



INTERNATIONAL STANDARD ISO/IEC 14888-3:2006
TECHNICAL CORRIGENDUM 1

Published 2007-09-01

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 — Digital signatures with appendix —

Part 3: Discrete logarithm based mechanisms

TECHNICAL CORRIGENDUM 1

Technologies de l'information — Techniques de sécurité — Signatures numériques avec appendice —

Partie 3: Mécanismes basés sur un logarithme discret

RECTIFICATIF TECHNIQUE 1

Technical Corrigendum 1 to ISO/IEC 14888-3:2006 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

Annex F

Replace the text in F.1 *DSA mechanism* by the following text.

F.1 DSA mechanism

F.1.1 Example 1

A complete explanation of the generation of all values is given in FIPS 186-3. This example is sample value for DSA with $\alpha = 2048$ and $\beta = 224$. All hashing, including generation of domain parameters, is performed with SHA-224.

F.1.1.1 Parameters

$\alpha = 2048$

$\beta = 224$

SEED = 0C088E11 2F88B186 90421876 5614496E C2AF9770 C71D0A56 87F489B6

$F = 2$

$P =$ B4865EFC 44BFB4CB 7EE034F0 EAE8A72D 25897819 9BF9BA28 8462FD97
 19F33272 C010A11B 33BCE4E8 481B6EC7 AB1229D9 FC7BEA43 8055907F
 F1E28FAC 33716089 DCED277F 9036440A 887D4B22 CAC5BABD ECD6A1B3
 A1731594 20371025 BAAB5F18 D5FDE928 CE4F5EE4 5352785F 20057782
 2C20756E 171CBDD8 1CEB932A E0F29109 5CFFD9C2 3A07AC6B C2F5250B
 B9F8E2E6 5AF85215 6E8EEBF8 31C098FB 010057BD 425132B8 0A46BB5C
 E801E241 05058E58 091383F1 6F124894 FB6DE9CD 3BCC4C6E 64901743
 AF8F47C3 5CC2177E B15ED172 B4969174 FE3F645A 9D3BEFC6 811A9074
 BF702024 98E5E157 ECDBED3C 1FDF3C4F 00DAB43A CBA49802 79392E18
 B515851F

$Q =$ B4D0963C 40D74138 69F42710 BBEF73CB C6C1C4E6 35C6B9F3 CF7A6255

Counter = 24

$G =$ A92434D5 6752B028 CF11954E 0F3B1BED 8804EB74 8DEED793 E2932E80
 8F37C34A 15444A06 9A8B17E5 4BF7FB82 7D6FE959 428BA0CC 1F3B2B8E
 EA0A25A2 CAF73A0C 68C7DC48 093374A3 CD1F2250 8EF05038 9E8AE58C
 E6A8AD50 2510B4CA C42528B7 BCA0993C C959C630 61D7BA3A 885E9C6D
 CA6EAE44 E2D3C050 A236645F FBDE4BA6 1ECEB17B 941F85E9 C5234A28
 FAD461DE 8B55F033 DB7E0CB4 DA5E115F FFCD416D 5A8BC9CD 9DAA6816
 010841CC 9F416A6F E109A40A 823874F0 EDD92F45 738918AC 0CB925E7
 AB8E692A 9336DB36 697E6C75 5B0243CA EBB61A38 79EABAF6 AC53F166
 2740D6ED 3E3DB9BF A629390A 6A517FB0 B50D02E2 57178145 AF964626
 57ABA465

F.1.1.2 Signature key and verification key

$X =$ A279D0A3 A4243A2B 16909C9E 0BBFEC32 0589E4DF 1BDDAE72 3BA7353B

$Y =$ 31246FA1 CB8D1430 BDCDEBF0 5BB8C967 D24E6728 BA5C900C 50852741
 3AFD496A F12EA9CC D80D8916 62A7B9B3 C2023212 08943D85 5D7EA110
 B9512D1B 9E4AABAB 72B99005 25127129 EAB2CC8E 66B6E09C 49341ABF
 184B2733 9114E39E FED6B90B 8D7BA182 3E3512D3 EB82F720 76C2815D
 A642DE61 D808DCF0 22A76077 1E22AA42 26997E41 EA142BAD BFD00011
 F7D27677 08A0313E 42255286 0D184F18 C4890ED3 A6CE8134 E1647DDC
 B292B5FD 5C5ED61C 1BF9567A E1E40CC5 F85F5B7D 1A09AAA1 08CFCFE2
 469360A9 48F61B4D 1CDCA791 1BB64070 94D9A78B A34ED943 97057791