AN OVERVIEW OF CRYPTOGRAPHY ALGORITHM WITH APPLICATION OF NUMBER THEORY

[1]Ajay Bhaurao Rathod

Government Vidarbha Institute of Science and Humanities, Amaravati

Abstract: The Advance cryptography is one of the important themes of mathematics in the current paper we discussed that how the application of mathematics especial Algebra including number theory is exploring the cryptographic concepts the primary intention of this paper is that to provided assort the study of cryptography in modern algebra or Number theory. The general use of cryptography is designing the system which is used for securing the data. Here we are more towards some various cryptographic ciphers and give a review on some mathematical concept regarding with Number theory and group theory.

Keywords: Cryptography, Number theory, group theory, system design.

Introduction:

Cryptography is the branch of mathematics which deals with improving schemes and different formulas to develop the personalization of communication system by using different code. This field allow us to use in different sectors it may be government of private sector. This is helpful to maintain confidential communication. Actually, it is the way to preserve a data from spoiling. Cryptography especially modern cryptography depends on the system which is associated with advance mathematics containing a sub branch of mathematics known as Number theory which studied various characteristic and relation between them.it is used to checked and to secure the data along with its isolation. Cryptography is Greek word which was originally Krypto's means to hide. Advance cryptography is constructed on algebraic foundation and number theory. The cryptography which is based on factorization and discrete log-based cryptography containing standard curve which was elliptical with a possibly quantum resistance is of cryptography was currently discovered. It makes use of isogonics on elliptical curve and its privacy depends on presumed complexity of observing an isogeny between and two elliptic curves that we have unity. An algorithm used for obtaining the solution of mathematics which is used to construct cryptosystem in the current paper we discuss what is the relation cryptography with mathematics and its application.

Cryptography with linear algebra:

1. Encoding which we are called encrypting of a massage is done by cipher through the Matrix application by inverting the matrix encrypting process was to be done for the use of decrypting.
2. In this matrix with three into three of integers which are used randomly as a sample in cipher matrix.
3. For decoding the plain text every term in that message must be shown by numerical value which we need to keep in the matrix.
4. The numerical value then planes in its range. But if we take an example of our alphabet number in which if we denote the numerical value 1 to 26 for the alphabet A to Z. and the number 27 are can used for the space.
5. After that the multiplicative matrix along with cipher matrix for the formation of new matrix which contain massage including cipher text.

Massage Encryption:

- The values especially numerical value which was obtained in decrypting contained every character of the plain text given in the form of numerical value.
- The numerical value which was obtained us we need to distribute in vector forms. So that we get the rows number of each vector which is equal to rows of cipher matrix.
- When we put all the values of matrix in each vector in one time, we move towards the down in the row for finding each and every value. The vector is putted by the plaintext and the persisting numbers will be number for space.
- The obtained vectors are then referred to form new matrix which include plaintext.
- The matrix which is to be plaintext is to be product with the matrix of cipher with the cipher text matrix.

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

Method of factorization:

It is depending on the thing in which every matrix is placed as the multiplication of lower triangular Matrix with a triangular matrix in which upper form given the form of minors with non-singular forms. i.e.

if M = [Pij] thenType equation here.

$$Pij \neq O\begin{bmatrix} P_{11} & P_{12} \\ P_{21} & P_{22} \end{bmatrix} \neq O\begin{bmatrix} P_{11} & P_{12} & P_{13} \\ P_{21} & P_{22} & P_{23} \\ P_{31} & P_{32} & P_{33} \end{bmatrix} \neq 0$$

$P_{11} L_1 + P_{12} L_2 + P_{13} L_3 = S_1$

$P_{21} L_1 + P_{22} L_2 + P_{23} L_3 = S_2$

$P_{31} L_1 + P_{32} L_2 + P_{33} L_3 = S_3$

So above equation we can write as a ML= S

$$M=\begin{bmatrix} P_{11} & P_{12} & P_{13} \\ P_{21} & P_{22} & P_{23} \\ P_{31} & P_{32} & P_{33} \end{bmatrix},\ L=\begin{matrix} L_1 \\ L_2 \\ L_3 \end{matrix},\ S=\begin{matrix} S_1 \\ S_2 \\ S_3 \end{matrix}$$

Let M= NR

$$\begin{pmatrix} 1 & 0 & 0 \\ L_{21} & 1 & 0 \\ L_{31} & L_{32} & 1 \end{pmatrix}, R=\begin{matrix} r_{11} \\ 0 \\ 0 \end{matrix}\begin{pmatrix} r_{12} & r_{13} \\ r_{22} & r_{23} \\ 0 & r_{33} \end{pmatrix}$$

Then NRM can be written as NRM = S

If we use RM = W_1

So that LW = S which is similar to the $W_1=S_1$

$L_{31}W_1 + L_{32}W_2 + W_3$ by solving this equation we can find the value of W_1, W_2, W_3

And the equation will be $R_{11}L_1+R_{12}L_2+R_{13}L_3=W_{11}R_{22}L_2+R_{23}L_3=W_{21}$

And $R_{33}L_3 = W_3$

From which L_1, L_2, L_3 found us through substitution so for finding matrix N and R written as

$$\begin{pmatrix} 1 & 0 & 0 \\ n_{21} & 1 & 0 \\ n_{31} & n_{32} & 1 \end{pmatrix}\begin{pmatrix} r_{11} & r_{12} & r_{13} \\ 0 & r_{22} & r_{23} \\ 0 & 0 & r_{33} \end{pmatrix}=\begin{pmatrix} P_{11} & P_{12} & P_{13} \\ P_{21} & P_{22} & P_{23} \\ P_{31} & P_{32} & P_{33} \end{pmatrix}$$

By multiplying with the matrix on left by equalizing respective terms from both side

$R_{11} = P_{11}$, $R_{12} = P_{12}$, $R_{13} = P_{13}$

$N_{11}R_{11} = P_{21}$, $N_{21}=P_{21}\backslash P_{11}$

$N_{21}R_{21} + N_{22} = P_{22}$

$N_{31}R_{31} + I_{32}R_{22} = P_{32}$

$N_{31}R_{31} + I_{33}R_{23} = P_{33}$

So, we get the elements of Nand R in the following sequence

a) Initial row of R
b) Initial row of N
c) Next row of R_1
d) Second next row of N_1
e) Next to second row of R_1

Which can be generalized easily.

We can encrypt the following.

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

X	Y	Z
1	2	3

G I V E M E

10 12 28 8 0 8 0

$$\begin{bmatrix}1 & 2\\3 & 4\end{bmatrix}\begin{bmatrix}1 & 2\\3 & 4\end{bmatrix} = \begin{bmatrix}10 & 24\\3 & 48\end{bmatrix}(mod 26)$$

$$\begin{bmatrix}1 & 2\\3 & 4\end{bmatrix}\begin{bmatrix}10\\12\end{bmatrix}=\begin{bmatrix}10+ & 24\\30+ & 48\end{bmatrix}(mod26)=\begin{bmatrix}34\\10\end{bmatrix}mod\ (26)$$

$$\begin{bmatrix}1 & 2\\3 & 4\end{bmatrix}\begin{bmatrix}28\\8\end{bmatrix}=\begin{bmatrix}28+ & 16\\84+ & 8\end{bmatrix}(mod26)$$

$$\begin{bmatrix}1 & 2\\3 & 4\end{bmatrix}\begin{bmatrix}28\\8\end{bmatrix}(mod26)=\begin{bmatrix}44\\92\end{bmatrix}(mod26)=\begin{bmatrix}16\\8\end{bmatrix}(mod26)$$

$$\begin{bmatrix}1 & 2\\3 & 4\end{bmatrix}\begin{bmatrix}0\\16\end{bmatrix}(mod26)=\begin{bmatrix}0+32\\0+16\end{bmatrix}(mod26)=\begin{bmatrix}8\\12\end{bmatrix}(mod26)$$

$$\begin{bmatrix}1 & 2\\3 & 4\end{bmatrix}\begin{bmatrix}8\\0\end{bmatrix}(mod26)=\begin{bmatrix}8+0\\32+0\end{bmatrix}(mod26)$$

$$\begin{bmatrix}1 & 2\\3 & 4\end{bmatrix}\begin{bmatrix}8\\0\end{bmatrix}(mod26)=\begin{bmatrix}8\\24\end{bmatrix}(mod26)=\begin{bmatrix}20\\4\end{bmatrix}(mod26)$$

Now the massage P H Y S I C S

P	H	Y	S	I	C	S
19	11	2	22	12	6	22

Similarly we can encoding the physic by using the matrix

$$P\begin{bmatrix}1 & 3\\2 & 1\end{bmatrix},B\begin{bmatrix}2 & 4\\1 & 3\end{bmatrix}$$

I G O T O C L A S S

A	B	C	D	E	F
4	5	6	7	8	9
G	H	I	J	K	L
10	11	12	13	14	15
M	N	O	P	Q	R

16	17	18	19	20	21
S	T	U	V	W	X
22	23	24	25	0	1
Y	Z				
2	3				

$S_1 = \begin{bmatrix}12\\0\end{bmatrix}, S_2 = \begin{bmatrix}11\\19\end{bmatrix}, S_3 = \begin{bmatrix}0\\24\end{bmatrix}, S_4 = \begin{bmatrix}19\\0\end{bmatrix}, S_5 = \begin{bmatrix}7\\16\end{bmatrix}, S_6 = \begin{bmatrix}5\\23\end{bmatrix}, S_7 = \begin{bmatrix}23\\0\end{bmatrix}$

'O' is the notation for space between two words.

$$\begin{bmatrix}1 & 3\\2 & 1\end{bmatrix}\begin{bmatrix}3 & 1\\2 & 4\end{bmatrix} 0(mod) = \begin{bmatrix}3+6 & 1+12\\6+2 & 2+4\end{bmatrix}\begin{bmatrix}12\\0\end{bmatrix}(mod\ 26)$$

$$\begin{bmatrix}1 & 3\\2 & 1\end{bmatrix}\begin{bmatrix}3 & 1\\2 & 4\end{bmatrix}\begin{bmatrix}12\\0\end{bmatrix} = \begin{bmatrix}9 & 13\\8 & 8\end{bmatrix}\begin{bmatrix}12\\0\end{bmatrix}(mod\ 26)$$

$$= \begin{bmatrix}108+ & 0\\96 & 0\end{bmatrix}(mod\ 26) = \begin{bmatrix}108\\96\end{bmatrix}(mod26) = \begin{bmatrix}12\\2\end{bmatrix}(mod\ 26)$$

$$= \begin{bmatrix}1 & 3\\2 & 1\end{bmatrix}\begin{bmatrix}3 & 1\\2 & 4\end{bmatrix}\begin{bmatrix}11\\19\end{bmatrix}(mod\ 26) = \begin{bmatrix}3+6 & 1+12\\6+2 & 2+4\end{bmatrix}\begin{bmatrix}4\\16\end{bmatrix}(mod\ 26)$$

$$\begin{bmatrix}1 & 3\\2 & 1\end{bmatrix}\begin{bmatrix}3 & 1\\2 & 4\end{bmatrix}\begin{bmatrix}11\\19\end{bmatrix} = \begin{bmatrix}9 & 13\\8 & 8\end{bmatrix}\begin{bmatrix}11\\19\end{bmatrix}(mod\ 26)$$

$$= \begin{bmatrix}99+247\\88+167\end{bmatrix}(mod\ 26) = \begin{bmatrix}346\\250\end{bmatrix}(mod\ 26)$$

$$\begin{bmatrix}1 & 3\\2 & 1\end{bmatrix}\begin{bmatrix}3 & 1\\2 & 4\end{bmatrix}\begin{bmatrix}0\\24\end{bmatrix}(mod\ 26) = \begin{bmatrix}3+6 & 1+12\\6+2 & 2+4\end{bmatrix}\begin{bmatrix}0\\24\end{bmatrix}(mod\ 26)$$

$$\begin{bmatrix}9 & 13\\8 & 6\end{bmatrix}\begin{bmatrix}0\\24\end{bmatrix}(mod\ 26) = \begin{bmatrix}0+312\\0+144\end{bmatrix}(mod\ 26)$$

$$\begin{bmatrix}1 & 3\\2 & 1\end{bmatrix}\begin{bmatrix}3 & 1\\2 & 4\end{bmatrix}\begin{bmatrix}19\\0\end{bmatrix}(mod\ 26) = \begin{bmatrix}3+6 & 1+12\\6+2 & 2+4\end{bmatrix}\begin{bmatrix}19\\0\end{bmatrix}(mod\ 26)$$

$$\begin{bmatrix}1 & 3\\2 & 1\end{bmatrix}\begin{bmatrix}3 & 1\\2 & 4\end{bmatrix}\begin{bmatrix}19\\0\end{bmatrix}(mod\ 26)\begin{bmatrix}9 & 13\\8 & 6\end{bmatrix}\begin{bmatrix}19\\0\end{bmatrix}(mod\ 26)$$

$$=\begin{bmatrix}171 & 0\\152 & 0\end{bmatrix}\begin{bmatrix}19\\0\end{bmatrix}(mod\ 26)$$

$$\begin{bmatrix}1 & 3\\2 & 1\end{bmatrix}\begin{bmatrix}3 & 1\\2 & 4\end{bmatrix}\begin{bmatrix}7\\16\end{bmatrix}(mod\ 26)=\begin{bmatrix}3+6 & 1+12\\6+2 & 2+4\end{bmatrix}\begin{bmatrix}7\\16\end{bmatrix}(mod\ 26)$$

$$\begin{bmatrix}9 & 13\\8 & 4\end{bmatrix}\begin{bmatrix}7\\16\end{bmatrix}(mod\ 26)=\begin{bmatrix}63+208\\56+64\end{bmatrix}(mod\ 26)$$

$$\begin{bmatrix}9 & 13\\8 & 4\end{bmatrix}(mod\ 26)$$

$$\begin{bmatrix}9\\2\end{bmatrix}(mod\ 26)$$

$$\begin{bmatrix}1 & 3\\2 & 1\end{bmatrix}\begin{bmatrix}3 & 1\\2 & 4\end{bmatrix}\begin{bmatrix}5\\23\end{bmatrix}(mod\ 26)=$$

$$\begin{bmatrix}3+6 & 1+12\\6+2 & 2+4\end{bmatrix}\begin{bmatrix}5\\23\end{bmatrix}(mod\ 26)$$

$$\begin{bmatrix}1 & 3\\2 & 1\end{bmatrix}\begin{bmatrix}3 & 1\\2 & 4\end{bmatrix}\begin{bmatrix}5\\23\end{bmatrix}(mod\ 26)=\begin{bmatrix}45 & 299\\40 & 138\end{bmatrix}(mod\ 26)$$

$$\begin{bmatrix}9\\8\end{bmatrix}(mod\ 26)$$

$$\begin{bmatrix}1 & 3\\2 & 1\end{bmatrix}\begin{bmatrix}3 & 1\\2 & 4\end{bmatrix}\begin{bmatrix}23\\0\end{bmatrix}=\begin{bmatrix}3+6 & 1+12\\6+2 & 2+4\end{bmatrix}(mod\ 26)$$

$$\begin{bmatrix}1 & 3\\2 & 1\end{bmatrix}\begin{bmatrix}3 & 1\\2 & 4\end{bmatrix}\begin{bmatrix}23\\0\end{bmatrix}=\begin{bmatrix}9 & 13\\8 & 6\end{bmatrix}\begin{bmatrix}23\\0\end{bmatrix}(mod\ 26)$$

$$=\begin{bmatrix}197 & 0\\184 & 0\end{bmatrix}(mod\ 26)$$

$$=\begin{bmatrix}197\\184\end{bmatrix}(mod\ 26)$$

REFRENCES

1. N. Koblitz. Elliptic curve cryptosystems. Math. Comp., 46(178):203-208, 1988.
2. L. J. William Veque. Fundamentals of Number Theory. Dover Publications, Inc., New York, 1975.
3. S. Victor a Computational Introduction to Number Theory and Algebra. Cambridge University Press, 2009.
4. S.H. Joseph. An Introduction to the Theory of Elliptic Curves, 2009. Slides of a summer school on Computational Number Theory and Applications to Cryptography at University of Wy
5. T.John ,H.S Joseph H. Rational Points on Elliptic Curves. Springer-Verlag, New York, 1993.
6. S.M. Harold M. S. An Introduction to Number Theory. The MIT Press, Com-bridge, Massachusetts, 1971.
7. T. Wade and Lawrence C. Introduction to Cryptography with Coding Theory. Pearson Prentice Hall, Upper Saddle River, New Jersey 07459, 2006.
8. C. Lawrence C. Washington. Elliptic Curves: Number Theory and Cryptography. Chapman & Hall/CRP, Boca Raton, 2004.
9. W Eric .and W. Rabin-M. Strong Pseudoprime Test. From Math-World – A Wolfram Web Resource.