BULETINUL INSTITUTULUI POLITEHNIC DIN IAŞI
Tomul LII(LVI), Fasc. 3-4, 2006
ELECTROTEHNICĂ. ENERGETICĂ. ELECTRONICĂ

IMPROVING THE ENCRYPTION ALGORITHMS

BY

LUMINIŢA SCRIPCARIU and PETRUŢ DUMA

Cryptography is essential to ensure the confidentiality of the transmitted information on different communication systems [1]. Many encryption algorithms were developed: Data Encryption System (DES), Triple DES, IDEA (International Data Encryption Algorithm), AES (Advanced Encryption System), etc. Their robustness depends on the complexity of the encoding algorithm and on the encryption key length. An arithmetic method for symbol permutation. using algebraic function defined on Galois Fields [2], is proposed to be used. The encryption key could be automatically changed using a short secret transmission key and a chaotic system [3]. These two elements reduce the redundancy of the transmitted sequence and the probability of deducing the plain-text in a very short time with a minimal computing capacity. Better performances of AES algorithm are obtained.