Załącznik nr 3.

DANE TESTOWE dla algorytmu CAMELLIA

(wersja 128 bitów podklucz, 128 bitów blok danych)

plaintext = 0123456789abcdeffedcba9876543210
key = 0123456789abcdef fedcba9876543210
ciphertext = 6767313854966973 0857065648eabe43

Key Schedule
Ffunc X=0123456789abcdef K=a09e667f3bcc908b Y=828787cc9eba002a
Ffunc X=7c5b3d54e8ee323a K=b67ae8584caa73b2 Y=3e0a9979813dfcd2
Ffunc X=3e0a9979813dfcd2 K=c6ef372fe94f82be Y=9415c76b0b42927c
Ffunc X=169240a795f89256 K=54ff53a5f1d36f1c Y=907b5aacda9b43cf
Encryption
Ffunc X=0000000000000000 K=ae71c3d55ba6bf1d Y=77933e474a99fa36
Ffunc X=77933e474a99fa36 K=169240a795f89256 Y=d5bd24691d280080
Ffunc X=d5bd24691d280080 K=a2b3c4d5e6f7ff6e Y=b2429066dee25493
Ffunc X=c5d1ae21947baea5 K=5d4c3b2a19080091 Y=4f6c7c916fb82d9e
Ffunc X=9ad158f872902d1e K=e1eaadd35f8e8b49 Y=c74c264cf87655ad
Ffunc X=029d886d6c0dfb08 K=2053cafc492b5738 Y=f38f754458e23ccf
FL X=695e2dbc2a7211d1 K=56e9afc745a49029 Y=86b8f745aae24ad9
FLinv X=029d886d6c0dfb08 K=e57e2495ab9c70f5 Y=ed007390a60dba29
Ffunc X=86b8f745aae24ad9 K=79bdffdb97530eca Y=b0ed505fda57d6fd
Ffunc X=5ded23cf7c5a6cd4 K=8642002468acf135 Y=4f666c45f7595105
Ffunc X=c9de9b005dbb1bdc K=d7e3a2d24814f2bf Y=224d9c4f4415e8f1
Ffunc X=7fa0bf80384f8425 K=00123456789abcde Y=cc83ebcec86675e5
Ffunc X=055d70ce95dd6e39 K=d169240a795f8925 Y=b22b639b588d74cd
Ffunc X=cd8bdc1b60c2f0e8 K=6ae71c3d55ba6bf1 Y=16d8f303b4ef9662
FL X=138583cd2132f85b K=97530eca86420024 Y=94f77e220730fdcb
FLinv X=cd8bdc1b60c2f0e8 K=68acf13579bdffdb Y=b47423e0208ab2a8
Ffunc X=94f77e220730fdcb K=1d950c840048d159 Y=7238119650358f5e
Ffunc X=c64c327670bf3df6 K=e26af37bffb72ea6 Y=3d68f605f0e7fbfb
Ffunc X=a99f8827f7d70630 K=e57e2495ab9c70f5 Y=6714ed54bc310864
Ffunc X=a158df22cc8e3592 K=56e9afc745a49029 Y=0d9d1a06f3955a8f
Ffunc X=a402922104425cbf K=19080091a2b3c4d5 Y=8f14b92279f2f132
Ffunc X=2e4c6600b57cc4a0 K=e6f7ff6e5d4c3b2a Y=f3db1f3e6cfb2800

CT = 6767313854966973 0857065648eabe43