Specifications

CLEFIA test vector generator specifications

Version 1.0.0 (January 29, 2010)

Sony Corporation

Change History

Version	Date	Description
1.0.0	January 29, 2010	Created

Contents

1. CLEFIA test vector generator usage

The CLEFIA test vector generator is used as follows.

1. Compile the reference code (clefia_ref.c) with the test vector generator (clefia_test.c).
2. Execute the executable file generated in Step 1.
3. Obtain the following test vectors via the standard I/O.

・1-block sample vector

plaintext = 0x000102030405060708090a0b0c0d0e0f

128-bit secret key = ffeeddccbbaa99887766554433221100
192-bit secret key = ffeeddccbbaa9988776655443322110f0e0d0c0b0a09080
256-bit secret key = ffeeddccbbaa9988776655443322110f0e0d0c0b0a090807060504030201000

・128-block OFB mode outputs using 10 different keys

IV = 0x000...0

These vectors correspond to results of 128-block data encrypted with 10 different keys

・Variable Text Known Answer Test (VarTxtKAT)

plaintexts = 0x800..., 0xc00..., 0xe00..., ..., 0xfff...

secret key (128/192/256-bit) = 0x000...0

・Variable Key Known Answer Test (VarKeyKAT)

plaintexts = 0x000...0

secret key (128/192/256-bit) = 0x800..., 0xc00..., 0xe00..., ..., 0xfff...

・ECB-mode Monte Carlo Test (ECB-MCT)

・CBC-mode Monte Carlo Test (CBC-MCT)

* These results are described in clefia_katmct.dat.