Stochastic Modeling and Applications
Vol.26 No. 1 (January-June, 2022)
ISSN: 0972-3641

Received: 14th December 2021 *Revised: 30th January 2022* *Selected: 03rd February 2022*

IMPLEMENTATION OF NUMBER THEORETIC FUNCTION IN DEVELOPING DATA SECURITY ALGORITHM

S. MALIK[1], S. AGARWAL[2*], A.S. UNIYAL[3]

ABSTRACT. A large number of information and data is progressively used in communication over the internet in today's world, such as online shopping, internet banking, and bill payments, etc. As a result, internet users' key concern is data security, which necessitates the development of an extremely robust and unbreakable algorithm capable of providing a high level of protection. The ideal answer for data security is to utilize cryptographic algorithms, which encrypt data in some code, send it through the communication medium, and then decrypt it to reveal the authentic data. In this paper, a number theoretic function τ(m) is used to construct a method for encrypting and decrypting ATM passwords.

1. Introduction

A number-theoretic function is one that has a domain of positive integers (*Burton 2006*). The number of divisors is a number-theoretic function denoted by τ(m). If m be a number whose prime factorization can be expressed as:

$$m = p_1^{k_1} p_2^{k_2} p_3^{k_3} \dots \dots \dots p_r^{k_r} \qquad \text{……..} \ (1)$$

Then the τ(m) can be expressed as:

$$\tau(m) = (k_1+1)(k_2+1)(k_3+1)\text{……..}(k_r+1) \qquad \text{……..} \ (2)$$

Due to the rapid development of modern information technology, more individuals, businesses, schools, and government departments are connecting to the Internet, allowing more illegal users to attack and decimate the network simultaneously by using fake sites, mail and computer viruses. The most fundamental difficulty in ensuring secure data transfer over the internet is information security. As society moves toward a digital information era, network security challenges are also becoming more essential. As more users connect to the internet, cyber-attacks becoming increasingly common. It's necessary to safeguard computer and network security, which are both essential challenges. (*Koblitz 1987*)

[*] ***Corresponding Author***

***Key words and phrases**: Cryptographic algorithms; Data security; Encryption; Decryption; Number theoretic function.*

The study of algorithms for encrypting plain text into cipher-text and decrypting cipher-text into plain text is known as cryptography. It is highly suggested in today's society to keep data safe and digital structures secure. In the digital world, there are a variety of encryption and decryption methods that are already in use.

(*Sharma et al. 2021*) created a Java programme to detect Multi-reverse primes within a given interval and discovered their distribution. In addition, employing multi-reverse primes in the RSA Technique, an algorithm for data encryption and decryption has been developed for secure communication. (*Agarwal et al. 2021*) suggested a Fibonacci primes-based data encryption and decryption technique. In comparison to existing encryption approaches, the suggested method provides a high level of security against unwanted access.

(*Bisht et al. 2019*) created a system that uses multiple factoriangular numbers to secure ATM passwords. (*Agarwal 2019*) created the non-singular prime matrix and utilised it and its inverse to develop encryption and decryption algorithms for safe communication using public key cryptography. In public key cryptography, (*Agarwal et al. 2017*) defined multi-dimensional tree and developed an encryption strategy for the security of ATM passwords using multi-dimensional tree. (*Agarwal et al. 2015*) define prime weighted graphs and presented an efficient encryption strategy for safe communication using prime weighted graphs in cryptographic systems. (*Agarwal et al. 2015*) created and utilized certain of distributions in the field of cryptography key systems.

(*Rupa et al. 2009*) proposed a new message encryption scheme using a concept called cheating text. The original message is embedded in a meaningful text called cheating text. The positions of the characters of the plain text in the cheating text are stored as real message index file (RIF). This file is encrypted and sent along with the cheating text. (*Agarwal et al. 2009*) suggested a secret key cryptosystem based on ternary codes (α, β, γ) and a binary operation (Θ) that appears to be highly difficult to crack yet has relatively easy encryption and decryption methods.

(*Lohani et al. 2009*) suggested a symmetric encryption technique in which any intruder has a limited number of exhaustible alternatives for finding the secret key, but even then it is difficult to succeed. For one such system, an observation on prospective problems in breaching the system was also made. (*Rivest et al. 1978*) described a method for obtaining digital signatures and public-key cryptosystems. An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key.

To secure ATM Password, a number-theoretic function has been employed for generating the encryption and decryption algorithm in this paper.

2. Proposed Algorithm

For the security of ATM passwords, the suggested technique generates a cryptographic algorithm for encryption and decryption using number theoretic function. Because the ATM password is encrypted in multi layers and in such a huge number, it is nearly impossible for an intruder to decrypt without knowing the encryption key (or encryption function). Due to multi-layer encryption, the provided approach improves the level of security of cryptographic algorithm.

3. Encryption Method

Let us have a four-digit ATM password **n**, which can be expressed as:

$$\mathbf{n = abcd}$$

where **d** is at ones, **c** is at tens, **b** is at hundreds and **a** is at thousands. **a, b, c** and **d** can be any number from set **{0, 1, 2, 3, 4, 5, 6, 7, 8, 9}**

Step-1: Add the digits of the number as

$$\mathbf{a + b + c + d}$$

The sum can be classified into two types such as:

- Either sum is a one-digit number.
- Or a sum is a two-digit number.

If the obtained sum is a two-digit number for example:

$$\mathbf{a + b + c + d = \alpha\beta}$$

where **β** is at ones and **α** is at tens.

Then again add the digits as:

$$\boldsymbol{\alpha + \beta}$$

If again a two-digit number is obtained, repeat the process until you get a one-digit number.

Let the obtained one-digit number can be denoted by **x**, then the number **x** can be categorized into three types:

- x = **0**
- x = **1**
- x = any element of the set **{2, 3, 4, 5, 6, 7, 8, 9}**

If the sum is **0** add **2** into it and if the sum is **1** add **1** into it.

Step-2: Obtained final number (m) in each case should be greater than or equal to **2**.

Step-3: Find the number of divisors **τ(m)** of number **m**.

Step-4: Encrypt the password **n** by the function:

$$\mathbf{f(n) = \tau(m)^{\mathit{n}}}$$

where $\boldsymbol{\tau(m)^{n}}$ is a number, denoted by **y**. Hence y is the encrypted password.

3.1 JAVA Program for Encryption

```
import java.util.Scanner;
import java.lang.Math;
public class Encryption
{
        static int getSum(int n)
        {
                int sum;
                for (sum = 0; n > 0; sum += n % 10,n /= 10);
                return sum;
        }

        static int countDigit(int n)
        {
                int count = 0;
                while (n != 0)
                {
                        n = n / 10;
                        ++count;
                }
                return count;
        }

        static int countDivisors(int n)
        {
                int cnt = 0;
                for (int i = 1; i<= Math.sqrt(n); i++)
                {
                        if (n % i == 0)
                        {
                                if (n / i == i)
                                cnt++;
                                else
                                cnt = cnt + 2;
                        }
                }
                return cnt;
        }

        public static void main(String[] args)
        {
                int number,digit, sum=0, finalSum=0;
                Scanner sc = new Scanner(System.in);
                System.out.println("Enter the number to be encrypted : ");
                number = sc.nextInt();

                sum = getSum(number);
                digit = countDigit(sum);

                if(digit!=0)
                {
                        while(digit!=1)
                        {
                                sum = getSum(sum);
                                digit = countDigit(sum);
                        }
                }

                if(sum == 0)
                {
                        sum=sum+2;
                }

                if(sum==1)
                {
                        sum=sum+1;
                }

                int numberOfDivisors = countDivisors(sum);
                Double exp = Math.pow(numberOfDivisors, number);

                System.out.println("Encrypted number = "+exp);
        }
}
```

4. Decryption Method

For decryption, to obtain the four-digit ATM password from encrypted password **y**, use the decryption function

$$\mathbf{g(y) = \log_{x} y}$$

where $\mathbf{x = \tau(m)}$ will be the decryption key and $\boldsymbol{\log_{x} y}$ a number, which can be a one-digit number, two-digit number, three-digit number, or four-digit number. If $\boldsymbol{\log_{x} y}$ is a four-digit number, it can be denoted by **abcd**. Where **d** is at ones, **c** is at tens, **b** is at hundreds and **a** is at thousands. If it is not a four-digit number, to obtain the four-digit number, put **0** on the left side of the obtained number using the following procedure:

- If the obtained one-digit number is **d**, then the four-digit number will be **000d**.
- If the obtained two-digit number is **cd**, then the four-digit number will be **00cd**.
- If the obtained three-digit number is **bcd**, then the four-digit number will be **0bcd**.

So, the original password is a four-digit number **abcd,** where a**, b, c** and **d** can be any number from set **{0, 1, 2, 3, 4, 5, 6, 7, 8, 9}**.

4.1 JAVA Program for Decryption

```
import java.util.Scanner;
import java.lang.Math;
public class Decryption
{
        public static int calculateLog(double number, int base)
        {
                int result =(int)(Math.log(number) / Math.log(base));
                return result;
        }

        public static void main(String[] args)
        {
                Double encryptedNumber;
                int publicKey, log, lengthOfString;
                Scanner sc = new Scanner(System.in);

                System.out.println("Enter the encrypted number : ");
                encryptedNumber = sc.nextDouble();

                System.out.println("Enter the private key : ");
                publicKey = sc.nextInt();
                log = calculateLog(encryptedNumber, publicKey);

                String logString = Integer.toString(log);
                lengthOfString = logString.length();
                if(lengthOfString == 1)
                {
                        String prefix = "000";
                        logString = prefix.concat(logString);
                }
                if(lengthOfString == 2)
                {
```

```
            String prefix = "00";
            logString = prefix.concat(logString);
        }

        if(lengthOfString == 3)
        {
            String prefix = "0";
            logString = prefix.concat(logString);
        }

        System.out.println("Original Pin = "+logString);
    }
}
```

5. Conclusion

The suggested encryption and decryption technique is more secure than existing algorithms since it is extremely difficult for an unauthorized person to decrypt the password into its original form without knowing the decryption key (or function).

6. Limitations

As integer variables in JAVA Language can store values within a specified range, the program for encryption & decryption is applicable only for the following values of n for different values of τ(m).

For base $\tau(m) = 2$, $0000 \leq n \leq 1022$

For base $\tau(m) = 3$, $0000 \leq n \leq 0607$

For base $\tau(m) = 4$, $0000 \leq n \leq 0510$

If any other language like Python (where large integers can be stored) is used, then the results for much larger values of n can be derived using the algorithm. Therefore the proposed method will then be applicable for the range $0000 \leq n \leq 9999$, i.e. the method is useful for the security of ATM password for any combination of digits.

References

1. Sharma, D., Agarwal, S. and Uniyal, A.S., 2021. Distribution of Multi-Reverse Primes within the Given Interval & Their Application in Asymmetric Cryptographic Algorithm. International Journal of Applied Engineering and Technology, 3(1), pp.29-33.
2. Agarwal, A., Agarwal, S. and Singh, B.K., 2021. Analysis of Fibonacci Primes & Their Application in Cryptography. Stochastic Modeling and Applications, 25(2), pp.73-82.
3. Bisht, S., Uniyal, A.S. and Agarwal, S., 2019. Security of ATM Password using Multiple Factoriangular Numbers. Proceedings of National Conference on "Paradigm Shift in Management Practices for Fostering Excellence" New Delhi Publishers, New Delhi, pp.76-79.

4. Agarwal, S., 2019. Encryption & Decryption Using Linear Algebra: Advancement in Public Key Cryptography. Indian Journal of Economics and Business, 18(1), pp.167-180.
5. Agarwal, S. and Uniyal, A.S., 2017. Enhancing the Security of ATM Password using Multi-dimensional Tree. International Journal of Mathematics Research, 9(1), pp.53-58.
6. Agarwal, S. and Uniyal, A.S., 2015. Prime Weighted Graph in Cryptographic System for Secure Communication. International Journal of Pure and Applied Mathematics, 105(3), pp.325-338.
7. Agarwal, S. and Uniyal, A.S., 2015. Multiprimes Distribution within a Given Norms. International Journal of Applied Mathematical Sciences, 8(2), pp.126-132.
8. Rupa, Ch. and Avadhani, P.S., 2009. Message Encryption Scheme Using Cheating Text. IEEE International Conference on Information Technology, pp.470-474.
9. Agarwal, S. and Uniyal, A.S., 2009. Application of Marvelous Ternary Codes in Classical Cryptosystem. Stochastic Modeling and Applications, 13(2), pp.41-49.
10. Lohani, D.K., Agarwal, S. and Uniyal, A.S., 2009. Scope of Multiple Encryption Schemes in Classical Cryptosystem using Ternary Codes. Stochastic Modeling and Applications, 13(2), pp.1-9.
11. Burton, D.M., 2006. Elementary Number Theory, Tata McGraw-Hill Publ. Comp. Ltd., New Delhi.
12. Koblitz, N., 1987. A Course in Number Theory and Cryptography, Springer-Verlag, New York.
13. Rivest, R.L., Shamir, A. and Aldeman, L., 1978. A Method for Obtaining Digital Signatures and Public key Cryptosystems. Communication of ACM, 21(2), pp.120-126.

[1]**SHIVALI MALIK**: RESEARCH SCHOLAR, DEPARTMENT OF MATHEMATICS, M.B. (GOVT.) P.G. COLLEGE, HALDWANI, INDIA

EMAIL: shivalimalik8@gmail.com

[2]**SHUBHAM AGARWAL**: ASSOCIATE PROFESSOR, DEPARTMENT OF MATHEMATICS, NEW DELHI INSTITUTE OF MANAGEMENT, NEW DELHI, INDIA

EMAIL: meshubhamagarwal@gmail.com

[3]**A.S. UNIYAL**: PROFESSOR, JOINT DIRECTOR, HIGHER EDUCATION, UTTARAKHAND, INDIA

EMAIL: asuniyal0111@gmail.com