

Додаток
до Вимог до алгоритмів формування ключів
шифрування ключів та захисту особистих
ключів електронного цифрового підпису та
особистих ключів шифрування
(пункт 5 розділу II)

Формування ключа шифрування ключа на основі паролльної інформації

Приклад 1.

PBKDF = PBKDF2

PRF = HMAC_GOST34311

sBox = SBOX-1

P = "password"

S = "salt"

C = 1

dkLen = 32

DK = 39 46 85 33 E7 8B 12 34 32 0F 2B F9 76 C4 E1 4B 10 B0 2C 70 86 10 07
79 50 4C 1C 07 2F B5 D7 3E

Приклад 2.

PBKDF = PBKDF2

PRF = HMAC_GOST34311

sBox = SBOX-1

P = "password"

S = "salt"

c = 2

dkLen = 32

DK = 13 65 54 93 83 AF FF 5B 1D F2 BF C8 F5 02 70 C6 86 57 5E 4E A6 C3
F3 D1 9C C7 7C 69 49 BB BD B3

Приклад 3.

PBKDF = PBKDF2

PRF = HMAC_GOST34311

sBox = SBOX-1

P = "password"

S = "salt"

c = 4096

dkLen = 32

DK = C7 9F 38 77 CF A7 26 4A 68 F3 E8 AA 6C 1E AF C7 98 52 51 36 8B DB
54 13 67 2F BE 0A AF 99 32 72

Приклад 4.

PBKDF = PBKDF2

PRF = HMAC_GOST34311

sBox = SBOX-1

P = "password"

S = "salt"

c = 10000

dkLen = 32

DK = 50 EA 98 2B 64 1A A7 43 DF 1B AF 65 1F C1 7A A3 D6 D0 77 F7 AD
52 E4 33 F1 7F B7 FD 0C 86 3E 45

Приклад 5.

PBKDF = PBKDF2

PRF = HMAC_GOST34311

sBox = SBOX-1

P = "passwordPASSWORDpassword"

S = "saltSALTsaltSALTsaltSALTsaltSALTsalt"

c = 4096

dkLen = 32

DK = B0 62 4C FD BE A4 89 0E 16 3E CC 24 98 81 65 42 4C B3 8F 9C F2 F3
E6 B9 B7 1E D3 47 34 8E 29 8A

Приклад 6.

PBKDF = PBKDF2

PRF = HMAC_GOST34311

sBox = SBOX-1

P = "pass\0word"

S = "sa\0lt"

c = 4096

dkLen = 32

DK = 8B 3E 73 F8 88 1C 02 9D 93 6B 68 1B 85 C2 76 3B 2F BF 30 58 56 B1
B9 7C 6D 6D 78 C9 BF A7 70 34