INTERNATIONAL STANDARD ISO/IEC 10118-3:2004
TECHNICAL CORRIGENDUM 1

Published 2011-12-01

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 — Hash-functions —

Part 3: Dedicated hash-functions

TECHNICAL CORRIGENDUM 1

Technologies de l'information — Techniques de sécurité — Fonctions de brouillage —

Partie 3: Fonctions de brouillage dédiées

RECTIFICATIF TECHNIQUE 1

Technical Corrigendum 1 to ISO/IEC 10118-3:2004 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

A.4.3, A.4.8, A.5.3, A.5.10, A.6.3 and A.6.10

Replace all occurrences of "Y_0, Y_1, …, Y_7" with "X_0, X_1, …, X_7".

Page 62, A.6.7

Replace

"
In this example the data-string is the 56-byte string consisting of the ASCII-coded version of

'abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq'

"

ICS 35.040 **Ref. No. ISO/IEC 10118-3:2004/Cor.1:2011(E)**

Published in Switzerland