Bul. Ştiinţ. Univ. Baia Mare, Ser. B,
Matematică-Informatică, Vol. XVIII(2002), Nr. 2, 129 - 132

A METHOD FOR INCREASING THE SPEED OF CERTAIN CSPRBG FOR ONE-TIME-PAD CIPHERS

Ileana BALAZS

Abstract. One-time-pad ciphers are very important because they are cryptographicaly secure, and are easy to implement, but the drawback is that the key should be as long as the plaintext.

Such keys are hard acquired and pseudorandom bit generators are used, but they slow down the encryption algorithm, in this article a method for increasing the encryption speed is showed.

Keywords: cipher, pseudorandom bit generator, encryption algorithm
MSC 2000: 94A60, 11K45, 65C10