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.

ICS 35.040 **Ref. No. ISO/IEC 14888-3:2006/Cor.1:2007(E)**

© ISO/IEC 2007 – 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

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 α = 2048 and β = 224. All hashing, including generation of domain parameters, is performed with SHA-224.

F.1.1.1 Parameters

α = 2048

β = 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

© ISO/IEC 2007 – 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

DFC56691 1B4F7DD9 61A7EBB8 74923C59 2458D43D F171CB81 698AB7EE
2E9B92E6

F.1.1.3 Per message data

M = ASCII form of "abc" = 61 62 63

K = 2973C724 7F9BD6DB 3C08CD7A 1DA427DF 6780A7DD F3E09362 E8BA1293

h(M) = 23097D22 3405D822 8642A477 BDA255B3 2AADBCE4 BDA0B3F7 E36C9DA7

F.1.1.4 Signature

R = 1DFAAA6F 87DA6148 6529A2F3 4EBC7D89 3D42F405 F8DCBB33 93CC1A00

S = 4A3E6377 D09A4CD6 67BA9F9C E3982EB9 C1AA6E90 70F7C2F7 0EA23173

F.1.1.5 Verification

$\overline{R}$ = 1DFAAA6F 87DA6148 6529A2F3 4EBC7D89 3D42F405 F8DCBB33 93CC1A00

F.1.2 Example 2

This example is sample value for DSA with α = 3072 and β = 256. All hashing, including generation of domain parameters, is performed with SHA-256.

F.1.2.1 Parameters

α = 3072

β = 256

SEED = 86B076A5 2B564328 87EBD66B 344DEEAC 952019AB 578CFF92 1AD0B26B
18ACA641

F = 2

P = CA863BE0 E5BA677A AA728CB9 67128ABB 5E27D82A AEC80778 9D3058AC
D58B0D0D F38715E3 7829893E A8DF495C A49D8F96 8BB668EE 72A62482
5BE22372 7EB07949 29BF0EEC 33212014 8DBEE767 54A41AB0 465ADDE1
D9BC592F 6D8CEC13 52DA5AF3 BC6DDF25 E6898BCF 9EF65C3B 2F3BD373
8BB6FDFD 7B5E367D A4DF7067 330BF9E1 7C374D13 749C9FF3 98A3A675
1A29B589 5D9D064A D96A86D3 810CC687 8A6B2B3C 4B56302B 221E31CA
12BB2116 D8A5FC5A ABEB143B 4EF7219B E221076F 802CED8C CC7DEF9E
2DE9D3FE 7FD34969 A406A753 3BCB326B C0913E85 1E4700BA 2403FB65
F206F5F1 B20B4EAA 83CFB034 77AE57BA 88901CDC 1A523768 B7F2E133
B2E6068A AC446C48 4F96BF42 B57BA354 556F6B8E 5CCBC746 F09BD34C
E23983B8 D77EE84E F1F2CC82 E153DA85 A81B3597 10FE6828 78C848E9
1CF73E0E 98261E96 423D61A1 F3F7DDF0 931B459E A6C5E354 F3DD435B
AB8D87F7 50E52C17 26123104 A65A47E2 523033C9 BAE45CE6 B531A450
5C9FB813 11918EC8 047C285F E57BA60E 9BB92997

Q = 8F40A65D 5449388B 3D1DA48A 150D5F43 EF7E401C 27D75A2E 57BB666C
3B9F0E9B

Counter = 202

G = 5A9E3F83 5EBEBAC5 AB17959A C806C807 59160C2A 7BDA079B 269D5278
4387A1AF D753452D 0196A7D7 F20577BE D6745289 C5D21D48 66182FA5
19870E14 F677EE2E C77BD08A 8C8549AF 369F3236 86FA2068 D3E0F195

© ISO/IEC 2007 - 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

ADC515F5 E0486952 657D9678 160F7EDA 39E6C1F3 4F47C202 0D0FF9E0
B7E79E70 30535ED9 5F871D56 025DF294 3D6DFB93 7FC36154 A74CC4CE
C3D5EC08 6DF6D706 B01D0326 A3A258D1 D1E28014 09FE70CF C383A64D
20B0E348 A3A3877C 0A5711A8 8FE6072B 6F7AAB8A A5BE28FC ECB05F89
1C11AC65 1B826C1D 00FADD4B 53340DE4 6CD530BB 2E50ACB4 D99B099C
40089588 D50A467C 82C503FF 1396D540 17188B18 55683828 B9F84942
F9ADCB08 ADA2C488 AB1AB9ED C71C71C0 25EC1F52 5B6A3123 DC36A548
083FA13B 2984A717 D00F111E 57A3D657 AEAD2EAF 1490EB3F 9A860625
7A5C8C3C 8B107E70 29A2BE10 241B932A 0754EDF8 5ED22B18 093BEE10
3EBE0022 25EF90EE EFF8BD16 C4C2E83F 0DDF24F9 CDE59CCB 87A5A706
5C9ACC98 61B2E0B1 65D05887 CA636622 E39AB3CB

F.1.2.2 Signature key and verification key

X = 8232BA35 48B1C420 315EF744 6E38F46D 880584EE C9BBE913 7192DA1E
C3136DC4

Y = A447DC6B 06664F47 CE180BFD 708D49BE 60A5DEA5 E48F6486 06CCF5A0
97B60271 0B43F76C A98FC035 41BF01C1 88B4A4B4 65F88239 F8826011
8D28F144 A1866BA9 D24F67E6 12E8995C 311BAA27 B40077CF 9ACB5BF2
002CADC2 3765075F C74C320E 40E31C31 2DD83FA2 07B6F884 FD8BA2E3
DCDC6CCF 1585C2C2 E2A3E845 C658B78C D315BCBD 1E83142E 7B7A802B
9D57601B 80288FDC 70682BD2 02CC160E 4D99FC5F A47EA128 3F446BAB
CC295714 F78DB41E 4C1E0DB3 BF99ED8C 0B1AC988 D141A623 B7A90E87
B214F82B 00077E8F 3C8D56D1 824A706A 8B002BE8 ED728EA3 B1B26F62
606BE1FF 1ED2E3CD 0B6672D5 ECFCCB9F 98678828 E1336D31 A57B14EA
0072B065 A3B6137B 4E9DE572 9D2EF0EE 37F62A04 10F86F1C D4B479F4
612F037A 5F3F9BF5 B483F6AF 9F7D9899 98CCDEDA 03C12CE0 87247BBE
5BC24B5D DF64FC25 2F2DF867 D8B645C2 D68B1260 1EF97FD1 9F0C1609
60C99E15 B3518AA2 2D5FB2AB 81C372C1 EF85ACC6 F8EAD835 42ED0015
A0944350 18F9D62B D3029147 BDA66AB1 7AE71384

F.1.2.3 Per message data

M = ASCII form of "abc" = 61 62 63

K = 8232BA35 48B1C420 315EF744 6E38F46D 880584EE C9BBE913 7192DA1E
C3136DC4

$h(M)$ = BA7816BF 8F01CFEA 414140DE 5DAE2223 B00361A3 96177A9C B410FF61
F20015AD

F.1.2.4 Signature

R = 87D8F12E B3144F25 26560768 E769D58A F6A80147 2AB0190B 96DBCE0D
05B1F79D

S = 39C4AC60 3F751663 A1C06849 BAFBAF84 7D6AF1B0 0E8BDDEA E3525E69
C908F87E

F.1.2.5 Verification

$\underline{R}$ = 87D8F12E B3144F25 26560768 E769D58A F6A80147 2AB0190B 96DBCE0D
05B1F79D

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
© ISO/IEC 2007 – All rights reserved
Not for Resale