

iii. Take Block size = 3

iv. Replace the 1st character with Right letter, 2nd character with Below letter, 3rd letter with Left letter.

Thi = Kit

s~i = h,t

s~t = h,E

he~ = 0f>

fin = DjX

al~ = +G>

tes = ifC

t~5 = i,;

.^^ = 3&G

Hence, The Cipher text is **Kith,th,E0f>DjX+G>ifCi,;3&G**

- **Decryption**

Cipher text = **Kith,th,E0f>DjX+G>ifCi,;3&G**

Keyword = **AllGooD100%**

Unique Characters = A,l,G,o,D,1,0,%

i. Constructing a *10 * 9* matrix.
ii. As the keyword starts with vowel letter, we will be arranging the keyword from top right to down following with remaining characters.

#	>	~	Z	Q	H	v	k	b	A
$	?	,	2	R	I	w	m	c	l
^	:	.	3	S	J	x	n	d	G
&	{	/	4	T	K	y	p	e	o
*	}	;	5	U	L	z	q	f	D
(	-	‘	6	V	M	B	r	g	1
)	=	[	7	W	N	C	s	h	0
_	!	]	8	X	O	E	t	i	%
+	@	<	9	Y	P	F	u	j	a

iii. Take Block size = 3

iv. Replace the 1st character with Left letter, 2nd character with Above letter, 3rd letter with Right letter.

Kit = Thi
h,t = s~i
h,E = s~t
0f> = he~
DjX = fin
+G> = al~
ifC = tes
i,; = t~5
3&G = .^^

Hence, The Plain text is **This is the final test 5.**

5. Evaluation.

5.1. Strengths of Modified Playfair Cipher.

- **Enhanced Complexity by using Alphanumeric Keywords:**
  The use of an alphanumeric keyword increases the complexity of the cipher which makes it more resistant to traditional cryptographic attacks.

- **Variable block size:**
  Instead of using 2 block-size like the traditional Playfair cipher, this modified Playfair cipher uses block size 3. It provides flexibility in encrypting and decrypting along with adding an extra layer of complexity to the algorithm.

- **Matrix Construction Variability:**
  The method for constructing the matrix is based on the keyword whether it starts with vowel letter, consonant letter or alphanumeric letter. It adds variability to the algorithm adding a unique aspect the encryption process.

- **Resistance to known-plaintext attacks:**
  Known-plaintext attacks means attacker having access to both the plaintext and the ciphertext. The larger character set and customizable arrangement of the modifier Playfair cipher makes it more resistant to such attacks because as the relation between the plaintext and its corresponding ciphertext is more complex and less predictable.

- **Handling Alphanumeric Values:**
  The modified Playfair cipher allows encryption of alphanumeric data which includes data of births, contact numbers, address etc. This versatility increases the range of data that can be encrypted securely.

5.2. Weaknesses of Modified Playfair cipher.

- **Complexity in implementation:**
  The modified Playfair cipher introduces additional complexities while constructing the matrix, handling alphanumeric keywords and managing the padding character. This makes the implementation of modified cipher more challenging and prone to vulnerabilities as well as implementation errors.

- **Key distribution and management:**
  Same as any symmetric encryption algorithm, the modified Playfair cipher requires a secure mechanism for key distribution and management. If the key management process is compromised it can impact overall security.

- **Lack of forward secrecy:**
  The modified cipher does not provide forward secrecy which means if the encryption key is compromised, all past and future encrypted messages can be decrypted.

- **Padding Character Usage:**
  The use of ^ as padding character to handle duplicate letters might introduces potential confusion during the decryption process. If the padding character is not properly managed, it may also result mislead information or data loss.

- **Lack of modern security features:**
  The modified Playfair cipher does not incorporate modern security features such as including authenticated encryption, ensuring confidentiality and integrity, perfect forward secrecy or support for key exchange protocols which are crucial for maintain secure communication over time.

5.3. Application area where Modified Playfair Cipher can be implemented.

- **IOT Security:**
  The Modified Playfair Cipher can be used to secure communication within Internet of Things (IOT) devices, preventing sensitive information from unauthorized access as it can handle wide range of characters which also include alphanumeric data.

- **Digital Transactions:**
  Modified Playfair Cipher can also be used in digital transactions due to it's ability to handle special characters and provide complexity with alphanumeric keywords as it can safeguard sensitive data during online transactions.

- **Database Security:**
  As Playfair Cipher can encrypt the alphanumeric data, it is suitable for securing the databases which contains the mixed types of information such as contact details, address, passwords, personal information etc.

- **Military and Government Communications:**
  It can be used in military and government communications to protect the sensitive data from disruption and unauthorized access.

- **Educational Purposes:**
  It can be used as educational tool for teaching students about enhanced cryptographic techniques. It gives practical example of how encryption algorithms can be implemented in different case scenarios.

6. Conclusion.

In conclusion, the report dives thoroughly into cryptographic systems, focusing particularly on the Playfair Cipher and its improved version. It starts off with an introduction to cryptography, which explores its history back to ancient times and emphasizes its critical role in protecting sensitive information. The Playfair Cipher, believed to come from Sir Charles Wheatstone, is extensively studied, with a focus on its mechanics, strengths, and drawbacks.

The improved Playfair Cipher takes centre stage, including an expanded 10x9 matrix that can handle a wide range of characters, including alphanumeric values. The algorithm's novel characteristics, such as the usage of an alphanumeric keyword, variable block size, and matrix construction diversity, help to increase complexity and resistance to known-plaintext attacks.

The test cases in the report demonstrate the modified Playfair Cipher's functionality, including encryption and decryption operation. While the cipher has advantages in terms of complexity and variety, users and implementers must be aware of the potential problems.

In the ever-changing cryptography world, the modified Playfair Cipher demonstrates the ongoing pursuit of creative solutions. While not without flaws, the cipher reveals significant perspectives on the difficult balance of complexity and practicality. As cryptographic approaches improve, learning from previous methods help to enhance secure communication practices.

7. References

Brooks, D. J., 2010. What is security: Definition through knowledge categorization. *Security Journal,* 3(23), pp. 1-15.

Cameroan Hashemi-Pour, W. C., 2023. *CIA triad (confidentiality, integrity and availability).* [Online]
Available at: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA
[Accessed 11 January 2024].

javatpoint, 2023. *Difference between Symmetric encryption and Asymmetric encryption.* [Online]
Available at: https://www.javatpoint.com/symmetric-encryption-vs-asymmetric-encryption
[Accessed 11 January 2024].

Javatpoint, 2023. *Difference between Symmetric encryption and Asymmetric encryption.* [Online]
Available at: https://www.javatpoint.com/symmetric-encryption-vs-asymmetric-encryption
[Accessed 26 Ocotber 2023].

Jussi Nikander, O. M. M. L., 2020. *The Confidentiality, Integrity, Availability (CIA) triad..* [Online]
Available at: https://www.researchgate.net/figure/The-Confidentiality-Integrity-Availability-CIA-triad_fig1_346192126
[Accessed 11 Janury 2024].

Nagaraj, K., 2023. *Exploring the Playfair Cipher: An Old but Effective Encryption Technique.* [Online]
Available at: https://cyberw1ng.medium.com/exploring-the-playfair-cipher-an-old-but-effective-encryption-technique-eadb9696c384
[Accessed 10 December 2023].

Rembert, L., 2022. *Playfair Cipher.* [Online] Available at: https://privacycanada.net/playfair-cipher/ [Accessed 10 September 2023].

Richards, Kathleen, 2023. *Cryptography.* [Online] Available at: https://www.techtarget.com/searchsecurity/definition/cryptography [Accessed 25 October 2023].

Sanjay Basu, U. K. R., 2012. Modified Playfair Cipher using Rectangular Matrix. *International Journal of Computer Applications (0975 – 8887),* 46(9), pp. 20-30.

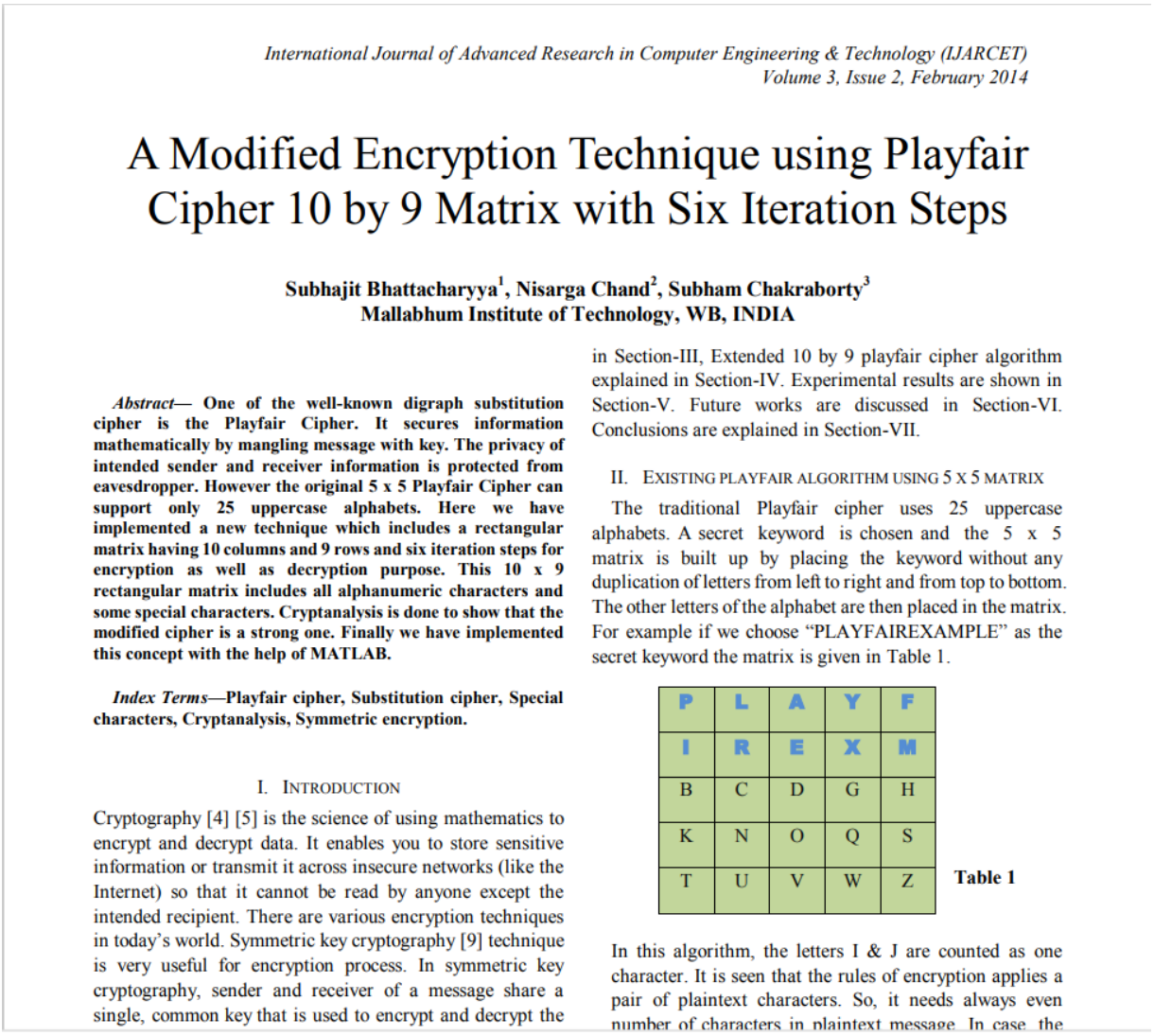
Shashank, 2023. *What is Cryptography? – An Introduction to Cryptographic Algorithms.* [Online]
Available at: https://www.edureka.co/blog/what-is-cryptography/#:~:text=Symmetric%20key%20encryption-,Symmetric%20Key%20Cryptography,the%20Data%20Encryption%20Standard%20(DES)
[Accessed 11 January 2024].

Stony Brook Computer Science, 2023. *An Introduction to Cryptography.* [Online] Available at: https://www.cs.stonybrook.edu/sites/default/files/PGP70IntroToCrypto.pdf [Accessed 25 Ocotber 2023].

Subhajit Bhattacharya, N. C. S. C., 2014. A Modified Encryption Technique using Playfair Cipher 10 by 9 Matrix with Six Iteration Steps. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),* 3(2), pp. 307-312.

8. Appendices.

- **Research Paper 1.**



International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 3, Issue 2, February 2014

A Modified Encryption Technique using Playfair Cipher 10 by 9 Matrix with Six Iteration Steps

Subhajit Bhattacharyya[1], Nisarga Chand[2], Subham Chakraborty[3]
Mallabhum Institute of Technology, WB, INDIA

***Abstract*— One of the well-known digraph substitution cipher is the Playfair Cipher. It secures information mathematically by mangling message with key. The privacy of intended sender and receiver information is protected from eavesdropper. However the original 5 x 5 Playfair Cipher can support only 25 uppercase alphabets. Here we have implemented a new technique which includes a rectangular matrix having 10 columns and 9 rows and six iteration steps for encryption as well as decryption purpose. This 10 x 9 rectangular matrix includes all alphanumeric characters and some special characters. Cryptanalysis is done to show that the modified cipher is a strong one. Finally we have implemented this concept with the help of MATLAB.**

***Index Terms*—Playfair cipher, Substitution cipher, Special characters, Cryptanalysis, Symmetric encryption.**

I. INTRODUCTION

Cryptography [4] [5] is the science of using mathematics to encrypt and decrypt data. It enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. There are various encryption techniques in today's world. Symmetric key cryptography [9] technique is very useful for encryption process. In symmetric key cryptography, sender and receiver of a message share a single, common key that is used to encrypt and decrypt the in Section-III, Extended 10 by 9 playfair cipher algorithm explained in Section-IV. Experimental results are shown in Section-V. Future works are discussed in Section-VI. Conclusions are explained in Section-VII.

II. EXISTING PLAYFAIR ALGORITHM USING 5 X 5 MATRIX

The traditional Playfair cipher uses 25 uppercase alphabets. A secret keyword is chosen and the 5 x 5 matrix is built up by placing the keyword without any duplication of letters from left to right and from top to bottom. The other letters of the alphabet are then placed in the matrix. For example if we choose "PLAYFAIREXAMPLE" as the secret keyword the matrix is given in Table 1.

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

Table 1

In this algorithm, the letters I & J are counted as one character. It is seen that the rules of encryption applies a pair of plaintext characters. So, it needs always even number of characters in plaintext message. In case the

Figure 5: Research Paper 1. (Subhajit Bhattacharya, 2014)

is very useful for encryption process. In symmetric key cryptography, sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. Symmetric key cryptography is also called the private key cryptography. Playfair cipher [3] is one of the popular symmetric encryption methods.

The first recorded description of the Playfair cipher [8] was in a document signed by Wheatstone on 26 March 1854. However Lord Playfair promoted the use of this cipher and hence it is called Playfair Cipher. It was used by the British in the Second Boer War and in World War I. It was also used by the Australians and Germans during World War II. Playfair is reasonably easy to use and was used to handle important but non-critical secrets. By the time the enemy cryptanalysts could break the message, the information would be useless to them. Between February 1941 and September 1945 the Government of New Zealand used it for communication between New Zealand, the Chatham Islands and the Pacific Islands.

The organization of the paper can be summarized as: The existing playfair algorithm using 5 x 5 matrix explained in Section-II. Limitations of existing playfair cipher discussed

In this algorithm, the letters I & J are counted as one character. It is seen that the rules of encryption applies a pair of plaintext characters. So, it needs always even number of characters in plaintext message. In case, the message counts odd number of characters a spare letter X is added at the end of the plaintext message. Further repeating plaintext letters in the same pair are separated with a filler letter, such as X, so that the words COMMUNICATE would be treated as CO MX MU NI CA TE.

Rules:

a. Plain text letters that fall in the same row of the matrix are replaced by the letter to the right, with the first element of the row circularly following the last. For example RE is encrypted as EX.

b. Plain text letters that fall in the same column are replaced by the letter beneath, with the top element of the row circularly following in the last. For example, RC is encrypted as CN.

c. Otherwise, each plaintext letter is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, OH becomes SD, and FD becomes AH.

307

ISSN: 2278 – 1323

Figure 5: Research Paper 1. (Subhajit Bhattacharya, 2014)

International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 3, Issue 2, February 2014

III. LIMITATIONS OF EXISTING PLAYFAIR CIPHER

The main drawback of the traditional Playfair cipher is that the plain text can consist of 25 uppercase letters only. One letter has to be omitted and cannot be reconstructed after decryption. Also lowercase letters, white space, numbers and other printable characters cannot be handled by the traditional cipher. This means that complete sentences cannot be handled by this cipher. Space between two words in the plaintext is not considered as one character. A spare letter X is added when the plaintext word consists of odd number of character. In the decryption process this X is ignored. X is a valid character and creates confusion because it could be a part of plaintext, so we cannot simply remove X in decryption process.

X is used a filler letter while repeating letter falls in the same pair are separated.

In a mono alphabetic cipher the attacker has to search in 26 letters only. Playfair cipher being a polyalphabetic cipher the attacker has to search in 26 x 26 = 676 diagrams. Although the frequency analysis is much more difficult than in mono alphabetic cipher still using modern computational techniques the attacker can decipher the cipher text.

To overcome the drawbacks we implement a modified cipher which uses a 10 x 9 matrix which will contain almost all the printable characters.

Keyword: Monarchy

M	**o**	**n**	**a**	**r**	**c**	**h**	**y**	b	d
e	f	g	i	j	k	l	m	p	q
s	t	u	v	w	x	z	A	B	C
D	E	F	G	H	I	J	K	L	N
O	P	Q	R	S	T	U	V	W	X
Y	Z	0	1	2	3	4	5	6	7
8	9	~	,	.	/	;	“	\	|
<	>	?	:	{	}	-	=	!	@
#	$	%	^	&	*	(	)	_	+

Fig 1

Keyword: Duplicate29

D	**u**	**p**	**l**	**i**	**c**	**a**	**t**	**e**	**2**
9	b	d	f	g	h	j	k	m	n
o	q	r	s	v	w	x	y	z	A
B	C	E	F	G	H	I	J	K	L
M	N	O	P	Q	R	S	T	U	V
W	X	Y	Z	0	1	3	4	5	6
7	8	~	,	.	/	;	“	\	|
<	>	?	:	{	}	-	=	!	@
#	$	%	^	&	*	(	)	_	+

Fig 2

Figure 6: Research Paper 1. (Subhajit Bhattacharya, 2014)

IV. EXTENDED 10 X 9 PLAYFAIR CIPHER ALGORITHM

This extended play fair algorithm is based on the use of a 10 by 9 matrix of letters constructed using a keyword. The 10 x 9 matrix contains almost all the printable characters. This includes lowercase and uppercase alphabets, punctuation marks, numbers and special characters. The matrix is constructed by filling in the letters, numbers or special characters of the keyword from left to right and from top to bottom, and the filling in the remainder of the matrix with the remaining letters in alphabetic order and digits in ascending order form 0 to 9 and special characters .The upper case alphabets are placed first then the lower case alphabets following the digits 0 to 9 can be placed next cells of the lower case alphabet z in an ascending order. And finally the special characters which are arranged in an order which is shown in Table1-6.In this we have not counted I/J as one letter instead we are placing both I and J in two different cells in order to avoid the ambiguity to the user at the time of decipherment. This algorithm can allow the plain text containing of alpha numeric values; hence the user can easily encrypt alpha numeric values efficiently. The plain text containing contact numbers, date of birth, house numbers and other numerical values can be easily and efficiently encrypted using this algorithm.

A. Assumption

Here we have used six reserved keywords: Monarchy, Duplicate29, Nisarga1987, Subho27, Eagle*& and Shiva@#. Then we construct six 10 by 9 matrices with the help of these six keywords. The six 10 by 9 matrices are shown in figure 1-6.

Keyword: Nisarga1987

N	**i**	**s**	**a**	**r**	**g**	**1**	**9**	**8**	**7**
b	c	d	e	f	h	j	k	l	m
n	o	p	q	t	u	v	w	x	y
z	A	B	C	D	E	F	G	H	I
J	K	L	M	O	P	Q	R	S	T
U	V	W	X	Y	Z	0	2	3	4
5	6	~	,	.	/	;	“	\	|
<	>	?	:	{	}	-	=	!	@
#	$	%	^	&	*	(	)	_	+

Fig 3

Keyword: Subho27

S	**u**	**b**	**h**	**o**	**2**	**7**	a	c	d
e	f	g	i	j	k	l	m	n	p
q	r	s	t	v	w	x	y	z	A
B	C	D	E	F	G	H	I	J	K
L	M	N	O	P	Q	R	T	U	V
W	X	Y	Z	0	1	3	4	5	6
8	9	~	,	.	/	;	“	\	|
<	>	?	:	{	}	-	=	!	@
#	$	%	^	&	*	(	)	_	+

Fig 4

ISSN: 2278 – 1323

Figure 7: Research Paper 1. (Subhajit Bhattacharya, 2014)

International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 3, Issue 2, February 2014

Keyword: Eagle*&

E	**a**	**g**	**l**	**e**	*	**&**	b	c	d
f	h	i	j	k	m	n	o	p	q
r	s	t	u	v	w	x	y	z	A
B	C	D	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	~	,	.	/	;	“
\	|	<	>	?	:	{	}	-	=
!	@	#	$	%	^	(	)	_	+

Fig 5

Keyword: Shiva@#

S	**h**	**i**	**v**	**a**	**@**	#	b	c	d
e	f	g	j	k	l	m	n	o	p
q	r	s	t	u	w	x	y	z	A
B	C	D	E	F	G	H	I	J	K
L	M	N	O	P	Q	R	T	U	V
W	X	Y	Z	0	1	2	3	4	5
6	7	8	9	~	,	.	/	;	“
\	|	<	>	?	:	{	}	-	=
!	$	%	^	&	*	(	)	_	+

Fig 6

occurs same row or same column and any one of the character occurs at the first column(for same row character) or at the first row(for same column character) then in the encrypted message they becomes last column character(for same row character) or last row character(for same column character).

- From the last stage of the decrypted message we get a message which is same as diagraph message.
- This message devoid of space but may include several capital “X”. Some of which may be unnecessary because they are inserted between two same occurrence character or may be inserted at the end of the message to make the message alphabet count even. Some of which may be with the original message. So we have to take only the necessary capital “X” and to discard the unnecessary capital ”X”.
- To make the above condition happen we scan the last decrypted message from left to right. If any capital “X” occurs we check the right most and left most character of this “X” if this two character found same we discard the corresponding “X”. If “X” occurs at the last of the string we also have to discard this “X” to recover the original message. For any other condition we have to include the “X” with the original message.
- After removing the unnecessary capital “X” we get our original message.

Figure 8: Research Paper 1. (Subhajit Bhattacharya, 2014)

B. Algorithm

- First we take input message which is user defined.
- If any space or punctuations occurs, then it should be automatically removed from the input message.
- After that we check any double occurrence, and then add "X" automatically in between these two characters.
- After removing the unwanted space we get a modified message that is called the digraph message.
- Next we encrypt this digraph message with the Keyword "Monarchy".
- After that corresponding five iteration steps introduced with five different keywords: "Duplicate29", "Nisarga1987", "Subho27", "Eagle*&" and "Shiva@#".
- During encryption process if any two character occurs same row or same column and any one of the character occurs at the last column(for same row character) or at the last row(for same column character) then in the encrypted message they becomes first column character(for same row character) or first row character(for same column character).
- Next we decrypt the last encrypted message with keyword "Shiva@#" and repeat the same decryption process five times with five different keywords: "Eagle*&", "Subho27", "Nisarga1987", "Duplicate29" and "Monarchy".
- During decryption process if any two character occurs

C. Cryptanalysis

The various types of cryptanalytic attacks are as follows.

1. Brute force attack
2. Cipher text only attack
3. Chosen plaintext/cipher text attack

1. Brute force attack

The size of the key domain is 90! (Factorial 90). Thus brute force attack will be very difficult for the modified Playfair cipher.

2. Cipher text only attack

The frequencies of digrams are preserved in the cipher text (to some extent). The cryptanalyst can launch a cipher-text only attack. However the number of digrams to be searched would be 90 x 90 = 8100.

3. Chosen plaintext/cipher text attack

Obtaining the key is relatively straightforward if both plaintext and cipher text are known.

V. EXPERIMENTAL RESULTS

In this thesis for implementation of techniques MATLAB 7.0.2 version is used. MATLAB® is a high-performance language for technical computing.

In our experiment we have used six different keywords and with the help of this six keywords we have encrypt and decrypt the text messages successfully.

Here we include two figures. The original text message with its encrypted six versions is shown clearly in the figure 7

ISSN: 2278 – 1323

Figure 6: Research Paper 1. (Subhajit Bhattacharya, 2014)

- **Research Paper 2.**

International Journal of Computer Applications (0975 – 8887)
Volume 46– No.9, May 2012

Modified Playfair Cipher using Rectangular Matrix

Sanjay Basu
Department of Information Technology
Jadavpur University
Kolkata, India

Utpal Kumar Ray
Department of Information Technology
Jadavpur University
Kolkata, India

ABSTRACT
One of the well known polyalphabetic ciphers is the Playfair cipher. In this cipher digrams or groups of 2 letters in the plain text is converted to cipher text digrams during encryption using a key. Similarly during decryption cipher text digrams are converted to plain text digrams using the same key. However the original 5 x 5 Playfair cipher can support only 25 uppercase alphabets. To overcome this drawback we propose a rectangular matrix having 10 columns and 9 rows which can support almost all the printable characters including white space. This paper analyses the original Playfair cipher, the different variations that have been proposed and the modified Playfair cipher that we propose. Cryptanalysis is done to show that the proposed cipher is a strong one.

Keywords
Playfair cipher, Polyalphabetic cipher, Special symbols, cryptanalysis, rectangular matrix

1. INTRODUCTION

When information is transmitted from the sender to the receiver care should be taken so that the information is not accessible to a third party. One of the ways to protect information is the method of encryption – decryption whereby the sender encrypts the message with a secret key which is

Table I: Traditional Playfair 5 x 5 matrix

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

The message is then broken up with digrams or groups of 2 letters. In case of duplication of letters in a digram one of the letters is used as padding and is placed between the letters. In case of odd number of characters the same padding is applied at the end. The substitution happens depending on the following three rules.

1. In case letters of a digram are in the same row the letters to the right of each letter are taken. Wrapping happens in case one of the letters is at the last column.

Figure 7: Research Paper 2. (Sanjay Basu, 2012)

receiver care should be taken so that the information is not accessible to a third party. One of the ways to protect information is the method of encryption – decryption whereby the sender encrypts the message with a secret key which is known only to the receiver. Once the receiver gets the message the message is decrypted using the same secret key. This type of encryption is known as symmetric encryption. Playfair cipher [1] is one of the well known symmetric encryption methods.

The first recorded description of the Playfair cipher [2] was in a document signed by Wheatstone on 26 March 1854. However Lord Playfair promoted the use of this cipher and hence it is called Playfair Cipher. It was used by the British in the Second Boer War and in World War I. It was also used by the Australians and Germans during World War II. Playfair is reasonably easy to use and was used to handle important but non-critical secrets. By the time the enemy cryptanalysts could break the message, the information would be useless to them. Between February 1941 and September 1945 the Government of New Zealand used it for communication between New Zealand, the Chatham Islands and the Pacific Islands.

2. EXISTING PLAYFAIR CIPHER

The traditional Playfair cipher [3] [4] uses 25 uppercase alphabets with I=J or Q omitted. A secret keyword is chosen and the 5 x 5 matrix is built up by placing the keyword without any duplication of letters from left to right and from top to bottom. The other letters of the alphabet are then placed in the matrix. For example if we choose **DUPLICATE** as the secret keyword the matrix is given in Table I.

1. In case letters of a digram are in the same row the letters to the right of each letter are taken. Wrapping happens in case one of the letters is at the last column.

2. In case of letters in the same column the letters to the bottom of each letter are taken. Again wrapping happens in case any letter is in the last row.

3. In case the letters are neither in the same row or column a rectangle is made with the letters and the letters at the opposite corners are taken.

In case of decryption the opposite is done with the cipher text and we get back the plain text.

If we take balloon as the plaintext and duplicate as the secret keyword the ciphertext can be derived as follows. First the plaintext is converted to uppercase and then broken up into digrams using X as the padding character. The digrams will be BA LX LO ON. For the first digram B and A are in the same row. Using rule 1 we get CT. Next we take LX – they are neither in the same row or column. Hence using rule 3 we get PY. The next digram is LO which as before are neither in the same row or column. Hence using rule 3 we get UR. The last digram is ON which are in the same row and so we get QO. Thus the cipher text is CTPYURQO.

3. VARIATIONS OF PLAYFAIR CIPHER

n the variation proposed by Ravindra Babu K, S. Uday Kumar, A. Vinay Babu, I.V.N.S Aditya , P. Komuraiah [5] the 5 x 5 matrix has been replaced by 6 x 6 matrix. In this system all the uppercase alphabets as well as numbers can be

28

Figure 8: Research Paper 2. (Sanjay Basu, 2012)

International Journal of Computer Applications (0975 – 8887)
Volume 46– No.9, May 2012

handled. However lowercase letters, white space and other printable characters cannot be handled.

In the variation proposed by Shiv Shakti Srivastava, Nitin Gupta [6] the 5 x 5 matrix has been replaced by 8 x 8 matrix. After converting plain text to cipher text using the 8 x 8 matrix, the characters are converted to the corresponding ASCII values in decimal and then to corresponding binary values of 7 bits. Linear Feedback Shift Register is then applied to get the final cipher text.

In the variation proposed by Gaurav Agrawal, Saurabh Singh, Manu Agarwal [7] the frequency of each alphabet in the text to be encrypted is calculated. The 2 letters with the least frequency are combined instead of combining I and J. The 5 x 5 matrix is formed by inserting the keyword without duplication of letters, the combined letters and lastly the other letters.

In the variation proposed by Packirisamy Murali and Gandhidoss Senthilkumar [8] random numbers are mapped to secret key of Playfair cipher method and corresponding numbers will be transmitted to the recipient instead of alphabetical letter. This method rapidly increases security of the transmission over an unsecured channel.

In the variation proposed by Harinandan Tunga, Soumen Mukherjee [9] multiple array of structure has been used to store the information about the spaces and the other to store the information about whether an 'X' has appeared in the alphabet matrix. Secondly the key table has been extended from 5 X 5 matrix to 16 X 16 matrix form. Finally, the 16 X 16 algorithm has been modified so that it can incorporate shifting of rows and columns of the 16 X 16 matrix to ensure that the encrypted text contains any ASCII ranging between 0 – 255.

In the variation proposed by V. Umakanta Sastry, N. Ravi Shankar, and S. Durga Bhavani [10] it is assumed that the characters of the plain text belong to the set of ASCII characters denoted by the codes 0 to 127. A substitution table is constructed in an appropriate manner and the rules 1 to 3 are modified suitably for encryption and decryption. Further

marks, numbers and special characters. The order of placement of different groups of characters can also be done so that the matrix formed by using the same secret keyword depends on the order of placement. This means that the ciphertext will also depend on the order of placement of different groups of characters. The matrix with the secret keyword as **Duplicate** and a particular placement order is given in Table II.

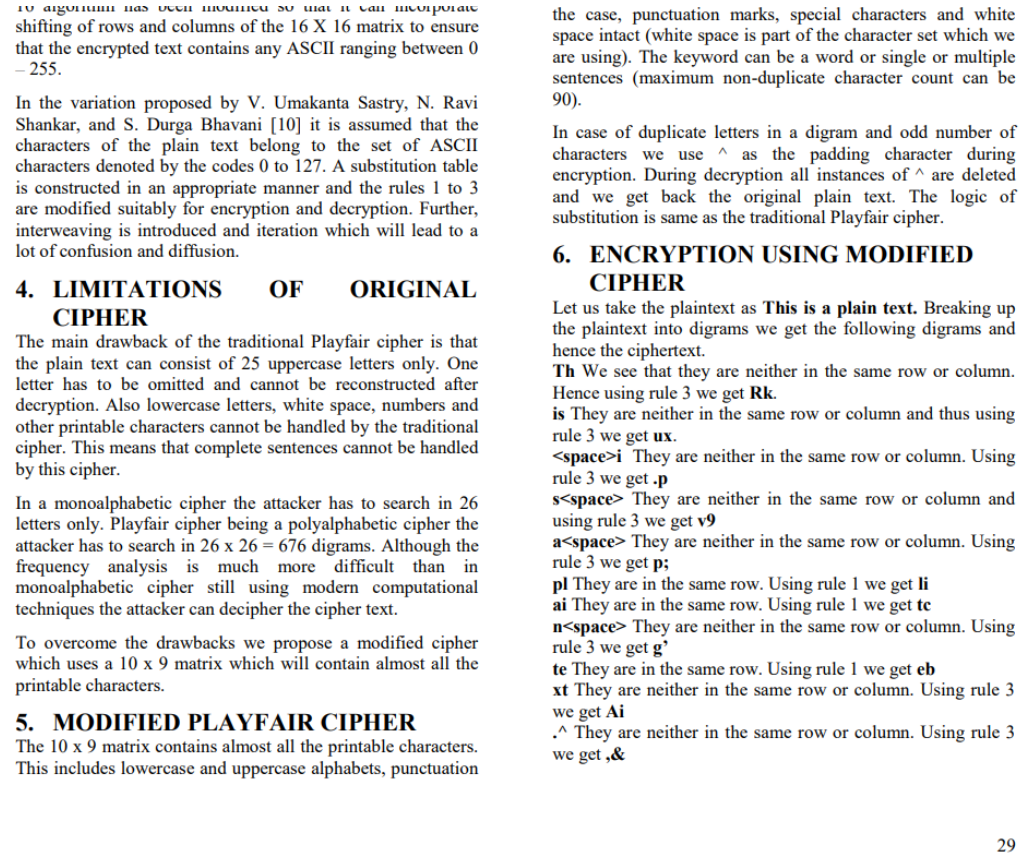
Table II: Modified Playfair 10 x 9 matrix

D	u	p	l	i	c	a	t	e	b
d	f	g	h	j	k	m	n	o	q
r	s	v	w	x	y	z	A	B	C
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		,	.	/	;	'	[	]
<	>	?	:	{	}	-	=	!	@
#	$	%	^	&	*	(	)	_	+

Lowercase as well as uppercase alphabets along with numbers and other printable characters can be handled. Single or multiple sentences can be encrypted and decrypted keeping the case, punctuation marks, special characters and white space intact (white space is part of the character set which we are using). The keyword can be a word or single or multiple sentences (maximum non-duplicate character count can be 90).

In case of duplicate letters in a digram and odd number of characters we use ^ as the padding character during encryption. During decryption all instances of ^ are deleted and we get back the original plain text. The logic of

Figure 9: Research Paper 2. (Sanjay Basu, 2012)



10 algorithm has been modified so that it can incorporate shifting of rows and columns of the 16 X 16 matrix to ensure that the encrypted text contains any ASCII ranging between 0 – 255.

In the variation proposed by V. Umakanta Sastry, N. Ravi Shankar, and S. Durga Bhavani [10] it is assumed that the characters of the plain text belong to the set of ASCII characters denoted by the codes 0 to 127. A substitution table is constructed in an appropriate manner and the rules 1 to 3 are modified suitably for encryption and decryption. Further, interweaving is introduced and iteration which will lead to a lot of confusion and diffusion.

4. LIMITATIONS OF ORIGINAL CIPHER

The main drawback of the traditional Playfair cipher is that the plain text can consist of 25 uppercase letters only. One letter has to be omitted and cannot be reconstructed after decryption. Also lowercase letters, white space, numbers and other printable characters cannot be handled by the traditional cipher. This means that complete sentences cannot be handled by this cipher.

In a monoalphabetic cipher the attacker has to search in 26 letters only. Playfair cipher being a polyalphabetic cipher the attacker has to search in 26 x 26 = 676 digrams. Although the frequency analysis is much more difficult than in monoalphabetic cipher still using modern computational techniques the attacker can decipher the cipher text.

To overcome the drawbacks we propose a modified cipher which uses a 10 x 9 matrix which will contain almost all the printable characters.

5. MODIFIED PLAYFAIR CIPHER

The 10 x 9 matrix contains almost all the printable characters. This includes lowercase and uppercase alphabets, punctuation the case, punctuation marks, special characters and white space intact (white space is part of the character set which we are using). The keyword can be a word or single or multiple sentences (maximum non-duplicate character count can be 90).

In case of duplicate letters in a digram and odd number of characters we use ^ as the padding character during encryption. During decryption all instances of ^ are deleted and we get back the original plain text. The logic of substitution is same as the traditional Playfair cipher.

6. ENCRYPTION USING MODIFIED CIPHER

Let us take the plaintext as **This is a plain text.** Breaking up the plaintext into digrams we get the following digrams and hence the ciphertext.

Th We see that they are neither in the same row or column. Hence using rule 3 we get **Rk**.
is They are neither in the same row or column and thus using rule 3 we get **ux**.
<space>i They are neither in the same row or column. Using rule 3 we get **.p**
s<space> They are neither in the same row or column and using rule 3 we get **v9**
a<space> They are neither in the same row or column. Using rule 3 we get **p;**
pl They are in the same row. Using rule 1 we get **li**
ai They are in the same row. Using rule 1 we get **tc**
n<space> They are neither in the same row or column. Using rule 3 we get **g'**
te They are in the same row. Using rule 1 we get **eb**
xt They are neither in the same row or column. Using rule 3 we get **Ai**
.^ They are neither in the same row or column. Using rule 3 we get **,&**

29

Figure 10: Research Paper 2. (Sanjay Basu, 2012)

International Journal of Computer Applications (0975 – 8887)
Volume 46– No.9, May 2012

Thus the ciphertext will be **Rkux.pv9p;litcg'ebAi,&**

7. DECRYPTION USING MODIFIED ALGORITHM

In case of decryption rules 1 and 2 have to be reversed. Breaking up the cipher text into digrams we get the following digrams and hence the plaintext.

Rk They are neither in the same row or column. Using rule 3 we get **Th**
ux They are neither in the same row or column. Using rule 3 we get **is**
.p They are neither in the same row or column. Using rule 3 we get **<space>i**
v9 They are neither in the same row or column. Using rule 3 we get **s<space>**
p; They are neither in the same row or column. Using rule 3 we get **a<space>**
li They are in the same row. Using reverse of rule 1 we get **pl**
tc They are in the same row. Using reverse of rule 1 we get **ai**
g' They are neither in the same row or column. Using rule 3 we get **n<space>**
eb They are in the same row. Using reverse of rule 1 we get **te**
Ai They are neither in the same row or column. Using rule 3 we get **xt**
,& They are neither in the same row or column. Using rule 3 we get **.^**

Since ^ is to be deleted the plain text which we get is as follows.
This is a plain text.

8. CRYPTANALYSIS OF MODIFIED CIPHER

The various types of cryptanalytic attacks are as follows.
1. Brute force attack
2. Ciphertext only attack
3. Chosen plaintext/ciphertext attack

As far as future scope of work is concerned, the 10 x 9 matrix which is being formed after taking the keyword is formed with a certain sequence of the different printable characters (small letters then capital letters then numerical and then the other printable characters). If we take small letters, capital letters, numerical and other printable characters as four different groups the sequence of the groups can change the 10 X 9 matrix with the same keyword. This should make cryptanalysis more difficult. This can be tried out and the results can be analyzed.

10. ACKNOWLEDGEMENT

The first author would like to thank Jadavpur University authorities for giving him the chance to undertake such a work. He also wishes to thank the second author for the guidance provided to him.

11. REFERENCES

[1] Behrouz A. Forouzan, Cryptography and Network Security. Special Indian Edition 2007, Tata McGraw-Hill Publishing Company Limited, New Delhi.

[2] Wikipedia (http://en.wikipedia.org/wiki/Playfair_cipher)

[3] William Stallings, Cryptography and Network Security Principles and Practices, 4th Edition, Pearson Education.

[4] Atul Kahate, Cryptography and Network Security, 2nd Ed., Tata McGraw-Hill Publishing Company Limited, New Delhi.

[5] Ravindra Babu K, S. Uday Kumar, A. Vinay Babu, I.V.N.S Aditya , P. Komuraiah "An Extension to Traditional Playfair Cryptographic Method", International Journal of Computer Applications (0975 – 8887) Volume 17– No.5, March 2011.

[6] Shiv Shakti Srivastava, Nitin Gupta "A Novel Approach to Security using Extended Playfair Cipher", International Journal of Computer Applications (0975 –

Figure 11: Research Paper 2. (Sanjay Basu, 2012)