Encryption with Irrational Numbers

Cankeles, Cenk

Donmez, Mehmet Burak

Our purpose is to produce high security encryption algorithms by using the irregularity of decimal expansions. Different from other methods, we make use of the irregularity of irrational numbers instead of prime numbers as the key and we are able to provide a more rapid encryption without using modular arithmetic. Moreover, such irregular encryption prevents hackers from cracking the encryption without a key by matching the most commonly used numbers and letters. Thanks to irrational numbers, different groups of numbers can be assigned to the same letters, hence producing an algorithm with an infinite period. As a result, it takes a very long time to calculate a prime number as a key. It is only a matter of seconds to calculate the decimal expansion of the irrational numbers to be used in our method. Even though it takes a long time to find the key in RSA, the time required might be shortened with the developments in technology just like the case of ENIGMA. However, the infinity of irrational numbers and the fact that the key can be changed easily thanks to the ease of calculating a key and the fact that it is not possible to find which used during calculating and encryption. Keys and password at desired strength levels can be calculated by calculating the decimal expansions of irrational numbers at desired lengths and subsequently matching them with a desired number of digits and characters with the help of a matrix we have created. In order to make it difficult to crack the password, random paddings of numbers are added between every number. Then, the algorithm is reverse operated to decrypt the encrypted data. In order to constantly change the key, an infinite number of irrational numbers can be obtained even from whole numbers by using irrational functions.

Awards Won: