



INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

CRYPTOGRAPHIC ALGORITHM WITH MATHEMATICAL PUZZLE

SONALI KULKARNI

Department of Computer Science, Fergusson College, Pune, India

Accepted Date: 05/03/2015; Published Date: 01/05/2015

Abstract: We use different algorithm to secure our online information. From child to elder person, most of the people like computer games or solving puzzles online or from newspaper. By solving different puzzles person will get knowledge. And this paper tells you the idea that instead of using only regular cryptographic algorithm if we combine mathematical puzzle with cryptographic algorithm, we can secure our information online from the third party.

Keywords: Cryptography, Puzzle



PAPER-QR CODE

Corresponding Author: MISS. SONALI KULKARNI

Access Online On:

www.ijpret.com

How to Cite This Article:

Sonali Kulkarni, IJPRET, 2015; Volume 3 (9): 992-997

INTRODUCTION

Using cryptography we can secure our details and because of which we can protect our sensitive information from third party [1]. There are different cryptographic algorithms available from simple to hard. Difficult algorithms are harder to crack which may take few days or months to crack it. For online security of the websites, we have https in the url. In https, s stands for SSL protocol that means website is secured. Puzzle plays important role in human life since by solving puzzles help to improve human's mental ability. Some puzzle provides different levels. It may be simple, medium or difficult level puzzle. It increases person's concentration and tells you how to solve particular problem. It helps to improve creativity.

II LITERATURE REVIEW

Mathematical puzzle also introduced many years ago [2].

Cryptography concept occurred in thousands of year ago for security purpose [3]. Now a day, different algorithms are used for this purpose.

III IMPLEMENTATION

Plain Text: cryptography

Step 1: Apply Caesar Cipher (Number of characters + 1) [1] ... (1)

So in alphabet after c, d comes. So our first character becomes D. Apply this rule for remaining characters. So final word becomes **dszquphsbqiz**

Step 2: Give the numbers serially for each character in the word which is shown in TABLE I. [2]

TABLE I **character in the word with serial number**

d	s	z	q	u	p	h	s	b	q	i	z
1	2	3	4	5	6	7	8	9	10	11	12

Step 3: If the word contains number ≤ 9 then apply 3X3 matrix and if the word contains number >9 and ≤ 16 then apply 4X4 matrix. **dszquphsbqiz** word contains 12 characters and therefore we are taking 4X4 matrix which is shown in TABLE II. [2]

TABLE II. 4X4 matrix

Step 4: Write the prime numbers which are in the step 2 diagonally which is shown in TABLE III.

TABLE III. Matrix with prime numbers

2			5
	3	7	
	19	13	
17			11

If the word is of small characters then instead of prime number, fill that gap with non-prime numbers and if non-prime number is also not there then fill those gaps with dash. And write down non-prime numbers and dashes which is shown in TABLE IV.

TABLE IV. Matrix with prime and non-prime numbers

2	1	4	5
-	3	7	6
-	-	13	8
12	10	9	11

For our algorithm matrix with prime and non-prime numbers are shown in TABLE V.

TABLE V. Matrix with prime and non-prime numbers

2	1	4	5
-	3	7	6

-	-	13	8
12	10	9	11

Step 5: Write down respective character in the box along with their numbers which is shown in TABLE VI.

TABLE VI. Matrix with prime and non-prime numbers along with respective character

2 s	1d	4q	5u
-	3z	7h	6p
-	-	-	8s
12z	10q	9b	11i

So for the word dszquphsbqiz, our square becomes **zqbi---s-zhpsdqu**
so this is our **cipher text**.

Decryption:

Cipher text: zqbi---s-zhpsdqu

Step 1: Count Number of characters. If it is ≤ 9 then apply 3X3 matrix and if the word contains number >9 and ≤ 16 then apply 4X4 matrix and so on. So here draw 4X4 matrix and for finding out position of the character in the matrix, temporarily write down position. There are 12 characters in the cipher text which is shown in TABLE VII.

TABLE VII. 4X4 matrix with numbers 1 to 12

2	1	4	5
-	3	7	6
-	-	-	8
12	10	9	11

Step 2: Write down characters row wise. In the above matrix there are 4 dashes that means there is no character or corresponding number of particular character which is shown in TABLE VIII.

TABLE VIII. Row wise characters, respective numbers and dashes

2 s	1 d	4 q	5 u
	3 z	7 h	6 p
-	-	-	8 s
12 z	10 q	9 b	11 i

Step 3: Write down the characters number wise from the step 2 of decryption which is shown in TABLE IX. [2]

TABLE IX. Number wise characters from the step 2 of decryption

d	s	z	q	u	p	h	s	b	q	i	z
1	2	3	4	5	6	7	8	9	10	11	12

So we got the word i.e. **dszquphsbqiz**

Step 4: Apply **Caesar cipher** (Number of characters - 1) [1] ... (2)

So in alphabet before d, c comes. So our first character becomes c. Apply this rule for remaining characters. So final word becomes

Cryptography and this is our plain text.

IV CONCLUSION

So we got cipher text as **zqbi---s-zhpsdqu** and plain text as **cryptography**.

By using cryptographic algorithm with mathematical puzzle, we will get better security since we have to think and apply some mathematical logic.

REFERENCES

1. Sumedha Kaushik, Ankur Singhal, "Network Security Using Cryptographic Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 12, December 2012, pp.105-107.
2. Aaron F. Archer," A Modern Treatment of the 15 Puzzle", November 1999], pp.793-799.
3. Mohammed AbuTaha, Mousa Farajallah, Radwan Tahboub, Mohammad Odeh," Survey Paper: Cryptography Is The Science Of Information Security", International Journal of Computer Science and Security (IJCSS), Volume (5): Issue (3): 2011,pp. 298-309.