Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 8, August 2015, pg.57 – 60

RESEARCH ARTICLE

New Approach of Encryption and Decryption Using Armstrong Numbers, Matrix Operation

* Ubhad Sanket A., Prof. Dubey Shyam P., Prof. Chaubey Nilesh

[1.] *M.Tech Scholar, Dept. of CSE, NCET, Nagpur,*
sanket.ubhad@gmail.com

[2.] *Asst. Prof. Dept. of CSE, NCET, Nagpur*
shyam.nuva@rediffmail.com

[3.] *Asst. Prof. Dept. of Electronics, MIET, Gondia,*
chaubey.nilesh@gmail.com

Abstract— ***Cryptography is only thanks to succeed information security. This is often done by changing the info into cipher text. The existing manner of doing this was victimization Armstrong range. Since there square measure few Armstrong numbers so a crypt-analyst will easily realize the key. Data Security is the science and study of methods of protecting data from unauthorized disclosure and modification as per the technology upgraded, there is need to secure data which is transmitted over the network. Unsecured networks can be hacked into easily, and hackers can do lots of things in short amounts of time. A hacker can search the hard drive of the average PC user in less than a minute. In this short time period a search can be conducted on spread sheets or databases that contain user names and passwords. This paper provides a technique to encrypt the data using a key involving Armstrong numbers. Central server system is used to provide secure intended Authentication between users. So here two way security is given to key as well as data.***

Keywords -Armstrong numbers, data security, authentication, cryptography.

I. INTRODUCTION

Security is one of the major concerns of all the users irrespective of the domain in which they work. There are various ways by which one can ensure the security for the data which is present in different files in the computer. Encryption-Decryption is one of those techniques which is quite popular. But, the complexity which is involved in this technique doesn't allow its users to apply it in a simpler way. Now, if we look into the detailed context of this technique then we may observe that there are number of ways which allows the user to encrypt the private files and information.

Now days, to make secure data transmission different methods are used. One of the techniques is Cryptography, in this encryption and decryption process is used to hide simple data from unauthorized users by converting it into unreadable form and again retrieve it in original form. Security is one of the major concerns of all the users irrespective of the domain in which they work.

II. CRYPTOGRAPHY

Cryptography, to most people, is concerned with keeping communications private. Encryption is the transformation of data into some unreadable form. The encrypted data obtained as a result of encryption process is called as cipher text. Depending on the encryption mechanism used, the same key might be used for both encryption and decryption, while for other mechanisms, the keys used for encryption and decryption might be different.

A. Types of Cryptographic Algorithms

There are several ways of classifying cryptographic algorithms. In general they are categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use as in [1]. The three types of algorithms are depicted as follows

1)*Secret Key Cryptography (SKC):*

Uses a single key for both encryption and decryption. The most common algorithms in use include Data Encryption Standard (DES), Advanced Encryption Standard (AES).

2) Public Key Cryptography (PKC): Uses one key for encryption and another for decryption. RSA (Rivest, Shamir, Adleman) algorithm is an example.

3) Hash Functions:

Uses a mathematical transformation to Irreversibly "encrypt" information. MD (Message Digest) Algorithm is an example.

III. SERVER ARCHITECTURE

Servers are often dedicated, meaning that they perform no other tasks besides their server tasks. On multiprocessing operating systems however, a single computer can execute several programs at once. A server in this case could refer to the program that is managing resources rather than the entire computer.

A. What is Server Platform?

A term often used synonymously with operating system. A platform is the underlying hardware or software for a system and is thus the engine that drives the server.

B. Types of server

1]FTP-Servers

One of the oldest of the Internet services, File Transfer Protocol makes it possible to move one or more files securely between computers while providing file security and organization as well as transfer control.

2]Mail-Servers

Almost as ubiquitous and crucial as Web servers, mail server's move and store mail over corporate networks via LANs and WANs and across the Internet.

3] Print-server

It is a computer that manages one or more printers and a network server is a computer that manages network traffic. There are so many servers according to requirement like Audio/video, Chat, Fax, News, Proxy, Web servers etc.

IV. PROPOSED SYSTEM

A. Introduction

In proposed approach we maintain server database with following fields-Unique name and id of sender and receiver, and encrypted key(Armstrong Number).

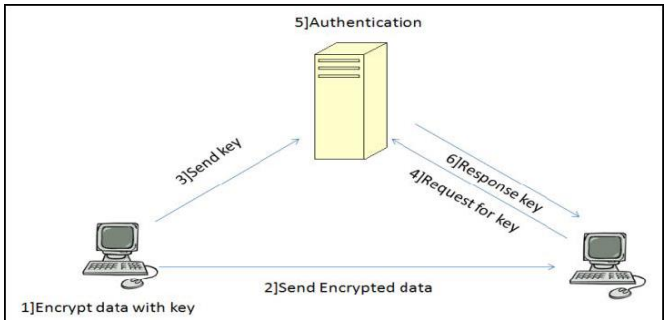


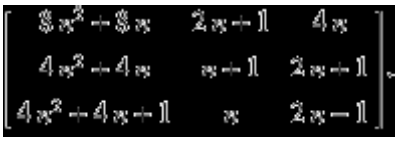
Fig 1. Server Architecture

Now, if sender „A‟ wants to send data to receiver „B‟, then he encrypts that data using randomly generated Armstrong number. That encrypted data is identified by unique timestamp given to it and sent to receiver. At the same time key (Armstrong Number) of encrypted data is sent to server with receiver ‟B‟ id and file name.

B. Illustration

1] Encryption:

Step 1: Unimodular matrix is used to create encoding matrix given below. Take random Armstrong Number and add its total digits like. (n=1+5+3=9) and substitute it in Unimodular matrix as below



After calculation Encoding matrix is

720 19 36
360 10 19
361 9 17

Step 2: (Encryption of the actual data begins here) Let the message to be transmitted be “ENCRYPT”. First find the ASCII equivalent of the above characters.

E	N	C	R	Y	P	T	Extra	Extra
69	78	67	82	89	80	84	-25 -	25

Step 3: Now add these numbers with the digits of the Armstrong number Encrypted matrix as follows:

E	N	C	R	Y	P	T	Extra	Extra
69	78	67	82	89	80	84	-25	-25
+720	19	36	360	10	19	361	9	17
789	97	103	442	99	99	445	-16	-8

Step 4: Convert the above data into a matrix as follows:

A=789 97 103
442 99 99
445 -16 -8

Step 5: Consider an encoding matrix...

B=720 19 36
360 10 19
361 9 17

Step 6: After multiplying the two matrices (B * A) we get

C= 54262 56951 48860
27256 28495 24445
27075 28534 24482

The encrypted data is...
54262, 56951, 48860, 27256, 28495, 24445, 27075,
28534, 24482

The above values represent the encrypted form of the given message. After storing this data into file it will be converted into byte array format as below:
-10, 119, -36, 120, 79, 125, -61, 118, -94.

2] Decryption:
Decryption involves the process of getting back the
original data using decryption key.
Step 1:(Decryption of the original data begins here)
The inverse of the encoding matrix is:

D = -1 1 1
43363 -43508 -43216
-21682 21755 21608

Step 2: Multiply the decoding matrix with the encrypted data
(C*D)
numbers as follows:

789	97	103	-53830	-56733	-53405	27581	28400	26872
+720	19	36	360	10	19	361	9	17
69	78	67 -	54190 -	56743	-53424	27220	28391	26855

Step 5: After converting the above data into byte array format and removing the extra parity bits we will get the original data.
69 78 67 82 89 80 84

Step 6: Obtain the characters from the above ASCII equivalent:
E N C R Y P T
69 78 67 82 89 80 84

V. CONCLUSION

Unimodular matrix is used to reduce the loss of data during encryption and decryption process. This encryption technique ensures that the data transfer can be performed with protection since it involves two main steps. First step is to convert the characters into another form that means in ASCII values, Second step by adding with the digits of the Encoding matrix to form the required encrypted data.

Tracing process becomes difficult with this technique. This is because data is encrypted by key using Armstrong number and again this Armstrong number is encrypted by using receives key. So it is more secure. In this proposed technique encryption algorithm is too difficult to trace or hack externally. Server plays vital role in authentication process.

References

[1] “Security Using Colors and Armstrong Numbers” by S. Pavithra Deepa, S. Kannimuthu, V. Keerthika 1,3UG Student, Department of IT, Sri Krishna College of Engineering and Technology.
[2] “Introduction to algorithms" by Cormen, Leiserson, Rivest and Stein, Ch 28
[3] “ALGORITHM ANALYSIS AND COMPLEXITY CLASSES” Rayward-Smith, chapter 6), (Lewis & Papadimitriou, chapter 6)
[4] Public Key Cryptography Applications Algorithms and Mathematical Explanations Anoop MS, Tata Elxsi Ltd, India
[5] Weisstein, Eric W. “Unimodular Matrix.” From MathWorld – A Wolfram Web Resource. http://mathworld.wolfram.com/UnimodularMatrix.html
[6] SP 800-44 Version 2, *Guidelines on Securing Public Web Servers.*

