SPECIAL SYMBOLIC CRYPTION – CRYPTANALYSIS

[1]V.Ramya , [2]E. Radhika , [3]E.Kalaivani
[1] Kallangutthu, Vandavasi , Thiruvannamalai District.
[2] Head & Assistant Professor, Department of Mathematics, King Nandhivarman College of Arts and Science, Thellar.
[3]Head & Assistant Professor, Department of Mathematics, Sri Akilandeswari Women's College, Wandiwash.

1.Abstract

Cryptography is a technique of sending and receiving secret messages. Simply, it is a very secure way of high end communication. In this competitive world it is safer but also it has to convey the exact message to the receiver. The shorter the message is convenient to encipher and then to decipher. This saves much time for both the sender and receiver of messages. In this concern, in this paper we have introduced the symbol " ^ " and " ~ " as the key for the word "AND " and "NO". For which we are using the symmetric key affine transformation.

2.Definitions

2.1.Plain Text

Plain Text is a message in a readable form, which has to be sent secretly.

2.2.Cipher Text

Cipher Text is a message which is not in a meaningful form.

2.3.Encryption

The process of transforming plain text into cipher text is called Encryption.

2.4.Decryption

The reverse process of turning the cipher text into plain text which is accomplished by the recipient who has the knowledge to remove the disguise is called Decryption.

2.5.Affine Transformation

The more general type of transformation of Z/NZ , is called an affine map

$$C = aP + b(\text{mod } N)$$

Where 'a' and 'b' are fixed integers together they form the enciphering key.

And for plain text $P = a'C + b' \ (\text{mod } N)$, where $a' = a^{-1}$ and $b' = - a^{-1} . b \ (\text{mod } N)$

2.6.Symmetric Key Cryptosystem

A Cryptosystem is called Symmetric key if for each pair (e ,d) , the key 'd' is computationally easy to determine knowing only the 'e' and similarly to determine the 'e' knowing only 'd'.

2.7.Defining the Special Symbolic Key

The Special Symbolic cipher key which has been introduced in this paper is the symbol "^ " and " ~ " as the key for the word "AND " and "NO".

The word "AND" and "NO" can be directly encrypted as "^" and "~".Also "^" and "~" can be directly decrypted as "AND" and "NO" without any kind of restrictions.

ALPHABET	A	E	I	O	U	B	C	D	F	G	H	J	K	L	M	N	P	Q	R	S	T	V	W	X	Y	Z	_
NUMERICAL EQUIVALENT	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

3.Problems

3.1.Encipher the message

“NORTHEAST_AND_NORTHWEST_ARE_NOTABLE”

With special symbolic key and the affine transformation. Use the value of a = 5 and b = 3.

Solution:For an affine transformation we have C = aP + b.

Given that a = 5 , b = 3

3.1.1.Enciphering table

Plain Text	Numerical Equivalent P	C = aP + b (mod 27)	Derivation / Description	Numerical Equivalent C	Cipher Text
N	Direct Transformation				~
O					
R	18	C = (5(18)+ 3) (mod 27)	93 (mod 27)	12	K
T	20	C = (5(20)+ 3) (mod 27)	103 (mod 27)	22	W
H	10	C = (5(10)+ 3) (mod 27)	53 (mod 27)	26	_
E	1	C = (5(1) + 3) (mod 27)	8(mod 27)	8	F
A	0	C = (5(0) + 3) (mod 27)	3 (mod 27)	3	O
S	19	C = (5(19)+ 3) (mod 27)	98 (mod 27)	17	Q
T	20	C = (5(20)+ 3) (mod 27)	103 (mod 27)	22	W
_	26	C = (5(26) +3) (mod 27)	133 (mod 27)	25	Z
A	Direct Transformation				^
N					
D					
_	26	C = (5(26) +3) (mod 27)	133 (mod 27)	25	Z
N	Direct Transformation				~
O					
R	18	C = (5(18) + 3)(mod 27)	93 (mod 27)	12	K
T	20	C = (5(20) + 3)(mod 27)	103 (mod 27)	22	W
H	10	C = (5(10) + 3)(mod 27)	53 (mod 27)	26	_
W	22	C = (5(22) + 3)(mod 27)	113 (mod 27)	5	B
E	1	C = (5(1)+ 3)(mod 27)	8(mod 27)	8	F
S	19	C = (5(19) +3) (mod 27)	98 (mod 27)	17	Q
T	20	C = (5 (20)+3) (mod 27)	103 (mod 27)	22	W
_	26	C = (5(26) +3) (mod 27)	133 (mod 27)	25	Z
A	0	C = 5(0) + 3 (mod 27)	3 (mod 27)	3	O
R	18	C = (5(18) +3) (mod 27)	93 (mod 27)	12	K
E	1	C = (5(1) + 3) (mod 27)	8(mod 27)	8	F
_	26	C = (5(26)+ 3) (mod 27)	133 (mod 27)	25	Z
N	Direct Transformation				~
O					

T	20	C = (5(20) +3) (mod 27)	103 (mod 27)	22	W
A	0	C = (5(0) + 3) (mod 27)	3 (mod 27)	3	O
B	5	C = (5(5) + 3) (mod 27)	28 (mod 27)	1	E
L	13	C = (5(13) +3) (mod 27)	68 (mod 27)	14	M
E	1	C = (5(1) + 3)(mod 27)	8(mod 27)	8	F

The cipher text is

“~KW_FOQWZ^Z~KW_BFQWZOKFZ~WOEMF”

3.2.Problem

Decipher the message

“~KW_FOQWZ^Z~KW_BFQWZOKFZ~WOEMF”

With special symbolic key and the affine transformation. Use the value of a = 5 and b = 3.

Solution

For an affine transformation we have C = aP + b.

Given that a = 5 , b = 3

We know that $P = a^{'}C + b^{'}$ (mod N), where $a^{'} = a^{-1}$ and $b^{'} = - a^{-1} . b$ (mod N)

To find the inverse

5.1 (mod 27) = 5 (mod 27) =5

5.2 (mod 27) = 10 (mod 27) = 10

5.3 (mod 27) = 15 (mod 27) = 15

5.4 (mod 27) = 20 (mod 27) = 20

5.5 (mod 27) = 25 (mod 27) = 25

5.6 (mod 27) = 30 (mod 27) = 3

5.7 (mod 27) = 35 (mod 27) = 8

5.8 (mod 27) = 40 (mod 27) = 13

5.9 (mod 27) = 45 (mod 27) = 18

5.10 (mod 27) = 50 (mod 27) = 23

5.11 (mod 27) = 55 (mod 27) = 1

$a^{'} = a^{-1}$

$a^{'} = 5^{-1}$

$a^{'} = 11$ (mod 27)

$b^{'} = - a^{-1} . b \pmod{27}$

$b^{'} = - 11 . 3 \pmod{27}$

$= - 33 \pmod{27}$

$b^{'} = 21 \pmod{27}$

3.2.1.Deciphering Table

Cipher Text	Numerical Equivalent C	P = Ca' + b' (mod 27) a' = 11 and b' = 21	Derivation / Description	Numerical Equivalent P	Plain Text
~	Direct Transformation				N
					O
K	12	P=(12(11)+21) (mod 27)	153(mod 27)	18	R
W	22	P=(22(11)+21) (mod 27)	263(mod 27)	20	T
_	26	P=(26(11)+21)(mod 27)	307(mod 27)	10	H
F	8	P=(8(11)+21)(mod 27)	109(mod 27)	1	E
O	3	P=(3(11)+21)(mod 27)	54(mod 27)	0	A
Q	17	P=(17(11)+21)(mod 27)	208(mod 27)	19	S
W	22	P=(22(11)+21)(mod 27)	263(mod 27)	20	T
Z	25	P=(25(11)+21)(mod 27)	296(mod 27)	26	_
^	Direct Transformation				A
					N
					D
Z	25	P=(25(11)+21))mod 27)	296(mod 27)	26	_
~	Direct Transformation				N
					O
K	12	P=(12(11)+21) (mod 27)	153(mod 27)	18	R
W	22	P=(22(11)+21) (mod 27)	263(mod 27)	20	T
_	26	P=(26(11)+21)(mod 27)	307(mod 27)	10	H
B	5	P=(5(11)+21)(mod 27)	76(mod 27)	22	W
F	8	P=(8(11)+21)(mod 27)	109(mod 27)	1	E
Q	17	P=(17(11)+21)(mod 27)	208(mod 27)	19	S
W	22	P=(22(11)+21) (mod 27)	263(mod 27)	20	T
Z	25	P=(25(11)+21))mod 27)	296(mod 27)	26	_
O	3	P=(3(11)+21)(mod 27)	54(mod 27)	0	A
K	12	P=(12(11)+21) (mod 27)	153(mod 27)	18	R
F	8	P=(8(11)+21)(mod 27)	109(mod 27)	1	E
Z	25	P=(25(11)+21))mod 27)	296(mod 27)	26	_
~	Direct Transformation				N
					O
W	22	P=(22(11)+21) (mod 27)	263(mod 27)	20	T
O	3	P=(3(11)+21)(mod 27)	54(mod 27)	0	A
E	1	P=(1(11)+21)(mod 27)	32(mod 27)	5	B
M	14	P=(14(11)+21)(mod 27)	175(mod 27)	13	L
F	8	P=(8(11)+21)(mod 27)	109(mod 27)	1	E

The plain text is

"NORTHEAST_AND_NORTHWEST_ARE_NOTABLE"

4.Conclusion

With this Special symbolic cryption, we have converted the plain text into the cipher text and it has been properly re-converted. In this conversion it has been made simpler to convert with help of the special symbolic cryption. The man power to convert the two letter alphabet and a three letter alphabet has been reduced. The number of times the word is repeated is as much as the man power for the conversion has been consumed. And also the time for the conversion has been reduced, which is the most necessary thing where a cryption is needed.

References

1. A Course in Number Theory and Cryptography (Second Edition) , Neal Koblitz, 1987, Springer – Verlag , New York.
2. An Introduction to Cryptography (Second Edition) , Richard A. Mollin, 2007, Chaman And Hall/CRC Taylor and Francis Group, New York.
3. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography(CRC Press Inc.1996).
4. Rosen,K.H.(1984).Elementary Number Theory and Its Applications.Pearson,Newyork.