2. Caesar Cipher

When Julius Caesar sent messages to his generals, he didn't trust his messengers. So he replaced every A in his messages with a D, every B with an E, and so on through the alphabet. Only someone who knew the "shift by 3" rule could decipher his messages

C = E (k, p) = (p + k) mod26

Example"**KURUKSHETRA UNIVERSITY KURUKSHETRA**" is encoded as (Key=2) "MWTWMUJGVTC **WPKXGTUKVA MWTWMUJGVTC**"

2.1 Analysing Caesar Cipher

Cryptanalysis means breaking codes and ciphers. The decryption algorithm of Caesar cipher is simple. P= D(C) = (C - k) mod 26 If it is known that given cipher text is a Caesar cipher, then a brute-force cryptanalysis can be easily performed. Simply by trying all possible 25 keys a cryptanalyst just has to find the shift that causes the cipher text frequencies to match up closely with the natural English frequencies and then decrypt the text using that shift. This method can be used to easily break Caesar ciphers by hand.

3. 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

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:

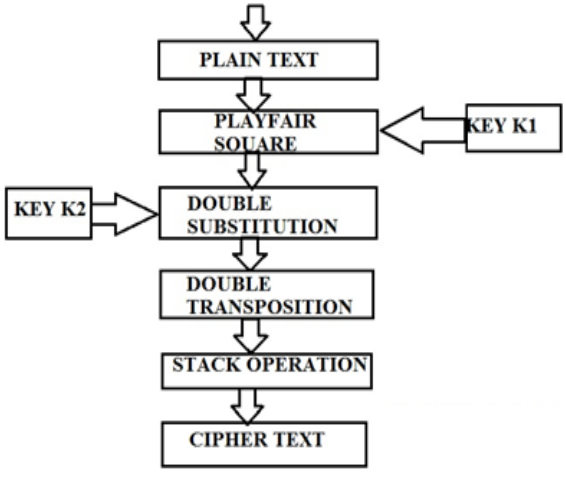
1) Plain text letters that fall in the same row of the matrix are replaced by the letter to the right, with the first element of the row circularly following the last. For example RE is encrypted as EX.
2) Plain text letters that fall in the same column are replaced by the letter beneath, with the top element of the row circularly following in the last. For example, RC is encrypted as CN.
3) 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.

3.1 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. So performing double substitution and transposition on playfair cipher will considerably increases its security.

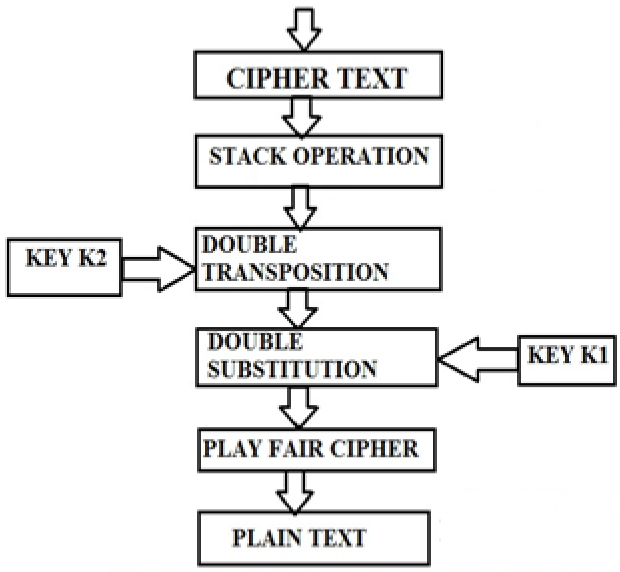
4. Proposed Work

4.1 Block diagram for Encryption algorithm



BLOCK DIAGRAM FOR ENCRYPTION

4.2 Block diagram for decryption algorithm



BLOCK DIAGRAM FOR DECRYPTION

4.3 Encryption Algorithm

1) Take Plain text as input from user.
2) Encrypt the plain text by using playfaircipher, we get CT1.
3) using key k1,encrypt CT1 by performing substitution technique, we get CT2
4) Again encrypt CT2,using key k1 by performing substitution, we get CT3
5) using key key k2,encrypt CT3,by spreading the data across rectangular rows and read them as columns(Transposition technique),we get CT4.
6) again performing Transposition technique on CT4,using key k2,we get CT5
7) now reverse the string CT5,using Stack operation by PUSH and POP,we get CT6
8) CT6 is our required Cipher Text

4.4 Decryption Algorithm

1) Take cipher text as input that is CT6.
2) using stack, reverse the string, we get CT5
3) using key k2 decrypt CT5 by spreading the data across rectangular columns and read them as rows, we get CT4.
4) again decrypt CT4 using key k2 by spreading it across the rectangular columns and read them as rows, we get CT3.
5) Now decrypt the CT3 using key k1,by substitution technique, we get CT2
6) again perform the same decryption technique using key k1,we get CT1
7) now using playfair cipher decrypt the CT1,we get our original plain text
8) Output of step 7,is our required plain text.

5. Example

5.1 Encryption

1) Let the plain text is MY NAME IS ATUL.
2) using playfair cipher encrypt the plain text to obtain cipher text CT1 as shown below, first we break the original plain text into pairs of two alphabets each this means that our original text would now look like this MY NA ME IS AT UL. Now we apply our plainfair cipher algorithm to this text as MY-→XF

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

Similarly the pairs NA,ME,IS,AT,UL
NA-→OL
ME-→IX
IS-→MK
AT-→PV
UL-→LR
As shown below

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

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

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

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

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

Therefore CT1=**"XFOLIXMKPVLR"**

3) Using key k1=2 perform substitution on CT1 as we get CT2 as=**"ZHQNKZOMRXNT"**
4) Repeat Step 3,using Key k2=2,we get CT3 as CT3=**"BJSPMBQOTZPV"**
5) Using key k2,perform transposition technique on CT3,by spreading data across rows and read them as columns as shown, we get CT4=**"SBTVJMOPBPQZ"**

Key k2=3 2 1

Key	3	2	1
	B	J	S
	P	M	B
	Q	O	T
	Z	P	V

6) Repeat Step 5,using key k2,we get CT5 as shown CT5=”**TMBZBJPQSVOP”**

key k2=3 2 1

Key k2	3	2	1
	S	B	T
	V	J	M
	O	P	B
	P	Q	Z
Key k2	3	2	1
	S	B	T
	V	J	M
	O	P	B
	P	Q	Z

7) PUSH CT5=”**TMBZBJPQSVOP”** on stack ,and then POP we get CT6 as shown,CT6=”**POVSQPJBZBMT**”

P
O
V
S
Q
P
J
B
Z
B
M
T

8) Output of CT6 is our required Cipher Text.

5.2 Decryption

1) Take cipher text as input, let it be CT6=”**POVSQPJBZBMT”**
2) Reverse the string, by inserting data into stack, using PUSH and POP operations we get CT5=”**TMBZBJPQSVOP”** as shown

T
M
B
Z
B
J
P
Q
S
V
O
P

3) Using key k2=321 Decrypt CT5 by spread the CT5=”**TMBZBJPQSVOP”** across rectangular columns and read them as rows as shown we get CT4=”**SBTVJMOPBPQZ**” as shown
4) Repeat Step 3,we get CT3,using key k2=321,as shown CT3=”**BJSPMBQOTZPV”**

Key	3	2	1
	B	J	S
	P	M	B
	Q	O	T
	Z	P	V

Key	3	2	1
	B	J	S
	P	M	B
	Q	O	T
	Z	P	V
Key k2	3	2	1
	B	J	S
	P	M	B
	Q	O	T
	Z	P	V

5) Using key k1=2 decrypt by perform substitution on CT3 as we get CT2 as=”**ZHQNKZOMRXNT”**
6) Repeat Step 5,using Key k2=2, decrypt CT2,we get CT1 as CT1=”**XFOLIXMKPVLR”**
7) Using play fair cipher decrypt CT1,we get our original plain text, as shown below

MY <--XF

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

Similarly the pairs NA,ME,IS,AT,UL
NA <--OL
ME <--IX
IS<--MK
AT <--PV
UL <--LR
As shown below

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

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

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

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

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

8) Output of step 7 is our reqired Plain text,which is **"MYNAME IS ATUL"**

6. Advantages of Proposed Algorithm

1) Diverse cipher text: If we scrutinize at the Algorithm we can notice at every Stage we are getting diverse cipher text, thus more trouble to cryptanalyst.
2) Brute force attack on it is impossible
3) There is no chance to cryptanalyze.
4) Overcomes the limitation of simple Playfair square cipher.
5) Easy to perform substitution

7. Disadvantage of Proposed Algorithm

1)It makes use of two keys.
2)Difficult to implement.

8. Conclusion

In this paper we have presented how to improve security of play fair square Cipher to make it more secure and strong by its implementation with substitution and transposition techniques. I we have analyzed the merits and demerits of the original playfair cipher. Then we discussed the modified playfair cipher using double substitution and transposition cipher..

9. Acknowledgment

Author would like to give sincere gratitude especially to Mr. Amit Verma, (HOD CSE) for his guidance and support to pursue this work.

References

[1] Jawadahmaddar,*"Humanizing the Security of Rail Fence Cipher Using Double Transposition and Substitution Techniques*, International *Journal of Science and Research (IJSR) ISSN (Online): 2319-7064,Volume 3 Issue 9, September 2014*
[2] AtulKahate (2009), *Cryptography and Network Security*, second edition, McGraw-Hill
[3] William Stalling"*Network Security Essentials(Applications and Standards)*",Pearson Education,2004
[4] practicalcryptography.com/ciphers/rail-fence-cipher/
[5] Charles P.Pfleeger "Security in Computing", 4th edition, Pearson Education
[6] Neal R. Wagner *"The Laws of Cryptography: Perfect Cryptography: The One-Time Pad "*
[7] jawadahmaddar,sandeepSharma" Implementation of One Time Pad cipher with Rail Fence and Simple Columnar Transposition Cipher, for Achieving Data security,, International *Journal of Science and Research (IJSR) ISSN (Online): 2319-7064,Volume 3 Issue 11, November 2014*
[8] jawadahmaddar, Enhancing the data security of simple columnar transposition cipher by Caesar cipher and Rail fence cipher technique. International Journal of Computer Science & Engineering Technology (IJCSET), ISSN : 2229-3345 Vol. 5 No. 11 Nov 2014

Author Profile

Jawad Ahmad Dar is currently in final year M TECH Computer science and Engineering from Kurukshetra University, Kurukshetra. He did B.TECH in Computer Science and Engineering from Islamic University of Science and Technology Kashmir in2013 (2009 Batch).He has 5 International Publications. His interested areas of research are, Neural Networks, Mobile computing, Network security, and Design and Analysis Algorithms, Advanced Optimization and Simulation Techniques.