عنوان مقاله:

A new algorithm for prime number production: usable in Cryptographic communication systems

محل انتشار:

کنفرانس بین المللی پژوهش در مهندسی، علوم و تکنولوژی (سال: 1394)

تعداد صفحات اصل مقاله: 9

نویسندگان:

Behzad Farhadi - *Department of mathematic Engineering, PN University-Hamadan branch Hamadan, Iran*

Behnam Farhadi - *Scientific-Research Institute of Iran Sensor Network -Tehran Hamadan, Iran*

Zahra Rouzegar - *Asaloye international University Iran*

خلاصه مقاله:

Prime number besides using in military and spying issues codes can be used in commercial and internet area. Computer builders and internet service providers try to protect private information of peoples against hackers and theirs, because, today many people do their transactions by internet such as , paying bills, enrolling in classes or reserving train tickets. One of the most important systems that is used in industries is called R.S.A that is based on prime numbers. R.S.A protocol is used in most recent computers and is added to main protocols for safe internet communication.077 companies bought the license for using this protocol and half a million copy have been sold in the world. For breaking R.S.A code, we need to find 077 digits multiple of numbers. Examine numbers by factories is harder than testing them for being prime number, but these two issues are in relationship and mathematicians use one tool for solving these two problems. All of this put emphasis on finding a new way for calculating prime numbers.In this paper we introduce a new algorithm NPNG and improve it named FTF. The proposed method compared with previous known algorithms such ATKIN and Eratosthenes, and we provide simulation results by the end

کلمات کلیدی:

prime number algorithm, methods for prime number production, the sieve of Eratosthenes, the sieve of Atkins