



INTERNATIONAL STANDARD ISO/IEC 10118-2:2010
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 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 10118-2:2010 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Page 16, B.3

Replace Padding method 1 with the following:

“

J	D_j	H^L_{j-1}	H^R_{j-1}
1	4e6f772069732074 68652074696d6520	5252525252525252	2525252525252525
2	666f7220616c6c20 0000000000000000	113fff9a8dfe98c1 6b704f1114ce1958	f3d9241c9087aba2 6ed8932aff2dfd9e

J	D_j	H^L_j	H^R_j
1		113fff9a8dfe98c1 6b704f1114ce1958	f3d9241c9087aba2 6ed8932aff2dfd9e
2		4fd1fe4b9ab6699d 22db4af462fad373	0f6990b902b8d6ed 3fc8fe860ffcf1bc

”

Replace Padding method 2 with the following:

“

j	D_j	H^L_{j-1}	H^R_{j-1}
1	4e6f772069732074 68652074696d6520	5252525252525252	2525252525252525
2	666f7220616c6c20 8000000000000000	113fff9a8dfe98c1 6b704f1114ce1958	f3d9241c9087aba2 6ed8932aff2dfd9e

j	D_j	H^L_j	H^R_j
1		113fff9a8dfe98c1 6b704f1114ce1958	f3d9241c9087aba2 6ed8932aff2dfd9e
2		4b0505561be3b0d5 27b9d7a11fb3e254	8eabdfdcc6641e6 c715d6acb73a1506

”