A New Algorithm With Its Randomness And Effectiveness Against Statistical Tests In Data Encryption

Sanjay Poptani , Manish Kumar Tiwari , Dr A.V.N Krishna

Abstract: In the world where security is one of the main concern, we are still not able to make our data secure. Privacy is one of the major concerns in today's world, where all the organization are dealing with data leak problem, data theft, data intrusion. We came up with a mathematical model to encrypt and decrypt data securely. In this paper we have came up with a technique to encrypt and decrypt data using non-deterministic random numbers and generating two cipher text for each data unit (character) and verified the randomness of our cipher text using chi-square test, Gaps test.

Index Terms : Non-deterministic random numbers, Cryptography, Encryption, Decryption, Chi-square test, Gaps test.

1 INTRODUCTION & LITERATURE STUDY

IN the present-day scenario, there is sudden increase in number of cases of data breaches ,at any time any data/information is transfer/send it need to be safe and secure. The ATM pins, credit card details and many other important information need to be protected from intruder and different encryption technique is used to achieve safe transfer to avoid information hacking. Different encryption techniques are use to attain the data security such as AES, DES, etc. Encryption - The process of encrypting data to secure it, it is process of converting data using different technique to transform data into unreadable/without any meaning form ,encrypted data is known as cipher text. Decryption - The process of decrypting the cipher text to get back the original data. Cipher text - Encrypted data, which is unreadable and makes no sense until converted to plain text. Plain text -The original data that need to be encrypted before transfer. Key – it is alphanumeric/numeric/text/special symbol which is used to encrypt/decrypt data. In the work [1], the authors discussed the concept of public Key cryptography using Matrices over group rings. The work [2] deals with development of New algorithm in symmetric encryption mode and work [3] deals with development of a model for random number generation. The work [4] deals with role of statistical tests in evaluating strength of New encryption algorithm and [5] deals with randomness in digital cryptography. James L. Massey [6] pointed out that there are two goals that cryptography aims to achieve as they are: authenticity and/or secrecy. In terms of the security that it affords (which can be either practical or theoretical), he discussed both Shannon's theory of theoretical secrecy as well as Simmon's theory of theoretical authenticity. Othman O. Khalifa [7] demonstrated the primary basic concepts, characteristics, and goals of cryptography.

- *Sanjay Poptani, Student, CSE, Faculty of Engineering, CHRIST (Deemed to be University), Bengaluru ,India , 7829171892, poptani360@gmail.com*
- *Manish Kumar Tiwari , Student, CSE, Faculty of Engineering, CHRIST (Deemed to be University), Bengaluru,India ,8225800163, manish.tiwari@btech.christuniversity.in*
- *Dr.Addepalli VN Krishna, Professor, CSE, Faculty of Engineering, CHRIST (Deemed to be University), Bengaluru, India , 9849520995,adapalli.krishna@christuniversity.in*

They discussed that in our age, i.e. the age of information, communication has contributed to the growth of technology and therefore has an important role that requires privacy to be protected and assured when data is sent through the medium of communication. A crypto analysis on Ergodic based systems are studied is discussed in this work [8].

2 METHODOLOGY USED

We have come up with an algorithm which uses non deterministic random number to encrypt data. We have formulated a mathematical model to encrypt the data using non-deterministic random numbers and generating two cipher text for single data unit (single character). In our mathematical model, the decryption is done using the two cipher text generated and the private key of the receiver . We have USED El-Gamal model of encryption and thus formulated different equation for decryption. Thus decryption takes place without using the non-deterministic random numbers which was used for encryption. There are two equations in our algorithm .First equation to generate two cipher text using non deterministic random numbers and second equation for decryption using two cipher texts. The randomness of cipher text is tested using Chi-square test.

3 DIFFERENT MODULES OF WORK

i. Generating a mathematical model
ii. Selecting suitable key
iii. Generating a Non-deterministic random number
iv. Converting plain text to intelligible form
v. Complexity Analysis
vi. Gaps test and Chi-Square test
vii. Example problem
viii. Conclusion and future work

4 GENERATING A MATHEMATICAL MODEL

Encryption Equation

$$C1 = pt + pb^{r} mod\ p$$
$$C2 = G^{r} mod\ p$$
$$E = (C1, C2)$$

Decryption Equation

$$D = C1 - (C2)^r mod\ p$$

Where,
Pt = plain text
Pb = Public Key = G ^ n mod p
r = random number taken
G= Base value considered
p= Field, which are used as Global parameters.
n = Private Key being used at Receiver's side.
C1=cipher text 1
C2 =cipher text 2

5 SELECTING A SUITABLE KEY

Selected randomly by any of the random number generation algorithms.

A prime number is considered.

The Base value considered and the field means prime number form the global variables.

Let n be the Private Key. The base value powered to the private key will form the public key.

Known the public key, it is powered with a random number and hence the sequence is generated.

6 EXAMPLE

G = 17
n = 5
p = 27
r = 89,16,7,6,14,12,2,5,21,4,9,38,13
Pt =" this is example "

Assigning alphabetic order to plain text such as below
a=1, b=2, c=3…….z=26

Encryption

$$T = (20 + (17^5 \bmod 27)^{89}, \quad 17^{89} \bmod 27$$
$$= (20 + 68590) mod\ 27, \quad 19$$
$$= 3, \quad 19$$
$$H = (8 + (17^5 \bmod 27)^{16} \bmod 27), \quad 17^{16} \bmod 27$$
$$= (8 + 19) \bmod 27, \quad 10$$
$$= 0, 10$$

Similarly,

Other values are as follows

$$I = 1, 10$$
$$S = 20, 1$$
$$I = 19, 19$$
$$S = 20, 1.$$
$$E = 15, 19$$
$$X = 14, 8$$
$$A = 2, 1$$
$$M = 5, 10$$
$$P = 15, 26$$
$$L = 22, 19$$
$$E = 24, 10$$

Alphabet(Alphabetic number)	Cipher text 1 (c1)	Cipher text 2(c2)
T(20)	3	19
H(8)	0	10
I(9)	1	10
S(19)	20	1
I(9)	19	19
S(19)	20	1
E(5)	15	19
X(24)	14	8
A(1)	2	1
M(13)	5	10
P(160	15	26
L(12)	22	19
E(5)	24	10

Decryption

$$T = 3 - 19^5 \bmod 27$$
$$= 3 - 10$$
$$= -7$$
$$= -7 \bmod 27$$
$$= 20$$

$$H = 0 - 10^5 \bmod 27$$
$$= 0 - 19$$
$$= -19$$
$$= -19 \bmod 27$$
$$= 8$$

Similarly,

Other values are as follows

$$I = 9$$
$$S = 19$$
$$I = 9$$
$$S = 19$$
$$E = 5$$
$$X = 24$$
$$A = 1$$
$$M = 13$$
$$P = 16$$
$$L = 12$$
$$E = 5$$

7 CHI-SQUARE TEST

Chi square test
In cryptanalysis, chi squared test is used to compare the distributions of plain text (possibly) decrypt cipher text. The lowest value of the test means the decryption was successful with high probability. This method can be generalized for solving modern cryptographic problems and their various approaches.

Dataset:-
It consists of various cipher text obtained from the plain text as C1 and C2.

[(3,19),(0,10),(1,10),(20,1),(19,19),(20,1),(15,19),(14,8),(3,1),(5,10),(15,26),(22,19),(24,10)]

$$N = 26 \text{ (total no of cipher text)}$$
$$E_i = N \div n \geq 5$$

$= 26 \div n \geq 5$

$n = 5$

Intervals	O_i	E_i	$(O_i - E_i)^2 \div E_i$
0-6	8	5	1.8
7-12	5	5	0
13-18	3	5	0.8
19-24	9	5	3.2
25-30	1	5	3.2

$= \sum(O_i - E_i)^2 \div E_i$

$= 9 \div 5$

$= 1.8$

$SINCE, the\ value\ obtained\ is\ less\ than\ 14.6$

$\therefore the\ sequence\ is\ random$

8 GAPS TESTS

Dataset:
[(3,19),(0,10),(1,10),(20,1),(19,19),(20,1),(15,19),(14,8),(3,1),(5,10),(15,26),(22,19),(24,10)]

	0	1	2	3	5	6	7	9	13	15
0	Y									
1			Y	Y	Y					
3										Y
5	Y									
8	Y									
10		Y			Y				Y	
14	Y									
15							Y			
19	Y			Y		Y		Y		
20				Y						
22	Y									
24	Y									
26	Y									

$N = 26 \qquad \{no\ of\ terms\}$

LIMIT	OCCURENCE	FREQUENCY	RELATIVE FREQUENCY	COMMULATIVE FREQUENCY	ABSOLUTE FREQUENCY
0-2	10	0.384	0.384	0.271	0.113 =x
3-5	5	0.192	0.576	0.468	0.108
6-8	2	0.076	0.652	0.612	0.04
9-11	1	0.038	0.69	0.717	0.027
12-14	1	0.038	0.72	0.794	0.074
15-17	1	0.038	0.766	0.849	0.083

$\text{Frequency(f)} = \text{Occurence(O)} \div N$

$\text{R. Frequency(RF)} = \text{Frequency(f)}_i + \text{Frequency(f)}_{i+1}$

$\text{C. Frequency(CF)} = 1 - 0.9^{\text{upperlimit+1}}$

$\text{A. Frequency(AF)} = |CF - RF|$

RESULTS VERIFIED VIA K-S TEST

$D = 1.36 \div \sqrt{N}$

$D = 1.36 \div \sqrt{26}$

$0.266 = \mathbf{x1}$

$\text{SINCE } \mathbf{x1} \text{ is } \geq \mathbf{x}$

$\therefore$ the sequence is accepted

9 COMPLEXITY ANALYSIS

This work is free from side channel attacks as a random number is used in encryption process..

10 CONCLUSION AND FUTURE WORK

The work considers exponential operations with random numbers for encryption process; the random number used in the encryption process makes the process to be free from side channel attack. The strength of the algorithm lies with strength of Discrete Logarithm problem which is a hard problem. The work can be extended to be applications in somewhat and Fully Homomorphic encryption process and can also be extended to digital signature standard.

REFERENCES

[1] Public Key Exchange using Matrices over group rings, Delaram Kahrobaei ,Charalambos Koupparis & Vlendimin Shpilrain , Lecture Notes.

[2] Krishna A.V.N, pandit,S.N.N(2004). A new Algorithm

in Network Security for data transmission ,Acharya Nagarjuna International Journal of Mathematics and Information technology . 1(2),2004,97-108.

[3] Krishna, A.V.N(2005).A simple algorithm for random number generation, Journal for Scientific & Indsutrial research,(64).

[4] Krishna A.V.N(2010), Role of statistical tests in terms of security of a new encryption algorithm, International Journal of Advancements in Technology, Vol1, No.1, 2010.

[5] Marton, K(2010), Randomness in Digital Cryptography.

[6] J. L. Massey, "Cryptography—A selective survey," Digital Communications, vol. 85, pp. 3-25, 1986

[7] O. O. Khalifa, M. R. Islam, S. Khan and M. S. Shebani, "Communications cryptography," in RF and Microwave Conference, 2004. RFM 2004. Proceedings, Selangor, 2004.

[8] A Public key cryptosystem based on Algebraic Coding theory, DSN progress report 42-44,114.