Applied Mathematical Sciences, Vol. 8, 2014, no. 174, 8675 - 8677
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ams.2014.410873

Transcendental Numbers and Cryptography

M. K. Viswanath

Department of Mathematics
Rajalakshmi Engineering College, Thandalam
Chennai-602 105, Tamil Nadu, India

Abstract

We propose a substitution cipher using transcendental numbers which is not susceptible to the usual frequency attack.

Mathematics Subject Classification: 11T71, 14G50, 68P25, 68R01

Keywords: Algebraic number, Transcendental number, Substitution cipher, Encryption and Decryption

1 Introduction

We recall some basic facts from number theory.

Definition1.1

An algebraic number is a number x which satisfies an equation of the type $a_0x^n + a_1x^{n-1} + \cdots + a_n = 0$ where $a_0, a_1, a_2, \cdots, a_n$ not all zero are integers. A number which is not algebraic is called a transcendental number.

For example any rational number $p/q\ (q \neq 0)$ is algebraic as it satisfies the polynomial $qx - p = 0,\ q \neq 0$. The numbers $\sqrt{2}, \sqrt{3}, \sqrt{5}, \cdots$ are algebraic as they satisfy the equations $x^2 - 2 = 0,\ x^2 - 3 = 0,\ x^2 - 5 = 0, \cdots$ respectively. It is a well known result from number theory that the set of all algebraic numbers are countable. The uncountable set R of real numbers is the union of the set of all real algebraic numbers and the set of all real transcendental numbers. From the preceding result it follows that the set of all real transcendental numbers is uncountable. Therefore almost all real numbers are transcendental numbers. However

people find it difficult to give examples of transcendental numbers. Some of the well known examples of transcendental numbers are π, e, $\log_{10} 2, \cdots$. Clearly any positive integral power of a transcendental number is again a transcendental number. The Euler's constant γ is known for more than a million place of decimals, but whether γ is transcendental or not is still an open question!.

2 A substitution cipher using transcendental numbers

It is well known that the decimal expansion of any transcendental number is non-terminating. For example consider the transcendental number π. The decimal expansion of π is known for more than 1000 million places of decimals and is known as the mountain of π. We use this mountain of π in the encryption of messages. One can use any other transcendental number for which the mountain is available!

Assume that Bob is encrypting a message with the mountain of π. In this encryption, the Key α is the position of the decimal place of π which is used to begin the encryption. The number at α^{th} place, say n is used to substitute the beginning letter of the plaintext by shifting the alphabet by n units(mod 26). Afterwards the process is continued with the next integer and the next alphabet in the plaintext and so on, till the entire message is encrypted. The encrypted message also carries the time and the name of the sender in encrypted form. This encrypted and authenticated message is sent to Alice for decryption. Even after being informed that we have used a substitution cipher for encryption, Alice could not decrypt the message using the usual frequency test. So Bob sends the Key (π, α) through a secure channel to Alice for decryption which indicates that the transcendental number used is π and α is the position of the decimal expansion, where the encryption process has begun. Once the Key α is known to Alice, she can easily decrypt the message sent by Bob. Alice can reply to Bob using the key $(\pi, \alpha+\delta)$ where δ is the length of the message sent by Bob. This way they can contact each other continuously. Bob never uses the key α more than once for encryption and this Key α is not known to any outsider. Hence an Eve cannot pretend as Alice and send a message to Bob without him noticing it. This process of Encryption/Decryption can be continued for a long time as we have the mountain of π.

One can raise the level of security further by using two transcendental numbers one for encryption and the other for decryption and the key is chosen as before. This process is quite secure, simple and can be implemented easily. We believe that this can be used effectively in sending cryptotexts through mobile phones (Mobile Cryptography).

3. Illustration with small parameter

We illustrate the process with an example. Suppose the plaintext is "*I*

bought a new red shirt for Diwali", and the key is $(\pi, \alpha = 3)$. Then the Cryptotext is "*JGXWMMWFVNDAHFVPMXVLSUGQZCSR*". In this case $\alpha = 3, \delta = 28$ and $\alpha + \delta = 31$ and the encryption key of Alice is 31. Alice can choose a key for encryption with Bob's knowledge in many ways. For example Alice can choose the decimal place where the numeral one occurs again in the expansion. We also note that even if π is made public it is difficult to determine α as the probability of guessing α from the mountain of π is close to zero.

Acknowledgements. We applied the frequency attack to decipher the above message and found it quite ineffective. We tried it with several other messages and the outcome was the same. The process of breaking it with frequency attack is more complicated than one might anticipate.

The author wishes to thank his student Ranjithkumar for acting as Alice in the decryption of messages.

References

[1] Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery, An introduction to The Theory of Numbers, John Wiley and Sons, Inc., 1991.

[2] N. Koblitz, A course in Number Theory and Cryptography, Springer, 1994. http://dx.doi.org/10.1007/978-1-4419-8592-7

[3] A. J. Menezes, P.C. Oorschot Van, S.A. Vanstoon, Handbook of Applied Cryptography, CRC Press, USA, 1997.

[4] Wade Trappe, Lawrence C. Washington, Introduction to Cryptography with Coding Theory, Pearson Education Inc., 2006.

Received: October 30, 2014; Published: December 4, 2014