Use of non English language to enhance Network Security

Rajesh Ramachandran

Senior Lecturer, Department of Computer Science,
Naipunnya Institute of Management and Information Technology, Pongam, Koratty, Thrissur, Kerala, India
Ph : 0091-9446265997(Mob), 0091-480-2730340(Off), Email: ryanrajesh@hotmail.com

Abstract

The major problem of English language we face in communication security is ***its*** *frequency analysis probability. That is probability of occurrence of some letters in English like 'e' is very large. Because of this, one can easily break the cipher text. To solve this problem, use a non English language whose frequency of occurrence of its alphabets are minimum. Such one language called "MALAYALAM", one of the very toughest languages in the world could be used for communication to enhance the network security.*

1. Introduction

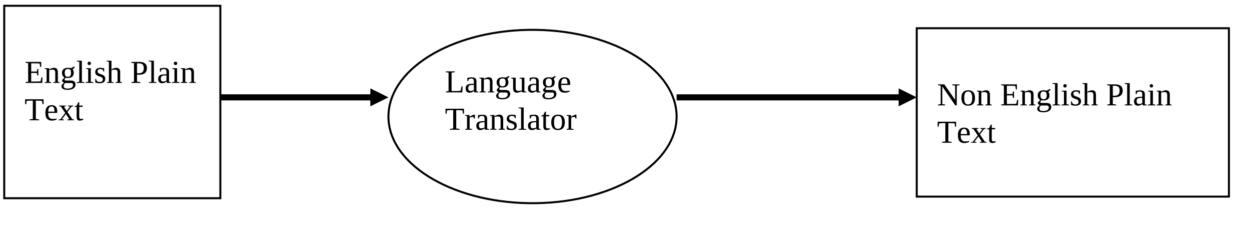
Transmission of data through unsecured medium is prone to security threats. Hackers are there to capture the data. Even though we have very good encryption algorithms still it is not possible to safeguard the data. One problem for this is the frequency analysis problem of English language. That is some characters in English language will appear more frequently than others. One solution to these problems is use of non English language. Since English is the global communication language we can not omit English as such also. A new method of communication is presented here

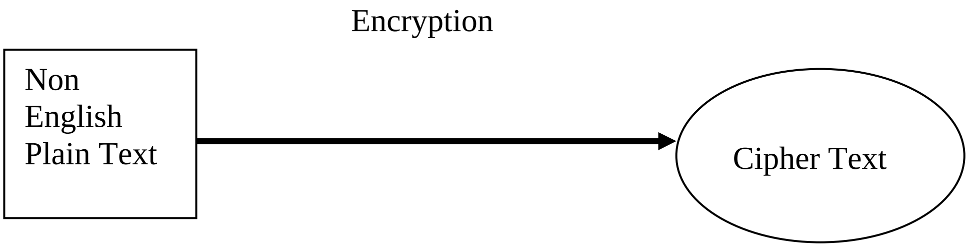
Using a language translator first convert the plain text to a non English language, for example, "MALAYALAM". Now do the encryption method to this converted data to obtain the cipher text. Send the cipher text to the destination. At the destination side, first decrypt the cipher text to get the message. Use again the language translator to convert the message from "MALAYALAM" to English.

2. Process

The process involves 3 steps. First at source side convert the English plain text to non English plain text using a translator. Next encrypt the non English plain text using standard encryption algorithm, transmit the cipher text to destination through the communication medium. And in the last step, at destination side, first decrypt the cipher text to get the non English plain text, then again using the language translator to translate the non English text to English text.

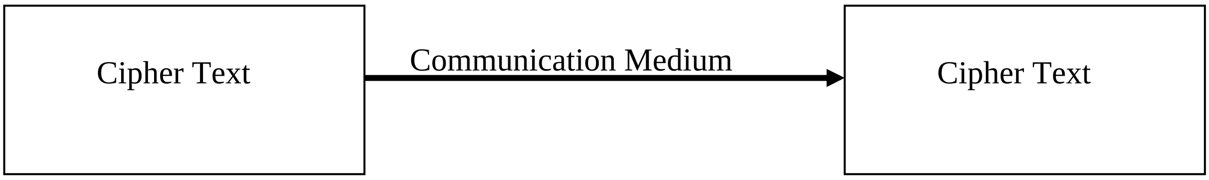
<u>a) Source side</u>



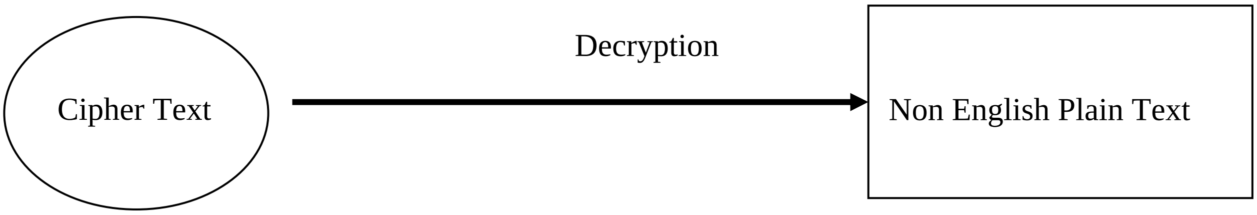


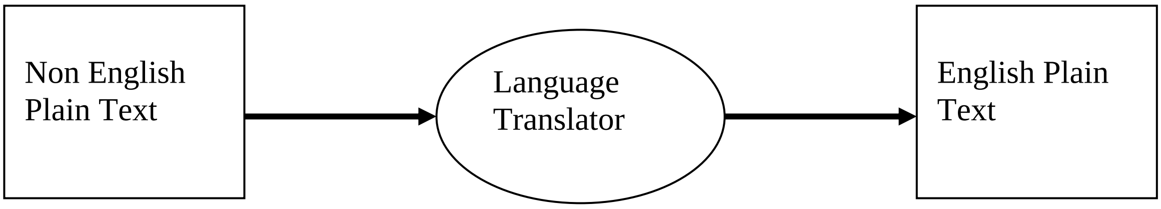
b) Transmission

Source **Destination**



c) Destination Side





Network Security

Here during the transmission if an intruder gets the cipher text, he will not be able to do the frequency analysis to get back the plain text. This is because of the property of the language selected.

MALAYALAM

We can select one non English language “MALAYALAM” for our transmission. There are 52 alphabets, including 15 vowels, are used in “MALAYALAM”. Out of 15 vowels only few are not used frequently. Similarly out of 37, only a few are not used frequently. Because of this property one can not do the frequency analysis to guess the plain text from cipher text. Moreover frequency of one letter word, two letter words, three letter words are less in “MALAYALAM”.

Issues

The one major current issue is in this technique is currently there is no translator as such to translate English and Malayalam.

Conclusion

This techniques of translation of English to other language before transmission will enhance the security of the message. But we have to make a good translator to translate English to other language.

Article received: 2009-06-09