Załącznik

DANE TESTOWE dla algorytmu Hierocrypt –3

(wersja 128 bitów podklucz, 128 bitów blok danych)

key: 4703c87e817842c4ce6b167d43701b76
plaintext: 85693846db4c1b3487272e555761c7f5
ciphertext: 5c5f4b00aec36d893cf1041e7fa8bae8

extended keys:
K1-0: 46053dc5 e5b67ff9 a613939b bfd6885f
K1-1: a4737e7f 700e4a19 bda3284c 23478c93
K2-0: 6a553c23 72ee45b6 9b7672f0 7ae488c7
K2-1: 8f4cf0ec 4a78560c 32a28c81 28afce46
K3-0: 6bf075b3 514e2174 d51e0ff1 c7138a29
K3-1: 060558c2 de4bce44 41a52c97 185dd57f
K4-0: 181e7f2a 17248ca1 ac32a5b8 82a05cce
K4-1: 14088d78 495ff4c1 0db3bbc2 7ddb1ca2
K5-0: b42cda92 9584d06f a150143a 7c928d7a
K5-1: 40e317d0 dc620eed 5958216a e8e6e68e
K6-0: beee7a42 965dab5d 39cfca6a 84648046
K6-1: 69ce27f9 6ddb6d2e 2e6e53ac abcd7615
K7-0: f1234ed3 080acd71 f98bac4c 48b925f5

r state: hexdata hexdata hexdata hexdata
---
1 in: 85693846 db4c1b34 87272e55 5761c7f5
1 k1: 46053dc5 e5b67ff9 a613939b bfd6885f
1 s1in: c36c0583 3efa64cd 2134bdce e8b74faa
1 s1out: 10ca8ec5 f9b496cf 9b29a635 242b1eee
1 MDS_L out: 24f3f35e d0ce9611 c03fecfa e2b7fc1e
1 k2: a4737e7f 700e4a19 bda3284c 23478c93
1 s2in: 80808d21 a0c0dc08 7d9cc4b6 c1f0708d
1 s2out: 0606589b 52adcdbc b0e7eb26 68ead658
2 in: bc007e83 dda34136 f02f5a1f 39594f0c
2 k1: 6a553c23 72ee45b6 9b7672f0 7ae488c7
2 s1in: d65542a0 af4d0480 6b5928ef 43bdc7cb
2 s1out: da094452 5b859806 b681b92a d7a6f214
2 MDS_L out: e4e2e91a 1e7ed2a4 25e7e72f a7535e5a
2 k2: 8f4cf0ec 4a78560c 32a28c81 28afce46
2 s2in: 6bae19f6 540684a8 17456bae 8ffc901c
2 s2out: b6f47a04 7c841b59 e80db6f4 0a162cb2
3 in: 383ce243 ab0a4c3a 84411d72 ec44f060
3 k1: 6bf075b3 514e2174 d51e0ff1 c7138a29
3 s1in: 53cc97f0 fa446d4e 515f1283 2b577a49
3 s1out: 9a6eb8ea b411faec 9f0f78c5 f7b17d01
3 MDS_L out: e4fe07b0 cf1ac1c2 68cd102b a0e6686c
3 k2: 060558c2 de4bce44 41a52c97 185dd57f
3 s2in: e2fb5f72 11510f86 29683cbc b8bbbd13
3 s2out: 254f0fcc 609f804b 2d9995fe 00ffa642
4 in: 9b2821b6 4c2b8670 8cc61a8f e79663ff
4 k1: 181e7f2a 17248ca1 ac32a5b8 82a05cce
4 s1in: 83365e9c 5b0f0ad1 20f4bf37 65363f31
4 s1out: c5de51e7 0880ced2 0ba50527 13ded85a
4 MDS_L out: 2f16be35 0b08d761 68679ace 0ad5ea11
4 k2: 14088d78 495ff4c1 0db3bbc2 7ddb1ca2
4 s2in: 3b1e334d 425723a0 65d4210c 770ef6b3
4 s2out: a819c985 44b1d352 13939b02 655d04f3

5 in: bb22b0cb 294cbe6b a9015b78 bed3a9be
5 k1: b42cda92 9584d06f a150143a 7c928d7a
5 s1in: 0f0e6a59 bcc86e04 08514f42 c24124c4
5 s1out: 805d5e81 fe469e98 bc9f1e44 a18bc3eb
5 MDS_L out: b2755333 a5d3b98c c892b3f8 5fcb5a69
5 k2: 40e317d0 dc620eed 5958216a e8e6e68e
5 s2in: f29644e3 79b1b761 91ca9292 b72dbce7
5 s2out: dd201176 39d42b7f 736cd1d1 2ba7fe3a
6 in: 58b4f12d 9c69272f 4514722a 94972717
6 k1: beee7a42 965dab5d 39cfca6a 84648046
6 s1in: e65a8b6f 0a348c72 7cdbb840 10f3a751
6 s1out: 2882c4df ce29efcc d5400021 1cc2be9f
6 MDS_L out: a99a98da d0e892bd ad77680c fb8927e2
6 k2: 69ce27f9 6ddb6d2e 2e6e53ac abcd7615
6 s2in: c054bf23 bd33ff93 83193ba0 504451f7
6 s2out: ad7c05d3 a6c9a0f8 c57aa852 37119f1d
Last K: f1234ed3 080acd71 f98bac4c 48b925f5
out: 5c5f4b00 aec36d89 3cf1041e 7fa8bae8

==========