INTERNATIONAL STANDARD ISO/IEC 10116:2006
TECHNICAL CORRIGENDUM 1

Published 2008-03-15

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 — Modes of operation for an n-bit block cipher

TECHNICAL CORRIGENDUM 1

Technologies de l'information — Techniques de sécurité — Modes opératoires pour un chiffrement par blocs de n bits

RECTIFICATIF TECHNIQUE 1

Technical Corrigendum 1 to ISO/IEC 10116:2006 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Page 8, 8.1

Delete the phrase "and $r < qn$" from the first list item.

Page 19, B.3.2

Extend list item f) with the following:

"the initial contents (SV) of the feedback buffer will only be completely replaced when the number of block cipher operations performed is greater than or equal to r / k;"

ICS 35.040 **Ref. No. ISO/IEC 10116:2006/Cor.1:2008(E)**

Published in Switzerland