До пунктів 6.3, 6.4 глави 6 розділу V Вимог до форматів

криптографічних повідомлень

**ПРИКЛАДИ ОБЧИСЛЕННЯ КЛЮЧА ШИФРУВАННЯ КЛЮЧА**

**(KDF-функція)**

1. **Приклади обчислення ключа шифрування ключа в циклічній групі поля**

Приклад 1. ГОСТ 34.310-95 1024 біт, “id-gost28147-ofb” KeyWrapAlgorithm

algorithm=1.2.804.2.1.1.1.1.1.1.2

sBox=SBOX-3

keyLen=256

partyAInfo=0123456789abcdeffedcba98765432010123456789abcdeffedcba98765432010123456789abcdeffedcba98765432010123456789abcdeffedcba9876543201

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=03 84 40 38 A3 69 BA 43 15 BB 3B 64 27 15 9C CE AC 37 E7 63 07 B5 B6 F5 23 EA 01 0A 0F 7A 04 BD

yb=00 D1 1F 56 A1 40 34 9A DC 48 F0 BD C5 5B BF B6 4E BC 59 5C 62 5A AB 93 EB E6 B6 49 C4 88 B2 E3 AB 51 76 58 BC 38 E7 EC 6A 2B A3 DF 03 2B 62 64 0E C0 92 B7 1B 61 EB FD 17 A3 CD 68 75 B8 14 C9 51 B8 36 D2 0C 32 CD 7D 6E 79 54 E7 06 4A 37 8E 77 88 2C 7A 09 BE 01 27 81 8C FF 88 53 9A C9 0E D3 FD BF 3E 76 65 13 D0 EA FA AF AB 17 01 58 92 70 7C 1D D5 60 8E 63 7D 4D 8E 5A 3F 47 ED E3 FC 10

Z=27 1C 54 DE AA AD 82 99 C1 7A C2 95 DE 74 0A 04 60 57 CD D2 A8 3E A4 27 A6 D1 AF 53 CC 0C 71 E7 8E B7 7B 1F 41 D3 97 45 9F EF 39 83 C9 7E 3F 53 74 BD 2B 82 F2 B8 E6 FF 0A 08 F2 E0 1E F5 4C BB EE DE FA 7E 23 D6 A4 66 E1 DF 8E E6 D8 DB 6D C9 2F 7D 67 9A 9F 23 F5 BE 16 5A 26 D6 1D 7D B2 0C C8 8F F7 E0 C1 CA E0 E6 1C BF EE 06 AD 52 16 F8 68 AC D3 16 FF B0 30 E6 BF 49 3E F8 9D 18 DA FD

KEK=36 C0 9A A8 83 A4 B5 83 EB C8 ED 28 17 7E 6C 35 BF A7 F4 57 8A 25 8E 4E 5C AE 35 05 82 FB D2 A7

Приклад 2. ГОСТ 34.310-95 1024 біт, “id-gost28147-ofb”KeyWrapAlgorithm

algorithm=1.2.804.2.1.1.1.1.1.1.2

sBox=SBOX-4

keyLen=256

partyAInfo=

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=03 84 40 38 A3 69 BA 43 15 BB 3B 64 27 15 9C CE AC 37 E7 63 07 B5 B6 F5 23 EA 01 0A 0F 7A 04 BD

yb=00 D1 1F 56 A1 40 34 9A DC 48 F0 BD C5 5B BF B6 4E BC 59 5C 62 5A AB 93 EB E6 B6 49 C4 88 B2 E3 AB 51 76 58 BC 38 E7 EC 6A 2B A3 DF 03 2B 62 64 0E C0 92 B7 1B 61 EB FD 17 A3 CD 68 75 B8 14 C9 51 B8 36 D2 0C 32 CD 7D 6E 79 54 E7 06 4A 37 8E 77 88 2C 7A 09 BE 01 27 81 8C FF 88 53 9A C9 0E D3 FD BF 3E 76 65 13 D0 EA FA AF AB 17 01 58 92 70 7C 1D D5 60 8E 63 7D 4D 8E 5A 3F 47 ED E3 FC 10

Z=27 1C 54 DE AA AD 82 99 C1 7A C2 95 DE 74 0A 04 60 57 CD D2 A8 3E A4 27 A6 D1 AF 53 CC 0C 71 E7 8E B7 7B 1F 41 D3 97 45 9F EF 39 83 C9 7E 3F 53 74 BD 2B 82 F2 B8 E6 FF 0A 08 F2 E0 1E F5 4C BB EE DE FA 7E 23 D6 A4 66 E1 DF 8E E6 D8 DB 6D C9 2F 7D 67 9A 9F 23 F5 BE 16 5A 26 D6 1D 7D B2 0C C8 8F F7 E0 C1 CA E0 E6 1C BF EE 06 AD 52 16 F8 68 AC D3 16 FF B0 30 E6 BF 49 3E F8 9D 18 DA FD

KEK=BA 3A 06 B2 C0 03 97 B1 02 DF 67 9E 5B 0C 9E 97 57 AB 34 8C 38 50 82 E8 7D EF 86 21 A5 21 93 E3

1. **Приклади обчислення ключа шифрування ключа в групі точок еліптичної кривої**

Приклад 1. ДСТУ 4145-2002 ПБ, m=163, “id-gost28147-оfb” KeyWrapAlgorithm

sBox=SBOX-1

curveOID=1.2.804.2.1.1.1.1.3.1.1.2.0

wrapAlgorithm=1.2.804.2.1.1.1.1.1.1.2

keyLen=256

entityUInfo=0123456789abcdeffedcba98765432010123456789abcdeffedcba98765432010123456789abcdeffedcba98765432010123456789abcdeffedcba9876543201

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

QAx=00 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

KEK=9F 61 94 11 BB 8D 53 C6 9C A7 C0 03 69 10 70 EF 31 C7 B7 2B 63 68

31 10 33 AB EF B8 A0 C1 2C 9D

Приклад 2. ДСТУ 4145-2002 ПБ, m=163, “id-gost28147-сfb” KeyWrapAlgorithm

sBox=SBOX-1

curveOID=1.2.804.2.1.1.1.1.3.1.1.2.0

wrapAlgorithm=1.2.804.2.1.1.1.1.1.1.3

keyLen=256

partyAInfo=

dA=01 E7 C0 CE 88 C8 D4 44 E8 BA 58 70 90 F2 72 6D B1 BB 27 FB 58”.

QAx=06 A7 1C 9B 54 16 05 BA AD 2A 32 5A 2C 63 E3 90 F6 52 A1 B9 B4

QAy=07 6D B8 D2 1D 01 41 D0 A9 E5 E5 BA 0C 66 A4 4A 23 A5 81 17 DB

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

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

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

ZZ=05 34 19 06 74 D9 3B 3D 23 27 D6 B0 65 20 7F 9D E7 80 63 65 CC

KEK=6B CC 82 B8 F7 A8 BC 9F C8 B9 BD 4C DE 18 FC FE 99 71 17 55 D9

AC 05 42 2C 33 32 F3 E9 6D 49 B8

Приклад 3. ДСТУ 4145-2002 ОНБ, m=173, “id-gost28147-сfb” KeyWrapAlgorithm

algorithm=DSTU4145

sBox=SBOX-1

curveOID=1.2.804.2.1.1.1.1.3.1.2.2.0

wrapAlgorithm=1.2.804.2.1.1.1.1.1.1.3

keyLen=256

entityUInfo=0123456789abcdeffedcba98765432010123456789abcdeffedcba9876543201

0123456789abcdeffedcba98765432010123456789abcdeffedcba9876543201

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

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

KEK=AF 7C 82 3E 78 AE E6 40 F6 DC 50 7D 49 EE F3 EB 6C 30 79 FF 33 9D 8C 84 A3 1B 40 7D 31 9D 0C EC

Приклад 4. ДСТУ 4145-2002 ПБ, m=257, «Dstu7624Wrap»

d=FCE983D429249532809C95049FD88BFF82F0FA85B7C5F5CEAD1944466E95673F

Qx=3EAFF221E4FDF96443CFB242B47E2EFC1C8855571985EF4C4C752DE5E4830E8900

Qy=8C38A23921C0EAAE0A23DA38534AB7CCD8422633DF9DF725AE8B6F2961D5256901

ZZ=68E88CF990AC369A124C6862474F760B06122F86E88FB169DFBCAF09B49C3017

counter = 00000001

SharedInfo=305D300F060B2A862402010101010101050500A042044065DCBC1FE1E13237B24EC8B1F357D1399B2EE2FA42175FD57B030B7F9F3640B7BB2BBC4851B9D8AE6A7B4A98EC9BCEF2C58377B88007C2337EB917C220A2AC44A206040400000100

KEK=0E6302280193432F1EB9F2D16DB00183AB65FCC74B0C2D5597B30613D484A0FB