INTERNATIONAL STANDARD ISO/IEC 18033-3:2005
TECHNICAL CORRIGENDUM 1

Published 2006-08-15

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОМИССИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

Information technology — Security techniques — Encryption algorithms —

Part 3: Block ciphers

TECHNICAL CORRIGENDUM 1

Technologies de l'information — Techniques de sécurité — Algorithmes de chiffrement —

Partie 3: Chiffrement par blocs

RECTIFICATIF TECHNIQUE 1

Technical Corrigendum 1 to ISO/IEC 18033-3:2005 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Page 32, Subclause 5.2.2.2

Replace the second line of (2) with the following:

$R_{i-1} = \mathrm{F}(R_i, k_i) \oplus L_i$

ICS 35.040 **Ref. No. ISO/IEC 18033-3:2005/Cor.1:2006(E)**

Published in Switzerland