INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

暗号モジュール試験及び認証制度(JCMVP)

暗号アルゴリズム確認対象
非承認セキュリティ機能
に関する仕様

LSF-01

Limited Security Functions

平成 26 年 4 月 1 日

独立行政法人　情報処理推進機構

目次

暗号アルゴリズム確認対象非承認セキュリティ機能に関する仕様

平成 26 年 4 月 1 日

1. 目的

本規程は、独立行政法人 情報処理推進機構 (以下｢機構｣という。) が、｢暗号モジュール試験及び認証制度の基本規程」 (JCM-01) (以下「制度基本規程」という。) に基づいて、暗号モジュール認証機関 (以下「認証機関」という。) として実施する暗号モジュール試験及び認証制度 (JCMVP) (以下「本制度」という。) における暗号アルゴリズム確認対象非承認セキュリティ機能に関する仕様等を定めるものである。

2. 暗号アルゴリズム確認対象非承認セキュリティ機能

本章は、暗号アルゴリズム確認対象非承認セキュリティ機能のリストを提供する。

公開鍵

現在、対象となるセキュリティ機能はない。

共通鍵

＜64 ビットブロック暗号＞

1. CIPHERUNICORN-E
   暗号技術仕様書 CIPHERUNICORN-E
   http://www.cryptrec.go.jp/cryptrec_03_spec_cypherlist_files/PDF/03_00jspec.pdf

2. Hierocrypt-L1
   暗号技術仕様書 Hierocrypt-L1 (May 2002)
   http://www.cryptrec.go.jp/cryptrec_03_spec_cypherlist_files/PDF/04_02jspec.pdf

3. MISTY1
   暗号技術仕様書 MISTY1 (updated 2002 年 5 月 13 日)
   http://www.cryptrec.go.jp/cryptrec_03_spec_cypherlist_files/PDF/05_02jspec.pdf

＜128 ビットブロック暗号＞

4. CIPHERUNICORN-A
   暗号技術仕様書 CIPHERUNICORN-A
   http://www.cryptrec.go.jp/cryptrec_03_spec_cypherlist_files/PDF/07_01jspec.pdf

5. CLEFIA
   128 ビットブロック暗号 CLEFIA 暗号技術仕様書 Version 1.0
   http://www.cryptrec.go.jp/cryptrec_13_spec_cypherlist_files/PDF/22_00jspec.pdf

6. Hierocrypt-3
   暗号技術仕様書:Hierocrypt-3 (May 2002)
   http://www.cryptrec.go.jp/cryptrec_03_spec_cypherlist_files/PDF/08_02jspec.pdf

7. SC2000
   共通鍵ブロック暗号 SC2000 暗号技術仕様書 (2001 年 9 月 26 日)
   http://www.cryptrec.go.jp/cryptrec_03_spec_cypherlist_files/PDF/09_01jspec.pdf

＜ストリーム暗号＞

8. Enocoro-128v2
   疑似乱数生成器 Enocoro 仕様書 Ver. 2.0 (2010 年 2 月 2 日)
   http://www.cryptrec.go.jp/cryptrec_13_spec_cypherlist_files/PDF/23_00jspec.pdf

9. MUGI
   疑似乱数生成器 MUGI 仕様書 Ver. 1.3 (2002 年 5 月 8 日)
   http://www.cryptrec.go.jp/cryptrec_03_spec_cypherlist_files/PDF/10_02jspec.pdf

10. MULTI-S01
    仕様書 MULTI-S01 暗号 第 1.2 版 (2002 年 5 月 12 日)
    http://www.cryptrec.go.jp/cryptrec_03_spec_cypherlist_files/PDF/11_02jspec.pdf

ハッシュ

現在、対象となるセキュリティ機能はない。

メッセージ認証

1. PC-MAC-AES
   暗号技術仕様書 PC-MAC-AES
   http://www.cryptrec.go.jp/cryptrec_13_spec_cypherlist_files/PDF/24_00jspec.pdf

乱数生成器

3 章を参照

鍵確立手法

4 章を参照

3. 乱数生成器

現在、対象となるセキュリティ機能はない。

4. 鍵確立手法

1. PSEC-KEM

   PSEC-KEM 仕様書 version 2.2 (平成 20 年 4 月 14 日)

   http://www.cryptrec.go.jp/cryptrec_03_spec_cypherlist_files/PDF/02_03j_jpsec.pdf

   注: 但し、楕円曲線の位数を 224 ビット以上とする。

改訂履歴

識別番号	LSF-01	
改訂年月日	作成者・承認者	改訂内容
平成 26 年 4 月 1 日	橋本・立石	新規制定