International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 225-228
Published Online June - July 2016 in IJEAST (http://www.ijeast.com)

SOME TECHNIQUE ALGORITHMS OF CLASSICAL CRYPTOSYSTEMS USING RESIDUE MODULO PRIME NUMBER

Dr.P. Sundarayya
Department of Mathematics
GITAM University, Visakhapatnam,
Andhra Pradesh, India

M .G .Vara Prasad
Department of Mathematics
NSRIT, Visakhapatnam
Andhra Pradesh, India

P.Pari Purna Chari
Department of Mathematics
NSRIT, Visakhapatnam
Andhra Pradesh, India

***Abstract*— The paper discusses about some classical techniques to introduce some strength to these classical encryption and decryption process. For that purpose focused on classical encryption with some techniques using residue modulo prime. The proposed method shown that it is better in terms of providing more security to given text message but it will be more difficult for the attacker to get the key using modulation of prime numbers.**

Keywords— **Encryption algorithm, Decryption algorithm, Residue modulo prime**

I. INTRODUCTION

Cryptography is the mathematical science of writing or solving ciphers. A cipher is a mathematical secret code used in cryptography, the process of convert a plaintext into cipher text is called encryption and reverse process is called decryption. Cryptography is branch of both mathematics and computer science and it is mathematical function of ciphers included drawing from computer science and number theory. A Cipher is a mathematical function which is used in encryption and decryption algorithms. A Cipher can be divided into Symmetric cipher and Asymmetric Cipher. Symmetric Cipher is also called as a secret key cryptography and Asymmetric Cipher is also called as a public key cryptography. A Symmetric Cipher can be divided into stream cipher and block cipher. Stream cipher can break the plain text messages into successive characters or bits p1,p2,p3…………. And encrypt each pk with ith element ki of a key stream K=k1k2k3………..that is ek(p)=ek1(p1)ek2(p2)…………..
Symmetric key cryptography is a classical cryptography .It is divided into four parts.

- The encryption algorithm: The encryption algorithm fulfills various transformations on the plaintext.
- The encryption key: The encryption key is input to the encryption algorithm. The encryption key is a value independent of the plaintext. The exact transformations fulfilled by the encryption algorithm depend on the encryption key.
- The decryption algorithm: The decryption algorithm fulfills various transformations on the cipher text.
- The decryption key: The decryption key is input to the decryption algorithm.

In the symmetric key algorithm authentication and confidentiality are the same because the sender and receiver knows secret keys, the sender sent messages to receiver using secret key and receiver will open the messages using secret key. In this paper we discuss about similar technique of linear cipher and affine cipher. The Proposed method showed that it is better in terms of providing more security to given text message but it will be more difficult for the attacker to get the key using modulation of prime numbers.

II. PRELIMINARIES

P is finite set of possible plain text
C is is finite set of possible cipher text
K is finite set of possible keys
For Key k $\in$ K, there is encryption e_k:P $\rightarrow$ C, decryption d_k: C$\rightarrow$ P such that $d_k(e_k(x))=x$ for every plaintext x$\in$ P [1].

A. *Linear (transformation)cipher-*

In Linear cipher , the cipher text is to be getting from the plain text .Let P=C=Z_m and
K={a$\in$ Z_m / $g.c.d(a,m) = 1$}, Key a $\in$ K ,where Z_m is ring of integers and m>1.Define encryption $e_k(x)$=a x(mod m) and decryption $d_k(y)$= a^{-1}x(mod m **)[1].**

B. Affine cipher-

Let P=C=Z_m and K ={(a,b)$\in$ $Z_m \, X \, Z_m$ / $g.c.d(a,m) = 1$}, Key k=(a, b) $\in$ K, where Z_m is ring of integers and m>1.Define encryption $e_k(x)$=(a x +b)(mod m) and decryption $d_k(y)$= a^{-1} (y-b) (mod m)[1].

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 225-228
Published Online June - July 2016 in IJEAST (http://www.ijeast.com)

III. PROPOSED WORK

A. Computational requirements-

Linear congruence in one variable-

A congruence of a form ax ≡ b (mod m), where ‘x’ is an unknown integer is called linear congruence in one variable

Inverse of a modulo prime number q-
Given an integer a with (a,q)=1, a solution of ax ≡ 1(mod q) is called Inverse of a modulo prime number q .

B. Proposed technique#1-

Let P=C=Z_q,
Let K={(a ,b ,c ,d) /ad-b c $\neq$0, g.c.d($(cx+d),q$)=1, g.c.d($(cy-a),q$)=1 }, , $a,b,c,d \in$ Z_q

$$\text{Encryption: } e_k(x)= \frac{ax+b}{cx+d} \text{ (mod q)}$$

$$\text{Decryption: } d_k(y)= \frac{-dy+b}{cy-a} \text{ (mod q)}$$

For all x,yϵ Z_q

C. Encryption algorithm of proposed technique#1-

- step1:Choose a,b,c,d so that g.c.d($(cx+d),q$) =1, g.c.d($(cy-a),q$)=1 for all x, y, $a,b,d \in$ Z_q, Where q is prime number
- step2: Write $\frac{ax+b}{cx+d}$= $(ax+b)(cx+d)^{-1}$
- step3: Calculate $(cx+d)^{-1}$
- step4:Calculate
  $e_k(x) = (ax+b)(cx+d)^{-1}$ (mod q)
- step5: Write Cipher text

Where q is prime number, for all x , yϵ Z_q

D. Decryption algorithm of proposed technique#1-

- step1: Write $\frac{-dy+b}{cy-a}$=$(-dy+b)(cy-a)^{-1}$
- step2: Calculate $(cy-a)^{-1}$
- step3: Calculate
  $d_k(y) = (-dy+b)(cy-a)^{-1}$(mod q)
- step4: Write Plain text

E. Tables

Table-1
The letters corresponding 29 letters where q=29 is prime number

A	B	C	D	E	F	G	H	I	J
1	2	3	4	5	6	7	8	9	10
K	L	M	N	O	P	Q	R	S	T
11	12	13	14	15	16	17	18	19	20
U	V	W	X	Y	Z	!	?	SPACE	
21	22	23	24	25	26	27	28	29	

Table-2
Multiplicative inverse modulo 29

x	1	2	3	4	5	6	7	8	9	
x≡1mod29	1	15	10	22	6	5	25	11	13	
x	10	11	12	13	14	15	16	17	18	
x≡1mod29	3	8	17	9	27	2	20	12	21	
x	19	20	21	22	23	24	25	26	27	28
x≡1mod29	26	16	18	4	24	23	7	19	14	28

Table-3
The letters corresponding 37 letters q=37 prime

A	B	C	D	E	F	G	H	I	J
1	2	3	4	5	6	7	8	9	10
K	L	M	N	O	P	Q	R	S	T
11	12	13	14	15	16	17	18	19	20
U	V	W	X	Y	Z	0	1	2	3
21	22	23	24	25	26	27	28	29	31
4	5	6	7	8	9	SPACE			
31	32	33	34	35	36	37			

Table-4
Multiplicative inverse modulo 37

X	1	2	3	4	5	6	7	8	9
x≡1mod37	1	19	25	28	15	31	16	14	33
X	10	11	12	13	14	15	16	17	18
x≡1mod37	26	27	34	20	8	5	7	24	35
X	19	20	21	22	23	24	25	26	27
x≡1mod37	2	13	30	32	29	17	3	10	11
X	28	29	30	31	32	33	34	35	36
x≡1mod37	4	23	21	6	22	9	12	18	36

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 225-228
Published Online June - July 2016 in IJEAST (http://www.ijeast.com)

F. Example of Proposed technique#1

Plain text="YEAR 2016"
From the table-3 assigning labels to YEAR 2016

Y	E	A	R	SPACE	2	0	1	6
25	5	1	18	37	29	27	28	33

Encryption:

Choose a, b, c, d so that g.c.d $((cx+d), q)$ =1, g.c.d $((cy-a), q)$ =1 for all x, y, $a, b, d \in Z_q$

Choose $q = 37, a = 2, b = 5, c = 3, d = 3,$
ad-b c $\neq 0$

$\therefore$ g.c.d $((3x+3), 37)$ =1, g.c.d $((3y-2), 37)$ =1 for all x, y $\in Z_{37}$

$e_k(25) = \frac{2(25)+5}{3(25)+3} = (2(25)+5)(3(25)+3)^{-1}$
$=(55)\ (78)^{-1}$ mod 37=(18) $(4)^{-1}$(mod 37)
($\because$ Table-4)

=(18)(28)(mod 37)=23

$e_k(25)$= 23

$e_k(5) = \frac{2(5)+5}{3(5)+3}$=(15) $(18)^{-1}$(mod 37) =7

$e_k(1) = \frac{2(1)+5}{3(1)+3}$=(7) $(6)^{-1}$(mod 37) =32

$e_k(18) = \frac{2(18)+5}{3(18)+3}$=(4) $(20)^{-1}$(mod 37) =15

$e_k(37) = \frac{2(37)+5}{3(37)+3}$=(20) $(20)^{-1}$mod 37 =14

$e_k(29) = \frac{2(29)+5}{3(29)+3}$=(26) $(16)^{-1}$(mod 37) =34

$e_k(27) = \frac{2(27)+5}{3(27)+3}$=(22) $(10)^{-1}$(mod 37) =17

$e_k(28) = \frac{2(28)+5}{3(28)+3}$=(24) $(13)^{-1}$(mod 37) =36

$e_k(33) = \frac{2(33)+5}{3(33)+3}$=(34) $(28)^{-1}$(mod 37) =25

23	7	32	15	14	34	17	36	25
W	G	5	O	N	7	Q	9	Y

Cipher text="WG5ON7Q9Y"

Decryption:

$d_k(23) = \frac{-3(23)+5}{3(23)-2}$== (18) $(4)^{-1}$(mod 37)=23

$d_k(7) = \frac{-3(7)+5}{3(7)-2}$== (21) $(19)^{-1}$(mod 37)=5

$d_k(32) = \frac{-3(32)+5}{3(32)-2}$== (20) $(20)^{-1}$(mod 37)=1

$d_k(15) = \frac{-3(15)+5}{3(15)-2}$== (34) $(6)^{-1}$(mod 37)=18

$d_k(14) = \frac{-3(14)+5}{3(14)-2}$== (0) $(3)^{-1}$(mod 37)=37

$d_k(34) = \frac{-3(34)+5}{3(34)-2}$== (14) $(26)^{-1}$(mod 37)=29

$d_k(17) = \frac{-3(17)+5}{3(17)-2}$== (28) $(12)^{-1}$(mod 37)=27

$d_k(36) = \frac{-3(36)+5}{3(36)-2}$== (8) $(32)^{-1}$(mod 37)=28

$d_k(25) = \frac{-3(25)+5}{3(25)-2}$== (4) $(36)^{-1}$(mod 37)=33

Plain text="YEAR 2016"

G. Proposed technique#2-

Let P=C=Z_q,
Let K={(a ,b ,c ,d, e) /ad-b c $\neq$0, g.c.d$((cx+d), q)$=1, g.c.d$((cy-a), q)$=1 },
a ,b ,c ,d, e ϵ Z_q

Encryption: $e_k(x) = \left(\frac{ax+b}{cx+d} + e\right)$ (mod q)

Decryption: $d_k(y) = \left(\frac{-d(y-e)+b}{c(y-e)-a}\right)$ (mod q)

Where q is prime number, for all x , yϵ Z_q

G. Encryption algorithm of proposed technique#2-

- step1:Choose a, b, c, d, e so that g.c.d$((cx+d), q)$ =1, g.c.d$((cy-a), q)$=1 for all x, y, $a, b, d, e \in Z_q$
- step2: Write $\frac{ax+b}{cx+d} = (ax+b)(cx+d)^{-1}$
- step3: Calculate $(cx+d)^{-1}$
- step4:Calculate
  $e_k(x) = ((ax+b)(cx+d)^{-1} + e)$ (mod q)
- step5: Write Cipher text

H. Decryption algorithm of proposed technique#2-

- step1: Write $\frac{-dy+b}{cy-a}$=$(-dy+b)(cy-a)^{-1}$
- step2: Calculate $(cy-a)^{-1}$
- step3: Calculate
  $d_k(y) = (-d(y-e)+b)(c(y-e)-a)^{-1}$(mod q)
- step4: Write plain text

I. **Example of Proposed technique#2-**

Plain text=ÝES

From the Table-1 assigning labels to YES

Y	E	S
25	5	19

Encryption:

Choose a, b, c, d, e so that g.c.d $((cx+d), q)$ =1, g.c.d $((cy-a), q)$ =1 for all x, y, $a, b, d, e \in Z_q$

Choose $q = 29, a = 6, b = 1, c = 6, d = 5,$ ad-b c $\neq$0,e=5

$\therefore$ g.c.d $((4x+3), 29)$ =1, g.c.d $((4y-2), 29)$ =1 for all x, y $\in Z_{29}$

$e_k(25)=(\frac{6(25)+1}{6(25)+5}+5)=((6)\ (10)^{-1}+5)$(mod 29) =23

$e_k(5)=(\frac{6(5)+1}{6(5)+5}+5)=((2)\ (6)^{-1}+5)$(mod 29) =15

$e_k(19)=(\frac{6(19)+1}{6(19)+5}+5)=((10)\ (21)^{-1}+5)$(mod 29) =11

23	15	24
W	O	X

Cipher text="WOX"

Decryption:

$d_k(23) = \frac{-5(23-5)+1}{6(23-5)-6}$== (27) $(15)^{-1}$(mod 29)=25

$d_k(15) = \frac{-5(10)+1}{6(10)-6}$== (2) $(6)^{-1}$(mod 29)=5

$d_k(24) = \frac{-5(19)+1}{6(19)-6}$== (22) $(21)^{-1}$(mod 29)=19

Plain text=ÝES'

IV. SECURITY ANALYSIS

Proposed technique #1 consists four tuple keys so it is more secure whereas proposed technique #2 is more more secure than Proposed technique #1as it has five tuple keys but Proposed technique #1 and Proposed technique #2 must satisfy the following conditions

g.c.d($(cx+d), q$)=1…………(1)

g.c.d($(cy-a), q$)=1…………(2)

for all x ,y $\in Z_q$

As the two techniques satisfy above conditions then These two techniques overcome the known plain text attack, chosen cipher text attack and chosen plain text attack.

V. CONCLUSION

This paper presents a classical cryptosystem that is variation of the linear cipher and the affine cipher because of proposed technique#1 has 4 tuple keys and proposed technique#2 has 5 tuple keys. The proposed algorithms providing some classical cryptosystems increasing its defiance to various attacks such as a known plain text attacks .The proposed algorithm is more secure in encryption and decryption under modulation prime numbers than original linear and affine cipher. Since the modulus is a prime number and the proposed key security greatly increased and the cipher text-only attack is also to oppose successfully.

VI. REFERENCE

[1] Douglas R. Stinson, Cryptography Theory and practice third edition (2006) by chapman & Hall/CRC Taylor &Francis Group.

[2] Castaneda, Roberto. G. (2009). Using Classical Ciphers in Secondary Mathematics. Thesis, Presented to the Honors Committee of McCurry University

[3] Koblenz, N. A Course in Number Theory and Cryptography, 2nd ed. New York: Springer-Verlag, 1994

[4] Introduction to Analytic Number Theory, fifth edition. T. Apostol .Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1995

[5] Analysis and Design of Affine and Hill Cipher, Journal of Mathematics Research Vol. 4, No. 1; February 2012