www.ijrream.in Impact Factor: 2.9463

INTERNATIONAL JOURNAL OF RESEARCH REVIEW IN ENGINEERING AND MANAGEMENT (IJRREM)

A New Hybrid Technique for Data Encryption

A. Richard William, A. Karthik, Y. Sakthi Ganesh, N. Srinivas, A. Surya Prakesh

Department of Information Technology

Er. Perumal Manimekalai College of Engineering

ABSTRACT:

Development and management of good database system as well as providing security control for the database has always been a major issue in this digital age. Various encryption techniques has previously been developed to provide security to users. However, a number of these encryption algorithms are weak or have bottlenecks thereby putting the security of data stored in the database in question. In this research, we designed a new hybrid database encryption model that improves the security of the database. The new hybrid encryption algorithm combines the features of the Advanced Encryption Algorithm (AES) and the RSA algorithm for encryption of the database to provide integrity, authentication and key distribution.The results from the analysis demonstrate that proposed model offers a highly secure approach that provides users and organization with data confidentiality and integrity

Keywords: Encrytion, Decryption, AES, RSA, Fibonacci Series, PN Sequence, XOR Cipher, and Asysmmetric.

1. INTRODUCTION

Encryption is a way of scrambling data so that only authorized parties can understand the information. In technical terms, it is the process of converting plaintext to cipher text. In simpler terms, encryption takes readable data and alters it so that it appears random. In cryptography, a hybrid cryptosystem is one which combines the convenience of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem. Public-key cryptosystems are convenient in that they do not require the sender and receiver to share a common secret in order to communicate securely. There are two types of encryption in widespread use today: symmetric and asymmetric encryption. The name derives from whether or not the same key is used for encryption and decryption.

The RSA or Rivest-Shamir-Adleman encryption algorithm is one of the most powerful forms of encryption in the world. It supports incredibly key lengths, and it is typical to see 2048-

and 4096- bit keys. RSA is an asymmetric encryption algorithm. This means that there are two separate encryption keys. Encryption refers to any process that's used to make sensitive data more secure and less likely to be intercepted by those unauthorized to view it. There are several modern types of encryption used to protect sensitive electronic data, such as email messages, files, folders and entire drives.

2. EXISTING SYSTEM

Many of the existing systems are implemented using Cryptography, the use of codes and ciphers to protect secrets, began thousands of years ago. Until recent decades, it has been the story of what might be called classic cryptography — that is, of methods of encryption that use pen and paper, or perhaps simple mechanical aids. In the early 20th century, the invention of complex mechanical and electromechanical machines, such as the Enigma rotor machine, provided more sophisticated and efficient means of encryption; and the subsequent introduction of electronics and computing has allowed elaborate schemes of still greater complexity, most of which are entirely unsuited to pen and paper. However, one of the main problems with sending data over the internet is the "security threat" it poses i.e. the personal or confidential data can be stolen or hacked in many ways. Therefore it becomes very important to take data security into consideration, as it is one of the most necessary factors that need attention during the process of data transferring.

3. PROPOSED SYSTEM

Encryption is said to occur when data is passed through a series of mathematical operations that generate an alternate form of that data, the sequence of these operations is called an algorithm. To help distinguish between the two forms of data, the unencrypted data is referred to as the plain text and the encrypted data as cipher text. The security of encryption lies in the ability of an algorithm to generate cipher text that is not easily reverted to the original plaintext. As we have seen that the simple existing encryption methods are very easy to decrypt once the key or logic is known to the unauthorized person, so in order to enhance the security of the data we are

going for a combination of different encryption methods to form a hybrid technique of encryption. We have chosen the following

Simple Encryption Techniques:

1. Fibonacci Series
2. XOR Cipher
3. PN Sequence

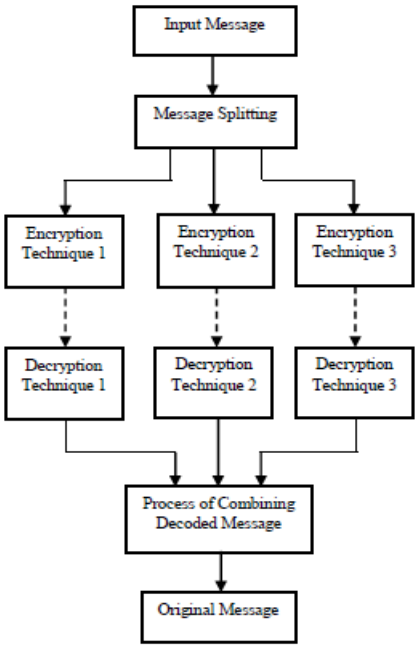

Fig. 1 Simple Encryption Techniques

4. ANALYSIS

A 21 character input message when encrypted using Fibonacci Series Method produces a 42 character encrypted data. The XOR Cipher method and PN Sequence method produce the same number of characters in the encrypted data as in the original input message. The Hybrid Technique produces 28 characters in the encrypted data which is considerably less than the Fibonacci Series Method as shown in Figure.

5. IMPLEMENTATION

It consider mainly of the following encryption techniques below flowcharts represent the working of those techniques,

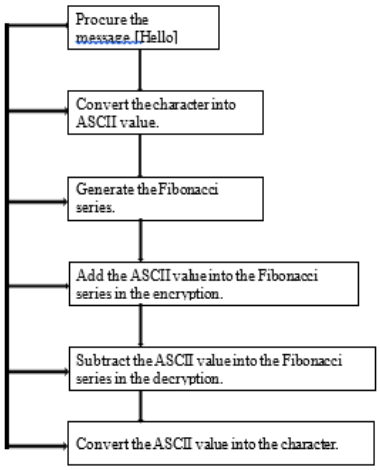

Fig. 3 Fibonacci Series

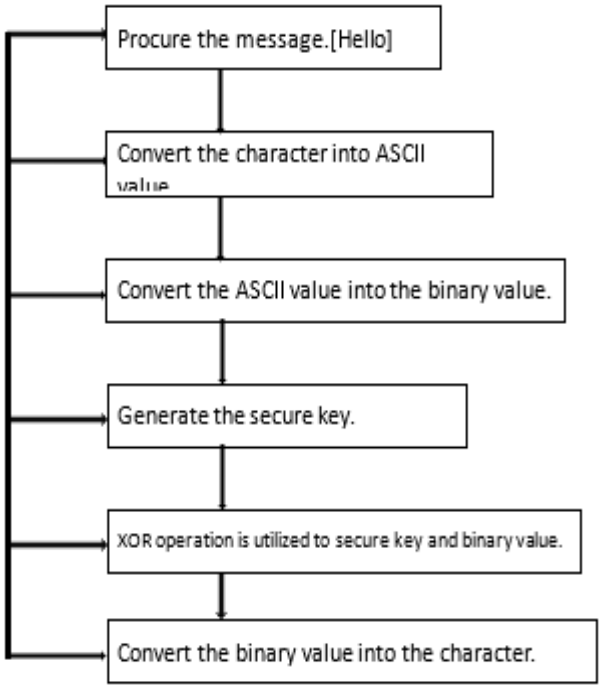

Fig. 4 XOR Cipher

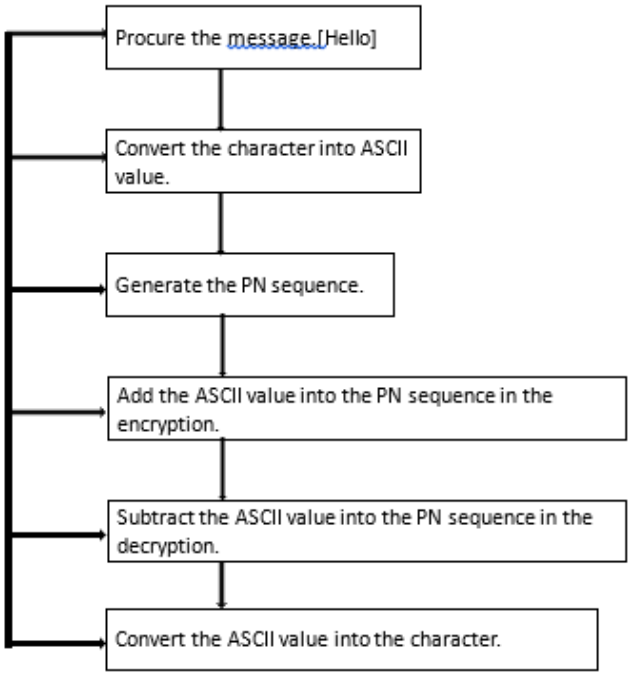

Fig. 5 PN Sequence

6. RESULT:

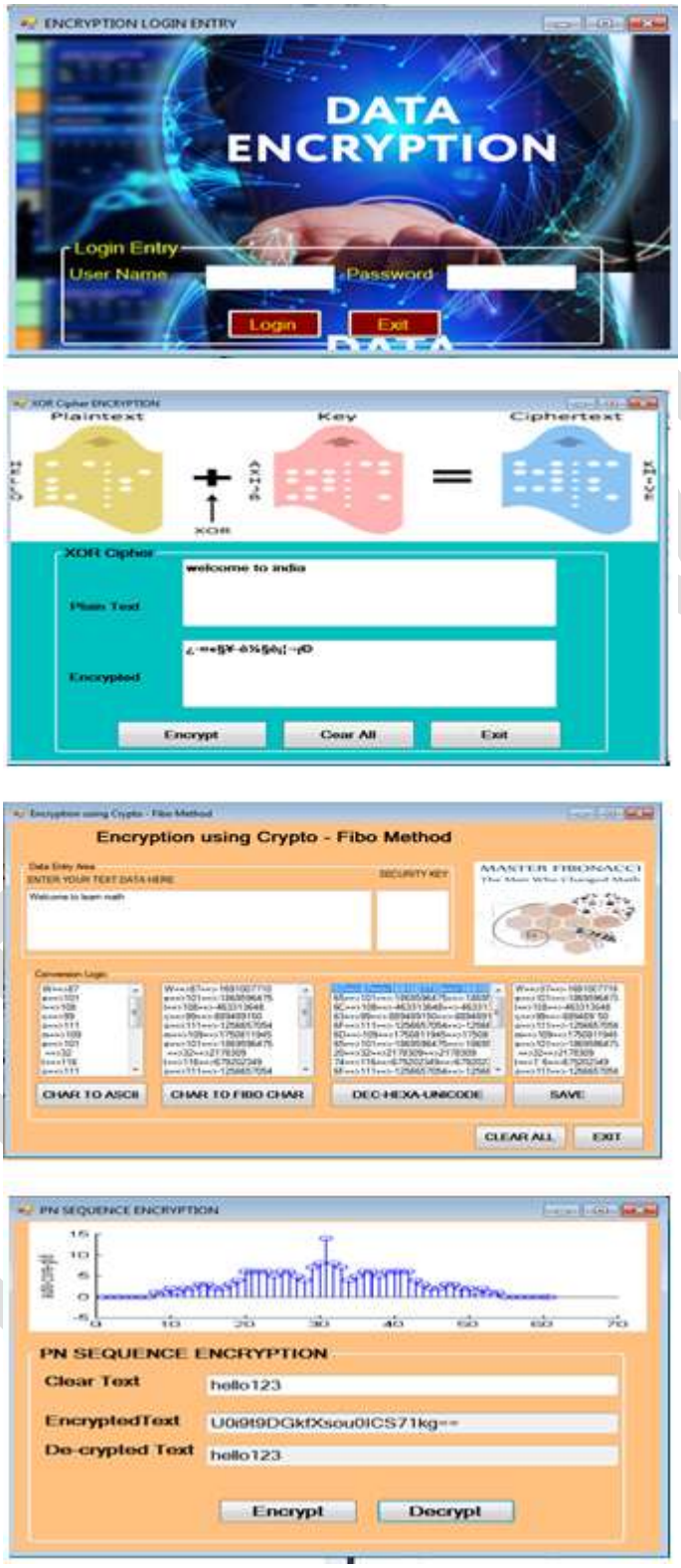

Fig. 6 XOR Encryption Page & PN Sequence & Fibonacci Crypto Method

7. CONCLUSION

Input messages of variable length were encrypted using the four techniques and the following observations were made. The Fibonacci series method leads to more number of bits during encryption than the original text. In the XOR CIPHER method, if the key is known once, the data can be easily decrypted. The PN sequence increases the storage requirement of the system and is complex. In the Hybrid Technique, the number of encrypted bits is lesser than that of Fibonacci method. The segmenting key here provides more security to the transmitted message by decrypting the original message at the receiver only when the segmenting key at both sides are equal, otherwise loss of data occurs if the message is not completely encrypted. Also the symmetric key provides authentication and validation. Also the C# code used is very simple and memory efficient. Although this method provides more safety and security, the system becomes complex due to involvement of three different types of encoders thereby increasing the cost and complexity in its hardware implementation.

References:

1. Udepal Singh and Upasna Garg, "An ASCII value based text data encryption System", in International Journal of Scientific and Research Publications, Volume 3, Issue 11, November 2013, ISSN 2250-3153.
2. Rina Choudhary, "An enhancement of code and energy optimization in PN Sequence generation", in International Journal of Engineering and Management Sciences, I.J.E.M.S., VOL.4 (4) 2013: 426-429, ISSN 2229-600X .
3. Sharad Kumar Verma and D.B. Ojha , "An application of data encryption technique using random number generator", in International Journal of Research Studies in Computing, Volume 1, Number 1, 35-42, April 2012.
4. A Joseph Raphael and V. Sundaram , "Secured Communication through Fibonacci Numbers and Unicode Symbols", in International Journal of Scientific & Engineering Research, Volume 3, Issue 4, April-2012, ISSN 2229-5518

5. Sudha Rani, T. C. Sarma and K. Satya, "Text File Encryption Using FFT Technique In Lab View 8.6", in IJRET: International Journal of Research in Engineering and Technology ISSN: 2319-1163, Volume: 01, Issue 01, Sep2012
6. D. Sravan Kumar, CH. Suneetha and A.Chandrasekhar, "A Block Cipher Using Rotation and Logical XOR Operations", in IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011, ISSN (Online): 1694-0814.
7. Himanshu Gupta and Vinod Kumar Sharma, "Role of multiple encryption in secure electronic transaction", in International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011.
8. V. Sundaram and A. Joseph Raphael, "Secured CryptoStegano Communication Through Unicode", in World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 1, No. 4,138-143, 2011.
9. Alberto Apostolico and Aviezri S. Fraenkel, "Robust Transmission of Unbounded Strings Using Fibonacci Representations", in Report Number : 85-545, 1985.