BULETINUL INSTITUTULUI POLITEHNIC DIN IAŞI
Publicat de
Universitatea Tehnică „Gheorghe Asachi” din Iaşi
Tomul LV (LIX), Fasc. 3, 2009
Secţia
ELECTROTEHNICĂ. ENERGETICĂ. ELECTRONICĂ

MULTIPLE DATA ENCRYPTION STANDARD ALGORITHM

BY

LUMINIŢA SCRIPCARIU, PETRUŢ DUMA
and ROXANA-MIHAELA HONCIUC

Abstract. Data Encryption Standard (DES) was the first encryption algorithm robust enough against the differential attack [1]. Soon its short encryption key of only 56 bits became vulnerable since computer technology evolves and catching the key through a brute force attack takes a convenient time. In this paper we propose to apply the DES algorithm on a Galois Field (GF) with multi-bit symbols obtaining a non-binary DES algorithm called *Multiple DES* (MDES) with a longer encryption key.

Key words: Data encryption; algorithm; encryption key; DES; Galois Field.