До пункту 5.3 глави 5 розділу V Вимог до форматів

криптографічних повідомлень

**ПРИКЛАДИ ОБЧИСЛЕННЯ СПІЛЬНОГО СЕКРЕТУ ZZ**

Приклад 1. Приклад обчислення спільного секрету ZZ у циклічній групі простого поля (FFC DH, ГОСТ 34.310-95, 1024 біти)

p= E4 C6 F8 34 11 B1 55 9B 99 5D 5E 15 30 84 50 98 C3 0D CB 3E 2A A1 C2 BD BE ED 4B EF 7D 92 2F DF 04 E1 A7 55 08 8F 46 39 85 19 20 51 DE 7A 06 03 0D B6 36 2F 5F C3 2A 99 88 02 96 27 66 7C BC B1 26 9A A2 11 11 56 3D A2 47 13 31 A2 88 9F 35 C7 52 CB E6 FF 02 25 61 43 DB 9A CA 45 87 C9 3E B6 F9 D0 51 78 54 7F F8 43 9C FA AB E2 37 9A 7D 9E 14 C5 EA 84 10 17 BB CA CA 9C 35 9C A6 B3 8A 6F

q= D0 BD 51 FB 45 F3 E4 A6 C8 16 97 D4 63 16 3B 03 1D F0 46 DF 19 05 4F BF D2 50 56 87 86 71 BF 91

a= BD A6 75 95 BC 18 A3 E5 27 13 A9 D4 E1 08 6E C3 E0 99 08 50 70 B0 28 57 59 57 E4 5B 28 DD 72 D8 2D 41 D2 B7 93 06 91 B5 BC 6C 79 81 86 39 6F 53 48 53 97 F0 F2 70 73 56 3A 79 56 0D 93 76 00 9C 9F 4B 63 CA 6C 9E E0 7D 12 B1 85 62 A8 CE 19 2E F9 1C 33 2F C4 1A AF 8A 59 E6 97 E8 D9 AE 0F 7E E5 07 D7 B4 3F 60 F4 A6 D0 8E 71 BE 08 8A E3 82 8B EC 91 BC 3D C6 B8 19 97 5D B3 E2 2D 98 AB A8

xa=00 93 49 C5 03 C3 09 FC 95 B0 6E 81 CB F5 0C 7E 8D 54 E4 1B 1A 3B F8 70 43 2A FC 14 A6 FA 80 A7 D5

ya=76 39 EF E2 1B 30 8D C4 6B F3 3F C6 9B AB 2F 12 EF 2E D5 18 E9 89 BB 3A D1 09 4C 9F F7 27 0C D2 C4 01 9A D8 2B 46 63 EA 77 24 E7 0F EF E2 A8 B1 B1 12 9E 2F 2A B0 A7 A5 50 B8 F1 A7 D4 06 07 E2 EE 95 52 3A F1 6C 07 DC C5 57 24 FD E7 9D EC 72 66 FD 6C DE 70 6C D4 BA C1 70 E3 C6 D8 56 01 12 E8 9F C3 2C A5 0F D2 74 1F 59 CF 41 98 CD 17 CC 88 DF 42 24 81 3A 5E E0 93 00 B8 2C 91 E2 B2 BD

xb=30 18 1A 92 B5 E0 54 42 97 E5 10 AF 20 51 FB C8 56 26 20 97 AD A7 47 5A 5B 70 15 67 5E 08 9D F9

yb=00 C0 6B DD D0 A4 0F CD 55 BA 79 54 A3 E7 9C DF F9 24 0C C0 48 B4 EA FA A5 91 AA 7E 75 6E 57 27 A1 98 4F 4D BC 01 3A C7 7A B8 16 A6 7C EA 53 75 8C 7E 2D A8 8F C1 25 30 C8 73 C6 CD F2 DD 1A FD 27 0F 14 7F 1F 49 BD 9B E7 68 04 3E B8 FC 95 A4 3A 0D 68 72 6B 8A C2 96 CD D1 05 88 89 CE 4D CA B9 BD CE 6B 3A E2 D7 96 34 FC AA 07 85 8B A4 3F 54 B4 CD E8 01 36 DD 1E 83 49 DE AE 0F 5E CE 8E DA

ZZ=BD 7F 88 9E 48 B7 D6 2A 37 1A 6C 52 B9 2F 90 24 A2 D6 B5 05 82 04 5E 31 E2 94 95 99 01 54 7D BF 6D 90 50 B0 A0 AC D0 50 FE 96 9A AE EF B8 51 85 15 4D 9E 1D F7 D7 F4 86 DB 00 13 31 86 C6 B7 F8 4D 66 93 F4 F0 83 C6 3C A7 79 B9 02 C5 B8 9D 7F 74 16 CD AF CA 69 55 55 61 C5 F4 2F 53 B4 89 B4 7A A0 F5 31 21 91 42 1F 57 01 C6 60 54 3B B7 22 2D F6 58 6A E8 61 74 75 E7 52 86 6B 84 51 5D BF

Приклад 2. Приклад обчислення спільного секрету ZZ у групі точок еліптичної кривої (ECDH), ДСТУ4145-2002 ПБ, m=163

curveOID=1.2.804.2.1.1.1.1.3.1.1.2.0

dA = 00 00 03 04 99 1F 9A C1 A8 09 4F 6F BF A0 09 25 0D 4A 80 99 32 0D 55

QAx = 30 01 C5 6A 32 99 13 07 62 6D 09 B5 FF 06 9C 6C B8 0B 79 4D 39 BD

QAy = 00 01 B9 85 8C 28 B9 BC DC A1 7B A3 5E 6D 5F 03 4B 23 AA 74 33 C7

dB = 00 01 FC 86 17 11 60 74 A8 FF 81 B4 2F 85 CA 25 16 CF 11 CE 2E 13

QBx = 00 01 F3 36 B1 E8 02 4B E4 AB E9 2D 26 CA 7F 30 22 0E 16 50 BC 1A

QBy = 00 02 F8 75 7B 1E 7E 72 E3 E5 46 B2 60 41 77 46 3D 3F C3 BE 63 C9

ZZ = 07 F8 4A DB A6 24 57 C5 DA 5D 95 94 47 C4 F6 C1 86 4C 9B 28 8E

Приклад 3. Приклад обчислення спільного секрету ZZ у групі точок еліптичної кривої (ECDH), ДСТУ4145-2002 ПБ, m=431

curveOID=1.2.804.2.1.1.1.1.3.1.1.2.9

dA = 4B 3A 17 07 F8 70 D0 C1 D4 CE 43 8E 88 AA 2B 36 15 06 91 62 86 F3 6F F3 5F 9C BE 9C 0F BD BE 1F 77 6B B5 C2 58 78 BA E1 C5 49 58 D1 B0 39 B1 2F F5 47 E0 08 63

QAx = 12 21 63 2E 63 D9 0A EB 4D B4 31 B9 9D E5 A8 7B 74 18 02 3D D7 12 B5 01 15 64 14 A0 F8 4C 07 41 B1 27 87 65 E6 3E A7 14 B3 D4 B6 8E A6 A1 04 53 08 B6 79 AD 96 69

QAy = 40 3D 64 C6 F5 15 62 B7 00 AC CD 27 AB CA 66 2F 87 97 74 4E 11 21 68 01 5E 0A 14 3A D0 29 62 7A 13 78 EB BA 93 48 70 D1 64 12 16 A4 8A 3F 10 17 FA 22 11 49 F6 83

dB = 06 FE 21 1C 55 5C B9 D3 A2 7B 7E C2 E2 FF BB 4C B1 67 EE 86 BB 7F 11 1E 7B CD 8F 65 64 E8 83 5B 09 E0 47 B9 28 6F BA 7F 83 50 78 79 BF EE 4C 33 EC BA 41 C5 DA B5

QBx = 50 B0 73 73 CF EE 5B 3F 7C 28 70 99 E3 B3 06 AE B1 69 0C 7E 66 92 6D C5 02 D1 88 D8 81 FC 17 DC 75 AF D6 CE 2B 1E 9C ED 7C 16 FF D3 29 CF 41 1A 4B 0A BC 98 53 F5

QBy = 56 9F F5 92 E5 8A 9A 4F C8 EF 7E B9 97 A1 AA AC 46 10 5D 90 32 F7 89 D7 7C 6B 3F 7C 7B AE D2 BE F4 C2 AE 10 42 E2 B2 5A 98 AD 00 74 9A 43 63 91CC 98 F2 7C 43 5A

ZZ = 4B CA 28 D6 48 A5 0D EE F8 5F 8A 34 73 5B AE 5C 1A FE A7 2D 35 15 E1 66 39 E5 F1 66 DD 0A 47 ED E3 33 EA 5A B3 41 5D BC 4F DB B7 B6 8B E2 49 FF 3C 5B 75 F8 2B 55

Приклад 4. Приклад обчислення спільного секрету ZZ у групі точок еліптичної кривої (ECDH), ДСТУ4145-2002 ОНБ, m=173

curveOID=1.2.804.2.1.1.1.1.3.1.2.2.0

dA = 02 4D D6 E9 66 40 D1 67 F3 41 6B 77 C6 21 1B 86 20 0C 10 CF A6 60

QAx = 12 BC 80 94 27 D6 11 D7 AE 2F 5A 2C EE 2C A5 8A D9 C3 CF 27 1D 9C

QAy = 15 D4 28 1B B8 12 E5 A5 C2 16 BE DB B6 70 30 3C 34 0B 0A E4 CD 7F

dB = 02 B1 63 9B 21 01 3E 34 E6 0A 3F 98 D3 04 A4 57 12 EB 10 18 EF 6B

QBx = 00 D3 C3 C6 32 76 EE 77 38 BA E5 D0 6D 01 F3 F5 2D B1 D2 F8 C3 CF

QBy = 06 CB 9C 6D BC 22 A2 D0 83 C0 A4 38 27 83 F5 29 6F D3 CF 7F 3B 14

ZZ = 1C E3 D0 85 F5 93 BF 26 64 25 35 BB 16 A7 F7 DD 53 10 46 A7 3D 2A