International Journal of Mathematics Research.
ISSN 0976-5840 Volume 9, Number 1 (2017), pp. 53-58

http://www.irphouse.com

Enhancing the Security of ATM Password Using Multi-dimensional Tree

Shubham Agarwal[1] and Anand Singh Uniyal[2]
[1,2] Department of Mathematics, M.B. (Govt.) P.G. College, Haldwani (U.K.), India.

Abstract

In this paper we have defined multi-dimensional tree and proposed an encryption scheme using multi-dimensional tree in public key cryptography for security of ATM password.

Keywords: Multi-dimensional tree, Public key cryptography, Security, Encryption, Decryption.

1. INTRODUCTION

S. Y. Yan [1] defined cryptography as the "science of secret writing", i.e. the process and skill of communicating or deciphering secret messages, or ciphers. In traditional cryptography, such as was available prior to the 1970s, the encryption and decryption operations are performed with the same key, called private key. Establishing a shared key between the parties is an interesting challenge. The face of cryptography was thoroughly changed when two Stanford University researchers, W. Diffie & M. Hellman [2, 3, 4], invented an entirely new type of cryptography. In this type of cryptography the encryption and decryption could be done with a pair of different keys rather than with the same key. The decryption key would still have to be kept secret, but the encryption key could be made public without compromising the security of the decryption key. This concept was called public-key cryptography because of the fact that the encryption key could be made known to anyone. Here we have designed an encryption scheme for public-key cryptography using multi-dimensional tree for enhancing the security of ATM password.

2. MULTI-DIMENSIONAL TREE

A multi-dimensional tree with the root β is represented by,

$$\beta i_1 i_2 i_3 \ldots\ldots i_n ,$$

which means the root β has out degree i_1 with i_1^{th} branch has out degree i_2 with i_2^{th} branch has out degree i_3 and so on. Fig. 1 shows a multi-dimensional tree β_{321}.

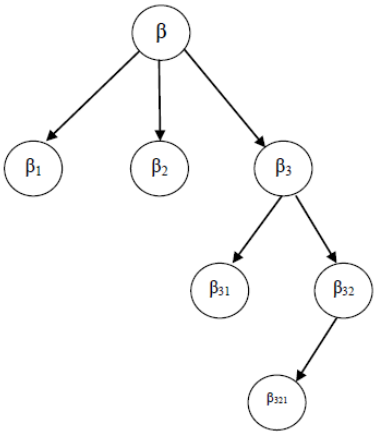

Fig. 1 A multi-dimensional tree β_{321}

3. TREE TRAVERSALS OF MULTI-DIMENSIONAL TREE

Let us consider the multi-dimensional tree β_{735} in Fig 2.

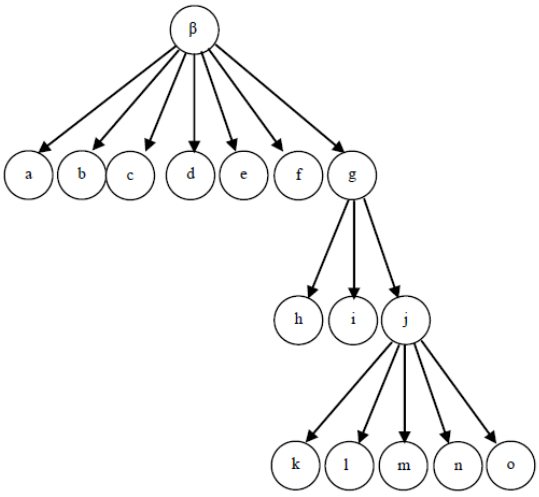

Fig. 2 A multi-dimensional tree β_{735}

Table I shows the pre-order, post-order and in-order for β_{735}.

Table I: Pre, Post and In Order for β_{735}

Pre-order	β_7	a	b	c	d	e	f	g_3	h	i	j_5	k	l	m	n	o
Post-order	k	l	m	n	o	h	i	j_5	a	b	c	d	e	f	g_3	β_7
In-order	a	b	c	d	e	f	β_7	h	i	g_3	k	l	m	n	j_5	o

4. PROPOSED METHOD

In our proposed method the password will be encrypted in the form of multi-dimensional tree, so it is very difficult for an unauthorized person to decrypt the tree in to original password even having the knowledge of encryption key.

5. APPLICATION OF MULTI-DIMENSIONAL TREE IN CRYPTOGRAPHY

Let,

$$\mathbf{p = d_3 d_2 d_1 d_0}$$

be the password where d_3, d_2, d_1 and d_0 are digits of that number. To encrypt the password, first replace every digit d_i (i = 0, 1, 2, 3) with nearest prime number p_i ($p_i > d_i$) to get new digits as,

$$\mathbf{p_3 p_2 p_1 p_0}$$

Let, the ATM password is **9231** with all non-zero digits.

Replace each digit of the password with the nearest primes to get the new digits as,

11352

The first decryption key will give the knowledge that how many of digits should be considered in each digit of encrypted password. Therefore, the first decryption key is

2111

The sequence of numbers which is to be added to get the sequence of prime numbers will work as the second decryption key,

i.e, $\mathbf{(p_3-d_3)(p_2-d_2)(p_1-d_1)(p_0-d_0).}$

Hence, the second decryption key is

2121

Draw the multi-dimensional trees $\beta p_3 p_2 p_1 p_0$ and $\beta(p_3-d_3)(p_2-d_2)(p_1-d_1)(p_0-d_0)$ for the sequence of prime numbers $p_3 p_2 p_1 p_0$ and second decryption key $(p_3-d_3)(p_2-d_2)(p_1-d_1)(p_0-d_0)$.

Fig 3 and Fig 4 represent the multi-dimensional trees β_{11352} and β_{2121}.

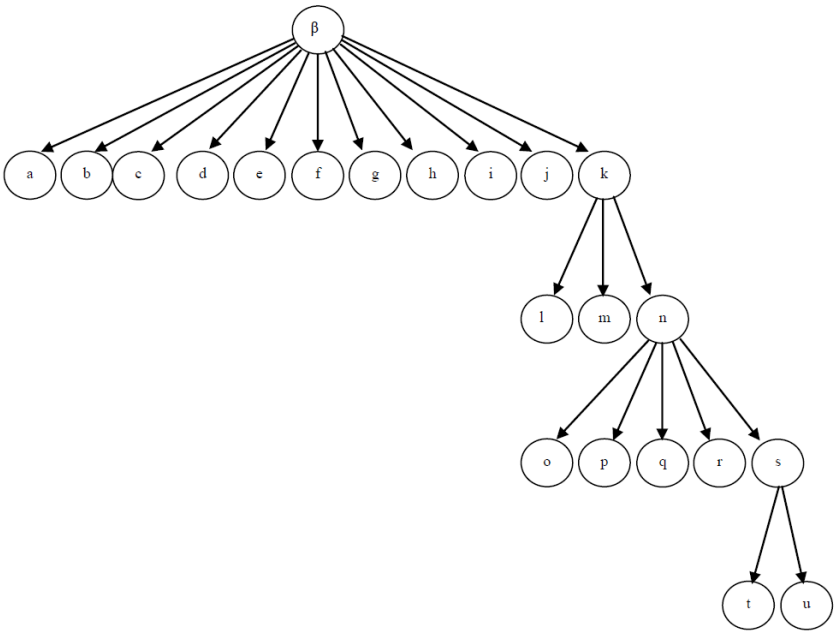

Fig. 3 Multi-dimensional tree β_{11352}

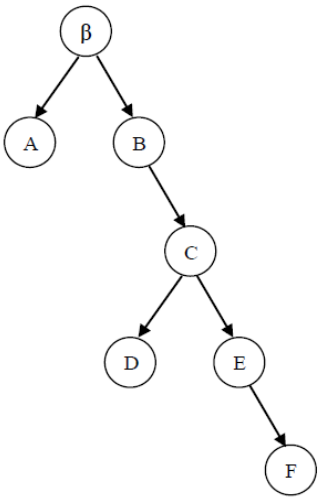

Fig. 4 Multi-dimensional tree β_{2121}

The pre-order and post-order for these multi-dimensional trees are shown in Table II and Table III respectively.

Table II: Pre and Post Order for β_{11352}

Pre-order	β_{11}	a	b	c	d	e	f	g	h	i	j	k_3	l	m	n_5	o	p	q	r	s_2	t	u
Post-order	t	u	o	p	q	r	s_2	l	m	n_5	a	b	c	d	e	f	g	h	i	j	k_3	β_{11}

Table III: Pre and Post Order for β_{2121}

Pre-order	β_2	A	B_1	C_2	D	E_1	F
Post-order	F	D	E_1	C_2	A	B_1	β_2

Send these orders of trees as encrypted password.

Now to decrypt the password into original form, first draw the multi-dimensional trees using these orders and find the position of last node of both multi-dimensional trees.

Position of node u = **11352** in β_{11352}
Position of node F = **2121** in β_{2121}

Now from the first decryption key 2111 find the sequence of prime numbers to be considered in first multi-dimensional tree β_{11352}.

Hence, the sequence of prime numbers is,

11 3 5 2.

Now subtract the corresponding digits of second decryption key obtained from the second multi-dimensional tree β_{2121}, i.e, **2 1 2 1** from the sequence of prime numbers to get the original password.

$$\begin{array}{cccc} 11 & 3 & 5 & 2 \\ -2 & -1 & -2 & -1 \\ \hline \mathbf{9} & \mathbf{2} & \mathbf{3} & \mathbf{1} \end{array}$$

Hence, the original password is **9231**.

6. CONCLUSION

It is clear that the multi-dimensional tree is useful in public key cryptography for security of ATM passwords.

REFERENCES

[1] Yan, S. Y., *Number Theory for Computing*, Second Edition, Springer-Verlag Berlin Heidelber New York (2002), ISBN 3-540-43072-5.

[2] Diffie, W. & Hellman, M., *New Directions in Cryptography*, IEEE Trans. Information Theory 22, (1976), pp 644-654.

[3] Diffie, W. & Hellman, M., *Multi-user Cryptographic Techniques*, IEEE Trans. Information Theory, November (1976).
[4] Hellman, M. E., *The Mathematics of Public Key Cryptography*, Scientific American, 241, pp 146-157, (1979).