International Conference on Computational Modeling and Security (CMS 2016)

Content Based Symmetric Key Algorithm

Manish Shrivastava\textsuperscript{a*}, Shubham Jain\textsuperscript{b}, Pushkar Singh\textsuperscript{c}

\textsuperscript{abc}CSE Department, Institute of Technology, Guru Ghasidas University, Bilaspur, India

Abstract — With the growth in technology, there is always a need of good encryption method which may provide better security and authenticity with lesser computational complexities. Although there are a lot of symmetric key algorithms which are already been proposed, yet we are going to propose a content based symmetric key algorithm. This algorithm has two rounds and each round uses the ASCII code of characters, round two serves as the heart of this algorithm as XOR operation is performed here. It uses only two operation addition and XOR for encryption process and to generate two sub key, it uses two operation addition and subtraction. The goal of the algorithm is to reduce the correlation between plain text and cipher.

Keywords — Cryptography; symmetric key cryptography; cipher text; encryption; decryption; content encryption

1.Introduction

In simple way suppose that one want to send a message to a receiver, and wants to be sure that no – one else can read the massage. However, there is possibility that someone else opens the letter or hears the electronics communication. Most security problems are intentionally caused by malicious people trying to gain some benefit or harm someone. Computers are used by millions of people for many purposes Banking, Shopping, Tax returns, Protesting, Military, Student records etc. The major change which affects the security is the introduction of distributed system and the use of networks and communication facilities for carrying data between terminal user and computer and between computer and computer. Network security measures are needed to protect data during their transmission. However there is the possibility that someone else opens the document or temper the document. People can usually make difference between an original and a photocopy of a cheque. However, an electronic cheque (document) is a sequence of bits; there is no difference what so ever between the “original” and any number of copies. People can authenticate other people by recognizing their face, voices, and hand writing proof of signing is handled by signatures on latter pad, raised seals and so on. Tampering can usually be detected by handwriting...
paper and ink expert none of this option are available electronically, altering bits in a computer memory or in a signal leaves no physical trace. So we need a solution and solution is cryptography because it deals with all aspect of network security. There are two main types of cryptography

1.1. Symmetric key cryptography
Symmetric key cryptography is also known as secret key cryptography. With this type of cryptography, both the sender and the receiver know the same secret code, called the key. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key. Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers.

Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing.

A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block.

1.2. Asymmetric key cryptography
Asymmetric key cryptography, also called Public key cryptography, uses a pair of keys for encryption and decryption. With public key cryptography, keys work in pairs of matched public and private keys. The public key can be freely distributed without compromising the private key, which must be kept secret by its owner. Because these keys work only as a pair, encryption initiated with the public key can be decrypted only with the corresponding private key.

2. Proposed content-based symmetric key algorithm
As in symmetric key the secret key is used for encryption and decryption of message so confidentiality of message is highly dependent on secret key. We have proposed a content-based algorithm which convert secret key into two sub keys one sub key for first round and other sub key for second round. This algorithm encrypts the plain text two times to generate the secure cipher text using addition in first round and XOR operation in its second round of encryption

2.1 Encryption Algorithm
There are following steps which are involved in the encryption algorithm:
Step 1: Get the secret key and plain text from the user.
Step 2: XOR each letter’s ASCII code of the key with each other to generate the two digit number which will act subkey1 for first round.
Step 3: Repeat the following steps to get the encrypted text from the first round:
   a. Count the length of each word given in the plain text and find out the ASCII value of each letter in the plain text (exclude the spaces while counting the word length).
   b. Add the subkey1 generated in step 2 with the length of a word along with the ASCII value of each letter.
Step 4: To generate the subkey2 for second round subtract second digit from first digit of the subkey1.
Step 5: Repeat the following steps to get the encrypted text:
a. Count the length of each word given in the plain text and find out the ASCII value of each letter in the plain text (include the spaces while counting the word length).

b. Add the subkey2 generated in step 4 with the word length and perform XOR operation with ASCII value of each letter to generate the cipher text.

Step 6: Send the cipher text and key to the recipient.

### 2.2 Decryption Algorithm

There are following steps are involved in the decryption algorithm:

Step 1: Get the key and cipher text.

Step 2: XOR each letter’s ASCII code of the key with each other to generate the two digit number. This will be the key for second round of decryption.

Step 3: To generate the key for first round subtract second digit from first digit of key generated in step 2.

Step 4: Repeat the following steps to get the decrypted text from the first round:

a. Find out the spaces by XORing the cipher text with 32(ASCII value of space) and subtracting key from this, if this value is equal to index then its equivalent character will be space.

b. XOR the each character of cipher text by (Length of the word + key generated in step 3)

Step 5: Repeat the following steps to get the plain text:

a. Subtract each character by (Length of the corresponding word + key generated in step 2)

Step 6: Print the Plain text.

### 3. Illustration of proposed algorithm

The proposed encryption and decryption algorithms are illustrated with an example.

#### 3.1. Encryption

Suppose “Hello World 2015” is a plain text which is to be encrypted. First we can generate two sub keys and perform encryption process to get chipper text. To obtain more secrecy we encrypt it twice, in the first encryption process we encrypt the words (excluding space) and in second round we encrypt the words (excluding space) which give us strong chipper text.
### 3.2. Decryption

The process of decoding the fetched ciphered text using the decryption key is illustrated as follows:

<table>
<thead>
<tr>
<th>Index</th>
<th>Cipher Text</th>
<th>P=XOR with 32 - (key 2) [Just to find out position of space]</th>
<th>If Index=P (The character is space)</th>
<th>Length of the word</th>
<th>XOR with (Key 2 + Length)</th>
<th>Decrypted text after first round</th>
<th>Subtract (Key 1 + Length)</th>
<th>Plain Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>c</td>
<td>69</td>
<td>FALSE</td>
<td>103</td>
<td>g</td>
<td>72</td>
<td>H</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Ç</td>
<td>-94</td>
<td>FALSE</td>
<td>132</td>
<td>ä</td>
<td>101</td>
<td>e</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Å</td>
<td>-79</td>
<td>FALSE</td>
<td>139</td>
<td>i</td>
<td>108</td>
<td>l</td>
<td></td>
</tr>
</tbody>
</table>
4. Results and discussion

4.1. Plain text, key and cipher text

In these section user can input plain text and key and getting cipher text after first round.

Enter key used in encryption  spider
Enter plain text to be encrypted  Hello! World 2015
After encryption of 1st round  gäííÅ@ uiééé OMNR

Fig.1. Plain text, key and cipher text after first round of encryption

4.2. 2nd cipher text without space encryption after second round.

The encrypted text after 2nd round is: cÇÅæD$vÄøü#MOLP

Fig.2. chipper text after second round of encryption
4.3 key, Cipher text after first round of decryption

Fig.3. Key and cipher text after first round of decryption

4.4 Plain text after second round of decryption

Fig.4. Plain text after second round of decryption

5. Conclusion
Our proposed algorithm follows a simple technique to encrypt the plain text, it uses only two operation addition and XOR for encryption process and to generate two sub key its uses two operation addition and subtraction. It works very fast because having only two round. We are getting strong cipher text because we are encrypting plain text twice with different key, so it is very difficult to break it. The goal of the algorithm is to reduce the correlation between plain text and cipher and we have successfully achieved this. Here we work with string and 8bit binary data and focused on symmetric key cryptography technique. Our future work will be focused to work with Doc file, Text File.

6. References
5. https://www.princeton.edu/~achaney/tmve/wiki100k/docs/Symmetric-key_algorithm.html