Enhanced Multilingual Key Generator

Rizwan Haider, Umar Badr Shafeeque
Department of Information Technology, Azad Institute of Engg. & Technology,
Lucknow, Uttar Pradesh, India.
Email: *rizwanhaider72@gmail.com , shafeeque.umar@gmail.com*

Abstract

Cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. Many symmetric and public key algorithms are given which are hard to break in practice by any adversary. There exist theoretically secure schemes that provably cannot be broken. However, these schemes are more difficult to implement than the very best theoretically breakable but computationally secure mechanisms. Till date old code schemes are used for computation even though we have new and improved code schemes. This paper develops an enhanced version of multilingual key generator [1], which will generate our cryptographic key with the help of various new and better code schemes. We have tried to increase the computational hardness and keeping it simple. The proposed paper will try to give a better and secure method to generate cryptography key that can be used both for symmetric key and public key cryptography.

Keywords —*Multilingual, key generator, cryptographic key.*

1. Introduction

Security is an important issue in communication and storage of messages, and encryption is one the ways to ensure security.The key is the soul of any cryptographic algorithm. If the key is weak then the data encrypted using that key can be easily decoded by cryptanalyst. In this paper, we focus on key generation using multilingual to translate plain text and then to generate key using it.

2. Problem

From the early time, messages were written in the language known by both the parties, i.e., sender and receiver. Even after encrypting the message, cipher text has the characters of the same language in which the plain text was. Even the cryptographic keys were in the same language; in cases where key were word(s). In recent times, we use English language as a standard for communication. ASCII code scheme is use to represent English language symbols, Arabic numbers and some special symbols which are used frequently.ASCII code scheme based key wereused, whose symbol values, which are in binary, are used to generate final key(s) after applying some mathematical functions. Cryptanalyst or a computer program only work upon these schemes to find the key of encrypted information.

3. Proposed Solution

The proposed paper will useUnicode code scheme that has character sets of almost all languages instead of ASCII code scheme that has character set of English language only and hex decimal numbers instead of decimal numbers. In our proposed procedure, the key is will be unique and it will be depending on user's choice of languages. Keeping partial information of the key in the plain text after its translation based on user's choice.

4. Procedure

Step 1- Enter your message.

Step 2- Select at least three different languages.

Step 3- Select the sequence of languages.

Step 4- Translate each word according to sequence.

Step 4.1- If there is no translation for the word, select next language in sequence.

Step 5- Find the largest word in terms of characters ignoring whitespaces in translation.

Step 5.1- If two or more words have same length then check their languages

Step 5.2- If they are of same language then select the word alphabetically in descending order.

Step 5.3- Else select the word according to sequence of language.

Step 6- Find the value of each character in hex decimal.

Step 7- Compute Base = Sum all the values

Step 8- Compute XOR of all values in pair wise

Step 9- Power = MAX(XOR of values)

Step 10- Key=Base ^ Power

Example

Step 1- “The quick brown fox jumps over the lazy dog”

Step 2- Arabic, Telugu and Lao.

Step 3- Telugu, Lao and Arabic

Step 4- ఆ□□ أسمر గుంటనక్క □□□□ خلال ఆ كسول కుక్క[4]

Step 5- గుంటనక్క

Step 6- గ: C17,ు: C41, ం: C02,ట: C1F,న: C28,క: C15, ్: C4D, క: C15[5]

Step 7- Base = C17 + C41 + C02 + C1F + C28 + C15 + C4D + C15 = 115EE (in decimal, 71150) [6]

Step 8- C17 XOR C41 = 56(86), C41 XOR C02 = 43(67), C02 XOR C1F = 1D(29), C1F XOR C28 = 37(55), C28 XOR C15 = 3D(61), C15 XOR C4D = 58(88), C4D XOR C15 = 58(88) [6]

Step 9- Power = 58(88)

Step 10- Key = 115EE ^58 (in decimal, 71150 ^ 88 = 9.803735574534250e+426) [6]

5. Key Strength Analysis for Brute-Force Attack Only

The key generation scheme require 1536 bits (assumed) to represent i.e. is there are 2 ^ 1536 = 2.4103124269210e+462 [6] possible keys. Now assume that a hacker have a very fast computer (at 3.5 GHz) using which our decryption algorithm can be executed in 3.5 x 1 Nano second for all possible key trials. Even if he tries quarter the set of keys then also he is quite successful in decrypting. Then also, the hackers require quite much time decrypting the cipher text and to try all possible keys, which is show as below:

In one second = 3,500,000,000 possible key trials
In one minute = 2.1e+11 possible key trials
In one hour = 1.26e+13 possible key trials
In one day = 3.024e+14 possible key trials
In one year = 1.10376e+17 possible key (much less than 1/10th of the total key set) [6]

6. Conclusion

The proposed key generation procedure is the new concept in modern cryptography. In our proposal, the key strength is increased to sufficiently high level. The proposal can surely be enhanced with much more advanced concepts. In our proposed procedure, the key is will be unique and it will be depending upon user's choice of languages. This method is efficient, and it is powerful against certain attacks. The partial information contained in the plain text (now cipher text) makes the method much stronger. Small amount of diffusion is added to make it stronger, but a percentage of increase of cipher size will be there.

References

[1] Rizwan Haider, Bhavana Srivastava and Umar Badr Shafeeque, "Multilingual Key Generator", COTII-2013, ISBN: 978-81-924738-5-7, Vol. 1, 2013

[2] William Stallings, Cryptography and Network Security, fourth Edition, Pearson Education, ISBN-978-81-775-8774-6.

[3] www.unicode.org/

[4] www.translate.google.co.in

[5] http://code.cside.com/3rdpage/us/javaUnicode/converter.html

[6] Calculator in Windows® 7