A New Encrypting Scheme for Hiding Text Messages

Mrs. Nidhi Sharma*
(Assistant Professor in TIT&S)
Bhiwani,India
nidhisharma1725@gmail.com

Mr. Alok Sharma**
(M.Tech Student,CSE Dept)
CDLU,Sirsa,India
aloksharma_tvm@rediffmail.com

Lovellin***
(B.Tech Student, TIT&S)
Bhiwani,India

Abstract - *Cryptography* is the science of using mathematics to encrypt and decrypt data. Cryptography enables to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers.

In this paper, a new message encryption scheme using a concept called Misleading Text is proposed. The original message is embedded in a meaningful text called misleading Text. The positions of the characters of plain text in the misleading text are stored as Real Message Index File (RIF). This file is encrypted and sent along with the misleading text. The receiver in turn decrypts RIF table and get back the original message from the received misleading text. Authentication is achieved by verifying the hash value of the plain text created by the Modified Message Digest Algorithm at the receiver side. So, this paper will discuss, hashing the plain text at sender's side using a Modified Message Digest algorithm and verifying that at the receivers end.

1. INTRODUCTION:

The protection of information authentication is based on cryptographically secure hash function. A function that compresses an arbitrarily large message into a fixed small size message digest' is known as a hash function.A new message encryption scheme using a concept called Misleading text is proposed. The original message is embedded in a meaningful text called misleading text.

Message encryption schemes presently being used requires that the total message is encrypted. It leads to increase in computational cost of message. The encryption scheme is based on misleading text and a Real Index File (RIF). The contents of RIF are encrypted instead of total message.

The authentication of the original message is achieved by a new hash algorithm. Misleading text is kind of meaningful text which is a metamorphosis of hidden writing. Hash function is a one way function 'H' such that a given hash value 'h', it is computationally infeasible to find 'x' such that H(x)=h.

2. MODIFIED MESSAGE DIGEST ALGORITHM

Step1. Read the Input File & take an extra digit from encryptor while encrypting.

Step2. Calculate the padding bits from the encryptor's extra digit.

Step3.Now add these padding bits to the original length of message.

Step 4.Append the length to the padded message. Now each extra bits padded bit corresponds to its different calculation & manipulations.

Step5.Now apply the corresponding calculations after converting all the length we have made after converting it to hexadecimal code.

Step6. Divide the message to 5-12 bit blocks.

Step7. Initialize 64-bit chaining variables go to Step10.

Step8. Divide 512-bit block into sixteen 32-bit blocks.

Step9. Process the block.

Step10. Convert 256-bit variable into 128-bit variable.

Step11. Convert 64-bit chaining variables to decimal value.

Step12. Pass these chaining variables to hexadecimal to Decimal Conversion method.

Step13. Multiply each value with decimal value of hexadecimal zero.

Step14. Divide first three values with 100.

Step15. Divide last value with 90.

Step16. Pass these values to decimal to hexadecimal conversion method.

Step17. Move to Step8 and get hash value. But for decryption we will send encryptor's external key into the misleading text.

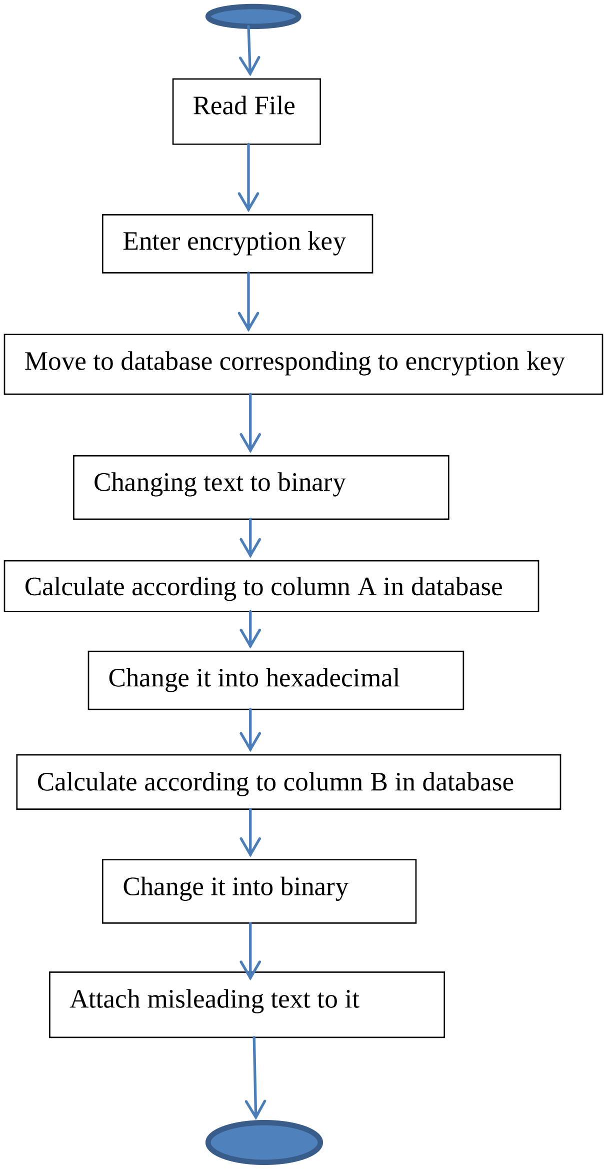
Read File
Enter encryption key
Move to database corresponding to encryption key
Changing text to binary
Calculate according to column A in database
Change it into hexadecimal
Calculate according to column B in database
Change it into binary
Attach misleading text to it

Figure1. Hash value generator

3. PROPOSED METHOD FOR DOCUMENT PROTECTION

In the proposed crypto system the message is embedded into another text called Misleading text. The position of the each character of the misleading is told in a table called character position table. Another table called RIF is generated from Cipher Plain Text for the characters of the original message. The RIF is encrypted with any public key crypto system. A hash value of the misleading text is prepared using the modified message digest algorithm. The receiver will decrypt the RIF and gets back the original message from the misleading text using RIF.

This received original message is again hashed and compared with the received hash value. If they are equal the original text is authenticated. The algorithm for encryption and decryption of the process is given below.

A. Encryption Algorithm

Step1. Enter the data you want to encrypt.

Step2. Enter the encryption key b/w 1 to 50.

Step3. Move to database corresponding to encryption key.

Step4. Change your entered data into binary.

Step5. After changing it into binary operate the calculations according to column A.

Step6. Then change it into hexadecimal and operate the operation corresponding to column B.

Step7. And change it into binary.

Step8. Send the binary code with misleading text.

Step9. Misleading will change the operation randomly those are corresponding to database.

Step10. Send this result along with misleading text to the receiver.

The original message is embedded in a meaningful misleading text. The positions of the characters of the plain text in misleading text are stored as Real Message Index File (RIF). This file is encrypted and sent along with the misleading text and hash value of original message in he zipped format.

B. Decryption Algorithm

Step1. Enter the decryption key

Step2. It will verify is the entered key is right or not.

Step3. If it is right then it will apply operation in inverse operations corresponding to the existing database.

Step4. Now it will generate the plain text again.

Step5. Now the data get decrypted result.

For Example
Entered data: Hi I am here
Entered Encryption Key: 5
Hash value generated corresponding to Encrypted key in database--
Hash: c0aart7197ecccoihuitglglthiopf7
Received data: Hi I am here
(Original message with authentication at the receiver side).

4. CONCLUSION

This paper discusses a message encryption scheme based on misleading text is proposed. The scheme is cost effective because only an index table called RIF file is hashed and sent to the receiver along with the misleading text in which the original message is embedded. The original message can be retrieved from RIF file table and the misleading text. Here authentication of the received message is also possible because of the hashing. This scheme can be applied for authentication like security in databases.

REFERENCES AND FURTHER READING

Bamford, J. *Body of Secrets : Anatomy of the Ultra-Secret National Security Agency from the Cold War Through the Dawn of a New Century.* New York: Doubleday, 2001.

_____. *The Puzzle Palace: Inside the National Security Agency, America's most secret intelligence organization.* New York: Penguin Books, 1983.

Barr, T.H. *Invitation to Cryptology.* Upper Saddle River (NJ): Prentice Hall, 2002.

Cryptography and network security by William Stallings

Computer and Network Security by Atul Kahate

Aameer Nadeem A Performance Comparison of Data Encryption Algorithm,0-7803-9421-6/2005 IEEE.

Bauer, F.L. *Decrypted Secrets: Methods and Maxims of Cryptology,* 2nd ed. New York: Springer Verlag, 2002.

Denning, D.E. *Cryptography and Data Security.* Reading (MA): Addison-Wesley, 1982.

John E Canavan, “The Fundamentals of Network security”

Diffie, W. & Landau, S. *Privacy on the Line.* Boston: MIT Press, 1998.

Electronic Frontier Foundation. *Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design*. Sebastopol (CA): O'Reilly & Associates, 1998.

C. Besnard and J. Martin, “DABO: proposed additional message authentication algorithms for ISO 8731,” preprint, 1992.

E. Biham and A. Shamir, “Differential cryptanalysis of Feal and N-hash,” Advances in Cryptology, Proc. Eurocrypt’91, LNCS 547, D.W. Davies, Ed., Springer-Verlag, 2005, pp. 1–16.