INTERNATIONAL STANDARD ISO/IEC 10118-2:2000
TECHNICAL CORRIGENDUM 1

Published 2006-10-01

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 2: Hash-functions using an *n*-bit block cipher

TECHNICAL CORRIGENDUM 1

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

Partie 2: Fonctions de brouillage utilisant un chiffrement par blocs de n *bits*

RECTIFICATIF TECHNIQUE 1

Technical Corrigendum 1 to ISO/IEC 10118-2:2000 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Page iii, Contents

Delete the entries for Annex A, Annex B and the Bibliography.

Page iv, Foreword

Delete the last sentence.

Page 2, Subclause 6.4

Delete "(see annex A for guidance)" at the end of the first paragraph.

ICS 35.040 **Ref. No. ISO/IEC 10118-2:2000/Cor.1:2006(E)**

© ISO/IEC 2006 – All rights reserved

Published in Switzerland

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

Page 4, Subclause 7.4

Delete “(see annex A)” at the end of the first paragraph.

Pages 11–19

Delete Annex A, Annex B and the Bibliography.

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale