Specifications

CLEFIA テストベクトル 生成ソースコード仕様書

Version 1.0.0 (2010年1月29日)

ソニー株式会社

変更履歴

バージョン	日付	説明
1.0.0	2010年1月29日	初版作成

目次

1. CLEFIA テストベクトル生成ソースコード使用法

CLEFIA テストベクトル生成ソースコードの使用法は以下の通り.

1. CLEFIA 参照コード (clefia_ref.c) と CLEFIA テストコード (clefia_test.c) をともにコンパイルする (CLEFIA 参照コード用ヘッダファイル (clefia_ref.h) をコンパイル時に参照)
2. Step 1 で生成された実行コードを実行
3. 以下のテストベクトルが標準出力に出力される

・1-block sample vector

以下の平文，鍵による 1-block 暗号化結果

平文 = 0x000102030405060708090a0b0c0d0e0f

秘密鍵(128-bit) = ffeeddccbbaa99887766554433221100
秘密鍵(192-bit) = ffeeddccbbaa99887766554433221100f0e0d0c0b0a09080
秘密鍵(256-bit) = ffeeddccbbaa99887766554433221100f0e0d0c0b0a090807060504030201000

・128-block OFB mode outputs using 10 different keys

OFB mode (IV は全て 0) を異なる 10 種の秘密鍵で 128-block (128 回) 実行した際の出力結果

これらのベクタは，10 例の鍵に対する 128 ブロックの処理例に対応する

・Variable Text Known Answer Test (VarTxtKAT)

秘密鍵を全て 0 とし，平文を 0x800..., 0xc00..., 0xe00..., ..., 0xfff... としたときの各暗号文

・Variable Key Known Answer Test (VarKeyKAT)

平文を全て 0 とし，秘密鍵を 0x800..., 0xc00..., 0xe00..., ..., 0xfff... としたときの各暗号文

・ECB-mode Monte Carlo Test (ECB-MCT)

・CBC-mode Monte Carlo Test (CBC-MCT)

※これらの出力結果は，ファイル clefia_katmct.dat に記録されている.