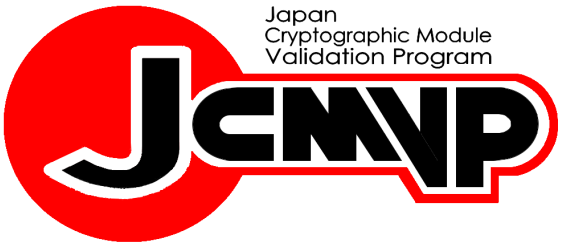


暗号アルゴリズム実装試験仕様書
– メッセージ認証 –

令和元年 7 月 11 日

IPA

ATR-01-D

Cryptographic Algorithm Implementation Testing Requirements

独立行政法人情報処理推進機構

目 次

1 目的

本書は, 暗号アルゴリズム実装試験ツール (JCATT) に実装されたメッセージ認証に関する暗号アルゴリズム実装試験仕様を記述するものである. 試験の対象とする暗号アルゴリズムは, 2 章に示す通りである.

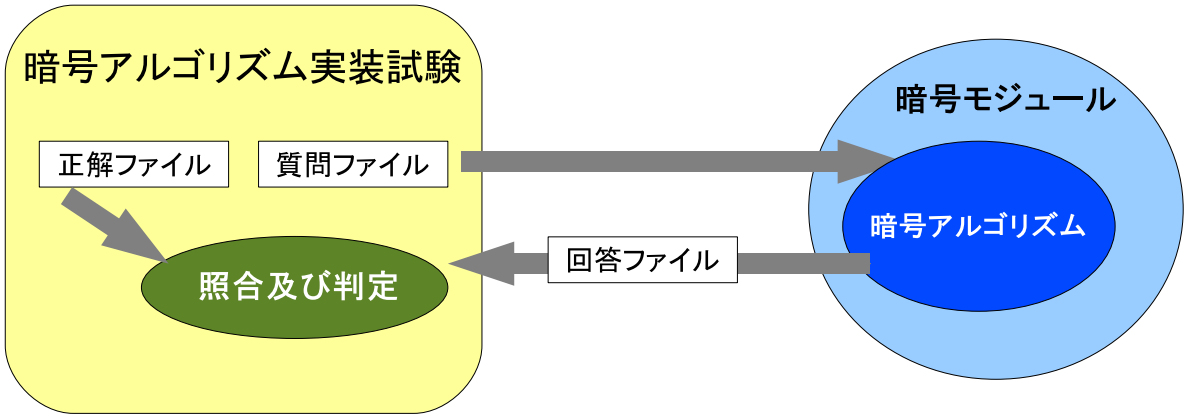
1.1 暗号アルゴリズム実装試験ツールの概要

暗号アルゴリズム実装試験ツールは次の特長を持つ.

- 試験対象の実装が暗号アルゴリズム仕様書に記述された事項に従って実装されているかどうかを試験する.
- 例えばメッセージ認証の場合はメッセージ認証子生成, メッセージ認証子検証など, 各暗号が有する機能ごとに試験を行う.
- 暗号アルゴリズム実装試験ツールと試験対象の実装は, 各種ファイルを介してデータの通信を行う. このことにより, 様々なプラットフォーム上の暗号実装を試験可能となる. ここで, ツールで使う各種ファイルの内訳は以下のとおりである.
  - 質問ファイル: 暗号アルゴリズム実装試験ツールが生成するファイル. 暗号アルゴリズムに対する入力データ及び制御情報が記録されている. 暗号モジュール試験機関からベンダ側へ送る.
  - 正解ファイル: 暗号アルゴリズム実装試験ツールが質問ファイルと同時に生成するファイル. 暗号アルゴリズムに対する入力データ, 制御情報及び対応する出力データが記録されている. 暗号モジュール試験機関で保存し, 回答ファイルが送られてきた際に回答ファイルと照合する.
  - 回答ファイル: ベンダ側で, 質問ファイルを元に暗号モジュールが生成したテキストファイル. ベンダから暗号モジュール試験機関側へ送る.

ファイルフォーマットは文献 [9], サンプルファイルは文献 [10] を参照.
暗号アルゴリズム実装試験の流れは, 図 1.1 の通りである.

図 1.1: 暗号アルゴリズム実装試験の流れ



- 試験対象の実装が暗号アルゴリズム仕様書に記述された事項に従って実装されているかどうかを試験する.
- 例えばメッセージ認証の場合はメッセージ認証子生成, メッセージ認証子検証など, 各暗号が有する機能ごとに試験を行う.

- 暗号アルゴリズム実装試験ツールと試験対象の実装は, 各種ファイルを介してデータの通信を行う. このことにより, 様々なプラットフォーム上の暗号実装を試験可能となる.

1.2 本書の構成

本書の以降の構成は次の通りである.

- 2 章: 本書が対象とする暗号アルゴリズムを示す.
- 3 章以降: 各暗号の試験項目を記述する.

なお, 本書を通して次の略語を使用する.

- JCATT: 暗号アルゴリズム実装試験ツール
- IUT: JCATT が試験の対象とする実装

2　本書で対象とする承認されたセキュリティ機能

本書が対象とする暗号アルゴリズムを次に示す.

2.1　メッセージ認証

- HMAC
- CMAC
- CCM モード
- GCM/GMAC
- GCM-AES-XPN

3 暗号アルゴリズム実装試験仕様 – メッセージ認証 –

3.1 メッセージ認証

メッセージ認証 HMAC, CMAC, CCM, GCM/GMAC , GCM-AES-XPN の各暗号アルゴリズム実装試験項目を記述する.

3.1.1 HMAC

HMAC の試験対象機能は次の通りである.

- メッセージ認証子生成機能

メッセージ認証機能の試験項目は, 試験 1 又は試験 2 である. 既定は試験 1 である.
HMAC は, 次の暗号アルゴリズムを組み合わせて使用する.

- FIPS 180-4 に記載されたハッシュ関数 又は FIPS 202 に記載されたハッシュ関数

メッセージ認証子生成機能試験に先立って, この暗号アルゴリズムの暗号アルゴリズム実装試験に合格している必要がある.

3.1.1.1 試験 1(既定の試験. JCMVP 推奨の試験)

HMAC [1] の仕様は, ハッシュ関数の入力ブロック長を B, HMAC の鍵長を $|K|$ としたとき, 次の 3 つに条件分岐する.

- $|K| < B$,
- $|K| = B$,
- $|K| > B$

そこで, IUT がサポートする鍵長の範囲について, 次の試験を行う.

- 短いメッセージに対する試験 (SMT)
- 選択された長いメッセージに対する試験 (SLMT)
- 擬似ランダムメッセージに対する試験 (PGMT)

これらの試験方法は, **暗号アルゴリズム実装試験仕様書 – ハッシュ –**(ATR-01-C) の 3.1 節及び 5.1.1 節に記述した SMT, SLMT, PGMT とそれぞれ同じである.

3.1.1.2 試験 2(HMACVS 互換 (CAVP 互換) の試験)

HMAC [1] の仕様は, ハッシュ関数の入力ブロック長を B, HMAC の鍵長を $|K|$ としたとき, 次の 3 つに条件分岐する.

- $|K| < B$,
- $|K| = B$,
- $|K| > B$

そこで, IUT がサポートする鍵長の範囲について, 複数個 (別途規定する数) のランダムな鍵, 及びメッセージ平文を与え, メッセージ認証子が期待値と一致するかどうかを試験する.

3.1.2 CMAC

CMAC の試験対象機能は次の通りである.

- メッセージ認証子生成機能
- メッセージ認証子検証機能

CMAC は, 次の暗号アルゴリズムを組み合わせて使用する.

- AES 又は 3-key Triple DES の ECB モード暗号化機能

CMAC の試験対象機能の試験に先立って, この暗号アルゴリズムの暗号アルゴリズム実装試験に合格している必要がある.

3.1.2.1 メッセージ認証子生成機能

メッセージ認証子生成機能に対する試験は, HMAC と同様に CMACVS[3] を SHAVS[4] に準じた仕様に拡張する. 試験項目は次の通りである.

- 短いメッセージに対する試験 (SMT)
- 選択された長いメッセージに対する試験 (SLMT)
- 擬似ランダムメッセージに対する試験 (PGMT)

3.1.2.1.1 短いメッセージに対する試験 (SMT)

ブロック暗号のブロック長 (ビット数) を m とする. SMT では, $m/8+1$ 個のランダムに生成されたメッセージのメッセージ認証子に対する既知入出力試験を行う. メッセージのビット長は $0, 8, 16, \ldots, m$ とする. 鍵長, メッセージ認証子長は別途定める規定値とする.

3.1.2.1.2 選択された長いメッセージに対する試験 (SLMT)

3.1.2.1.1 節のように, ブロックのブロック長 (ビット数) を m とする. SLMT では, ランダムに生成された $m/8$ 個の長いメッセージのメッセージ認証子に対する既知入出力試験を行う. 各メッセージのビット長は, $m+8\times i\times$ (“Upperbound of SLMT” -1), $1 \leq i \leq m/8$, である. Upperbound of SLMT は別途定める規定値とする. また, 鍵長, メッセージ認証子長は別途定める規定値とする.

3.1.2.1.3 擬似ランダムメッセージに対する試験 (PGMT)

与えられた Seed, outerloop 及び innerloop から, 次のアルゴリズムにより計算されるデータ MD[0]～MD[outerloop-1] に対する既知入出力試験を行う. 鍵長, メッセージ認証子長は別途定める規定値とする.

```
for (j=0; j<outerloop; j++)
{
  MAC[0] = Seed;
  MAC[1] = Seed;
  MAC[2] = Seed;
  for (i=3; i<innerloop+3; i++)
  {
    M[i] = MAC[i-3]||MAC[i-2]||MAC[i-1]; // 記号||はデータの連結
```

```
    MAC[i] = CMAC(M[i], key);
  }
  MAC[j] = MAC[i-1];
  Seed   = MAC[i-1];
  OUTPUT MAC[j];
}
```

3.1.2.2 メッセージ認証子検証機能に対する試験

メッセージ認証子検証機能試験の試験項目は次の通りである.

- JCATT が与えた正しい鍵, 平文及びメッセージ認証子に対して, IUT が検証合格と判定すること.
- JCATT が与えた改ざんされた鍵, 平文, 又はメッセージ認証子に対して, IUT が検証不合格と判定すること.

鍵長, 平文長, メッセージ認証子長は別途定める規定値とする.

3.1.3 CCM モード

CCM モードに対しては, CCMVS[5] に記述された試験を行う. 試験対象機能は次の通りである.

- 暗号化機能
- 復号機能

CCM は, 次の暗号アルゴリズムを組み合わせて使用する.

- 承認された 128 ビットブロック暗号アルゴリズムの ECB モード暗号化機能

CCM の試験対象機能の試験に先立って, この暗号アルゴリズムの暗号アルゴリズム実装試験に合格している必要がある.

3.1.3.1 暗号化機能試験

暗号化機能試験の試験項目は次の通りである.

- 種々の associated data に対する試験 (VADT)
- 種々の平文に対する試験 (VPT)
- 種々の nonce に対する試験 (VNT)
- 種々のメッセージ認証子に対する試験 (VTT)

3.1.3.1.1 種々の associated data に対する試験 (VADT)

種々の associated data に対する試験では, 鍵と nonce を固定にして複数個 (別途規定する数) のランダムな associated data, 及び平文を与え, 暗号文が期待値と一致するかどうかを試験する.
鍵長, 平文長, メッセージ認証子長, nonce 長, associated data 長は別途定める規定値とする.

3.1.3.1.2 種々の平文に対する試験 (VPT)

種々の平文に対する試験では, 鍵と nonce を固定にして複数個 (別途規定する数) のランダムな平文, 及び associated data を与え, 暗号文が期待値と一致するかどうかを試験する.
鍵長, 平文長, メッセージ認証子長, nonce 長, associated data 長は別途定める規定値とする.

3.1.3.1.3 種々の nonce に対する試験 (VNT)

種々の nonce に対する試験では, 鍵を固定にして複数個 (別途規定する数) のランダムな nonce, 及び平文, associated data を与え, 暗号文が期待値と一致するかどうかを試験する.
鍵長, 平文長, メッセージ認証子長, nonce 長, associated data 長は別途定める規定値とする.

3.1.3.1.4 種々のメッセージ認証子に対する試験 (VTT)

種々のメッセージ認証子に対する試験では, 鍵と nonce を固定にして複数個 (別途規定する数) のランダムな平文, associated data を与え, 暗号文が期待値と一致するかどうかを試験する.
鍵長, 平文長, メッセージ認証子長, nonce 長, associated data 長は別途定める規定値とする.

3.1.3.2 復号機能試験

復号機能試験の試験項目は次の通りである.

- 与えられた, 暗号文, 鍵, メッセージ認証子長, nonce, associated data の VALID な組に対して, もとの平文に復号できること.
- 与えられた, 暗号文, 鍵, メッセージ認証子長, nonce, associated data の INVALID な組に対して, INVALID を出力すること.

鍵長, 平文長は別途定める規定値とする.

3.1.4 GCM/GMAC

GCM/GMAC に対しては, GCMVS[6] に記述された試験を行う. 試験対象機能は次の通りである.

- 暗号化機能
- 復号機能

GCM/GMAC は, 次の暗号アルゴリズムを組み合わせて使用する.

- 承認された 128 ビットブロック暗号アルゴリズムの ECB モード暗号化機能

GCM/GMAC の試験対象機能の試験に先立って, この暗号アルゴリズムの暗号アルゴリズム実装試験に合格している必要がある.

3.1.4.1 暗号化機能試験

暗号化機能については, IV が外部で生成されるか, 内部で生成されるかによって, 以下の試験を行う.

- 外部生成 IV に対する試験
- 内部生成 IV に対する試験

3.1.4.1.1 外部生成 IV の場合

IUT が IV を外部から取り込む場合, 複数個 (別途指定する値) のランダムな鍵, 平文, AAD(Additional Autheticated Data), IV を与える. IUT はそれらの値から暗号文及び Authentication Tag を出力する. JCATT は, IUT から出力された暗号文及び Authentication Tag が期待値と一致するかどうかを試験する.

鍵長, 平文長, AAD 長, IV 長は別途定める規定値とする.

3.1.4.1.2 内部生成 IV の場合

IUT が IV を内部で生成する場合, 複数個 (別途指定する値) のランダムな鍵, 平文, AAD(Additional Autheticated Data) を与える. IUT は内部で IV を生成し, その IV を, 暗号文及び Authentication Tag とともに出力する. JCATT は, IUT が出力した暗号文及び Authentication Tag が, AAD, IUT の内部で生成された IV から生成される正しい暗号文, Authentication Tag と一致するかどうかを試験する.

IUT が以下の条件を満たしたとき, 試験は合格とする.

- IUT が出力した暗号文及び Authentication Tag が, AAD, IUT の内部で生成された IV から生成される正しい暗号文, Authentication Tag と一致すること.

鍵長, 平文長, AAD 長, IV 長は別途定める規定値とする.

3.1.4.2 復号機能試験

JCATT は複数個 (別途指定する値) のランダムな鍵, 平文, AAD, IV から暗号文, Authentication Tag を生成する. それらのデータのうちのいくつかを改ざんし, 検証がエラーとなるようにする. 改ざんは暗号文あるいは Authentication Tag に対して行う.

IUT が以下の条件を満たしたとき, 試験は合格とする.

- 与えられた, 暗号文, Authentication Tag, 鍵, AAD, IV の VALID な組に対して, もとの平文に復号できること.
- 与えられた, 暗号文, Authentication Tag, 鍵, AAD, IV の INVALID な組に対して, INVALID を出力すること.

鍵長, 暗号文長, AAD 長, IV 長, 改竄するデータの割合は別途定める規定値とする.

3.1.4.3 IV uniqueness についての追記

NIST SP800-38D[7] の Section 8 には, IV と鍵の uniqueness に関する要件が記述されている. この章に対する適合性の試験は暗号モジュール試験の範囲であり, 暗号アルゴリズム確認の範囲外である. JCATT ではこの章に関する試験は行わない.

3.1.5 GCM-AES-XPN

IEEE Std 802.1AEbw-2013 [8] は, 次の 2 つの暗号スイートを規定している.

- GCM-AES-XPN-128
- GCM-AES-XPN-256

GCM-AES-XPN に対しては, GCMVS[6] に記述された試験を行う. 試験対象機能は次の通りである.

- 暗号化機能
- 復号機能

GCM-AES-XPN は, 次の暗号アルゴリズムを組み合わせて使用する.

- AES ECB モード暗号化機能

GCM-AES-XPN の試験に先立って, この暗号アルゴリズムの暗号アルゴリズム実装試験に合格している必要がある.

3.1.5.1 Extended packet number recovery についての注記

IEEE Std 802.1AEbw-2013 [8] の 10.6.2 には, Packet Number (PN) の下位 32-bit から 64-bit の PN を復元する仕様が記述されている. PN の復元が正常に行われるかどうかは, 暗号アルゴリズム確認の範囲外である. 以下の GCM-AES-XPN に対する試験では, 正常に PN が復元された場合のみを対象とする.

3.1.5.2 記号の定義

GCMVS[6] における, GCM-AES-XPN に対する "*IV*" は, IEEE Std 802.1AEbw-2013 [8] 及び NIST SP800-38D[7] の *IV* の定義とは異なり, *IV* と *Salt* との排他的論理和 (xor) であるため, 次の記号を導入して試験仕様を記述する.

$$MIV \equiv SSCI||PN = IV \oplus Salt$$

ここで, *SSCI* は, IEEE Std 802.1AEbw-2013 [8] で定義された Short Secure Channel Identifier を指す.

3.1.5.3 暗号化機能試験

暗号化機能については, 次の実装の自由度が考えられる.

- *MIV* が外部で生成されるか, 内部で生成されるか
- *Salt* が外部で生成されるか, 内部で生成されるか

これらに対応して, 次の 4 つの試験仕様を記述する.

- 外部生成 *MIV*, 外部生成 *Salt* に対する試験
- 外部生成 *MIV*, 内部生成 *Salt* に対する試験
- 内部生成 *MIV*, 外部生成 *Salt* に対する試験
- 内部生成 *MIV*, 内部生成 *Salt* に対する試験

このうち, IUT が対応する試験を行うものとする.

3.1.5.3.1 外部生成 *MIV*, 外部生成 *Salt* の場合

IUT が *MIV* 及び *Salt* を外部から取り込む場合, 複数個 (別途指定する値) のランダムな鍵, 平文, AAD(Additional Autheticated Data), *MIV*, *Salt* を与える. IUT はそれらの値から暗号文及び Authentication Tag を出力する. JCATT は, IUT から出力された暗号文及び Authentication Tag が期待値と一致するかどうかを試験する.

鍵長, 平文長, AAD 長, *IV* 長, *Salt* 長は別途定める規定値とする.

3.1.5.3.2 外部生成 *MIV*, 内部生成 *Salt* の場合

IUT が *MIV* を外部から取り込み, *Salt* を内部で生成する場合, 複数個 (別途指定する値) のランダムな鍵, 平文, AAD(Additional Autheticated Data), *MIV* を与える. IUT は内部で *Salt* を生成し, その *Salt* を, 暗号文及び Authentication Tag とともに出力する. JCATT は, IUT が出力した暗号文及び Authentication Tag が, AAD, *MIV*, IUT の内部で生成された *Salt* から生成される正しい暗号文, Authentication Tag と一致するかどうかを試験する.

IUT が以下の条件を満たしたとき, 試験は合格とする.

- IUT が出力した暗号文及び Authentication Tag が, AAD, *MIV*, IUT の内部で生成された *Salt* から生成される正しい暗号文, Authentication Tag と一致すること.

鍵長, 平文長, AAD 長, *IV* 長, *Salt* 長は別途定める規定値とする.

3.1.5.3.3 内部生成 *MIV*, 外部生成 *Salt* の場合

IUT が *MIV* を内部で生成し, *Salt* を外部から取り込む場合, 複数個 (別途指定する値) のランダムな鍵, 平文, AAD(Additional Autheticated Data), *Salt* を与える. IUT は内部で *MIV* を生成し, その *MIV* を, 暗号文及び Authentication Tag とともに出力する. JCATT は, IUT が出力した暗号文及び Authentication Tag が, AAD, *Salt*, IUT の内部で生成された *MIV* から生成される正しい暗号文, Authentication Tag と一致するかどうかを試験する.

IUT が以下の条件を満たしたとき, 試験は合格とする.

- IUT が出力した暗号文及び Authentication Tag が, AAD, *Salt*, IUT の内部で生成された *MIV* から生成される正しい暗号文, Authentication Tag と一致すること.

鍵長, 平文長, AAD 長, *IV* 長, *Salt* 長は別途定める規定値とする.

3.1.5.3.4 内部生成 *MIV*, 内部生成 *Salt* の場合

IUT が *MIV* 及び *Salt* を内部で生成する場合, 複数個 (別途指定する値) のランダムな鍵, 平文, AAD(Additional Autheticated Data) を与える. IUT は内部で *MIV* 及び *Salt* を生成し, その *MIV* 及び *Salt* を, 暗号文及び Authentication Tag とともに出力する. JCATT は, IUT が出力した暗号文及び Authentication Tag が, AAD, IUT の内部で生成された *MIV* 及び *Salt* から生成される正しい暗号文, Authentication Tag と一致するかどうかを試験する.

IUT が以下の条件を満たしたとき, 試験は合格とする.

- IUT が出力した暗号文及び Authentication Tag が, AAD, IUT の内部で生成された *MIV* 及び *Salt* から生成される正しい暗号文, Authentication Tag と一致すること.

鍵長, 平文長, AAD 長, *IV* 長, *Salt* 長は別途定める規定値とする.

3.1.5.4 復号機能試験

JCATT は複数個 (別途指定する値) のランダムな鍵, 平文, AAD, *MIV*, *Salt* から暗号文, Authentication Tag を生成する. それらのデータのうちのいくつかを改ざんし, 検証がエラーとなるようにする. 改ざんは暗号文, Authentication Tag, あるいは *MIV* に対して行う.

IUT が以下の条件を満たしたとき, 試験は合格とする.

- 与えられた, 暗号文, Authentication Tag, 鍵, AAD, *MIV*, *Salt* の VALID な組に対して, もとの平文に復号できること.
- 与えられた, 暗号文, Authentication Tag, 鍵, AAD, *MIV*, *Salt* の INVALID な組に対して, INVALID を出力すること.

鍵長, 暗号文長, AAD 長, *IV* 長, *Salt* 長, 改竄するデータの割合は別途定める規定値とする.

4 確認書発行条件

4.1 パラメータについて

メッセージ認証において, 暗号アルゴリズム確認書を発行するための条件は, 網掛けされた試験対象機能を少なくとも 1 個実装し, 暗号アルゴリズム実装試験に合格することである. 暗号アルゴリズム実装試験に使用するパラメータの入力条件及びその既定値は, 表 4.1, 表 4.2, 表 4.3, 表 4.4 , 表 4.5 に記載する値とする.

4.1.1 HMAC

表 4.1: HMAC の既定値及び入力条件

試験対象機能	入力欄			既定値	入力条件
	ハッシュ関数			SHA-256	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256, SHA3-256, SHA3-384, SHA3-512
	試験 1	$\|K\| < B$	メッセージ認証用鍵のビット長	ハッシュ関数の入力ブロック長の半分	8 の倍数かつ 112 以上 16000 以下
		$\|K\| = B$		ハッシュ関数の入力ブロック長	ハッシュ関数の入力ブロック長 B に等しい
		$\|K\| > B$		ハッシュ関数の入力ブロック長の 2 倍	8 の倍数かつ B より大きく 16000 以下
		SLMT	Upperbound of SLMT	100	100 以上
		PGMT	内側ループ回数	1000	1000 以上
			外側ループ回数	100	100 以上
メッセージ認証子生成	試験 2	$\|K\| < B$	メッセージ認証用鍵のビット長	ハッシュ関数の出力長の半分 又は 112 のいずれか大きい方	8 の倍数かつ 112 以上 B 未満
			メッセージのビット長	1024	8 の倍数かつ 16000 以下
			メッセージの個数	200	15 以上
		$\|K\| = B$	メッセージ認証用鍵のビット長	ハッシュ関数の入力ブロック長	ハッシュ関数の入力ブロック長 B に等しい
			メッセージのビット長	1024	8 の倍数かつ 16000 以下
			メッセージの個数	100	15 以上
		$\|K\| > B$	メッセージ認証用鍵のビット長	ハッシュ関数の入力ブロック長の 2 倍	8 の倍数かつ B より大きく 16000 以下
			メッセージのビット長	1024	8 の倍数かつ 16000 以下
			メッセージの個数	200	15 以上

4.1.2 CMAC

表 4.2: CMAC の既定値及び入力条件

試験対象機能	入力欄		既定値	入力条件
メッセージ認証子生成	ブロック暗号		AES	AES 又は 3-Key Triple DES
	鍵長		128	AES の場合 128,192,256 のいずれか. 3-Key Triple DES の場合 192
	メッセージ認証子のビット長		128	8 の倍数. さらに, AES の場合 128 以下, 3-Key Triple DES の場合 64 以下
	Upperbound of SLMT		100	100 以上
	PGMT	内側ループ回数	1000	1000 以上
		外側ループ回数	100	100 以上
メッセージ認証子検証	ブロック暗号		AES	AES 又は 3-Key Triple DES
	鍵長		128	AES の場合 128, 192, 256 のいずれか. 3-Key Triple DES の場合 192
	メッセージ認証子のビット長		128	8 の倍数. さらに, AES の場合 128 以下, 3-Key Triple DES の場合 64 以下
	メッセージのビット長		256	8 の倍数かつ 16000 以下
	メッセージの個数		10	10 以上
	改ざんするデータの割合 (パーセント)		30	1 以上 99 以下

4.1.3 CCM

表 4.3: CCM の既定値及び入力条件

試験対象機能	入力欄		既定値	入力条件
暗号化	ブロック暗号		AES	128 ビットブロック暗号
	鍵長		128	128, 192, 256 のいずれか
	VADT	Associated data のビット長	240	8 の倍数かつ 16000 以下
		平文の個数	10	10 以上
	VPT	平文のビット長	256	8 の倍数かつ 16000 以下
		平文の個数	10	10 以上
	VNT	nonce のビット長	104	56, 64, 72, 80, 88, 96, 104 のいずれか
		平文の個数	10	10 以上
	VTT	メッセージ認証子のビット長	128	32, 48, 64, 80, 96, 112, 128 のいずれか
		平文の個数	10	10 以上
復号	ブロック暗号		AES	128 ビットブロック暗号
	鍵長		128	128, 192, 256 のいずれか
	メッセージ認証子のビット長		128	32, 48, 64, 80, 96, 112, 128 のいずれか
	平文のビット長		256	8 の倍数かつ 16000 以下
	暗号文の数		10	10 以上
	改ざんするデータの割合 (パーセント)		30	1 以上 99 以下

4.1.4 GCM/GMAC

表 4.4: GCM/GMAC の既定値及び入力条件

試験対象機能	入力欄	既定値	入力条件
暗号化	ブロック暗号	AES	128 ビットブロック暗号
	鍵長	128	128, 192, 256 のいずれか
	AAD のビット長	128	8 の倍数かつ 16000 以下
	平文のビット長	256	8 の倍数かつ 16000 以下
	平文の個数	20	20 以上
	IV 生成	内部	内部 又は 外部
	IV のビット長	96	8 の倍数かつ 8 以上かつ 16000 以下
	Authentication Tag のビット長	128	128, 120, 112, 104, 96, 64, 32 のいずれか
復号	ブロック暗号	AES	128 ビットブロック暗号
	鍵長	128	128, 192, 256 のいずれか
	AAD のビット長	128	8 の倍数かつ 16000 以下
	暗号文のビット長	256	8 の倍数かつ 16000 以下
	暗号文の個数	20	20 以上
	IV のビット長	96	8 の倍数かつ 8 以上かつ 16000 以下
	Authentication Tag のビット長	128	128, 120, 112, 104, 96, 64, 32 のいずれか
	改ざんするデータの割合 (パーセント)	30	1 以上 99 以下

4.1.5 GCM-AES-XPN

表 4.5: GCM-AES-XPN の既定値及び入力条件

試験対象機能	入力欄		既定値	入力条件
暗号化	ブロック暗号		AES	AES
	鍵長		128	128, 256 のいずれか
	平文のビット長が 0 でない場合	AAD のビット長	224	• 8 の倍数 • 16000 以下
	平文のビット長が 0 の場合	AAD のビット長の最小値	224	• 8 の倍数 • 16000 以下 • AAD のビット長の最大値以下
		AAD のビット長の最大値	11872	• 8 の倍数 • 16000 以下 • AAD のビット長の最小値以上
	IUT がサポートする平文のビット長の内, 128 で割り切れるものの最小値		0	• 128 の倍数 • 16000 以下 • 平文のビット長の最大値以下
	IUT がサポートする平文のビット長の内, 128 で割り切れるものの最大値		11648	• 128 の倍数 • 16000 以下 • 平文のビット長の最小値以上
	IUT がサポートする平文のビット長の内, 128 で割り切れないものの最小値		136	• 8 の倍数 • 16000 以下 • 平文のビット長の最大値以下
	IUT がサポートする平文のビット長の内, 128 で割り切れないものの最大値		11760	• 8 の倍数 • 16000 以下 • 平文のビット長の最小値以上
	平文の個数		20	15 以上
	IV 生成		外部	内部 又は 外部
	IV のビット長		96	96
	Salt 生成		外部	内部 又は 外部
	Salt のビット長		96	96
	Authentication Tag のビット長		128	128
復号	ブロック暗号		AES	AES
	鍵長		128	128, 256 のいずれか
	平文のビット長が 0 でない場合	AAD のビット長	224	• 8 の倍数 • 16000 以下
	平文のビット長が 0 の場合	AAD のビット長の最小値	224	• 8 の倍数 • 16000 以下 • AAD のビット長の最大値以下
		AAD のビット長の最大値	11872	• 8 の倍数 • 16000 以下 • AAD のビット長の最小値以上
	IUT がサポートする平文のビット長の内, 128 で割り切れるものの最小値		0	• 128 の倍数 • 16000 以下 • 平文のビット長の最大値以下
	IUT がサポートする平文のビット長の内, 128 で割り切れるものの最大値		11648	• 128 の倍数 • 16000 以下 • 平文のビット長の最小値以上
	IUT がサポートする平文のビット長の内, 128 で割り切れないものの最小値		136	• 8 の倍数 • 16000 以下 • 平文のビット長の最大値以下
	IUT がサポートする平文のビット長の内, 128 で割り切れないものの最大値		11760	• 8 の倍数 • 16000 以下 • 平文のビット長の最小値以上
	暗号文の個数		20	15 以上
	IV のビット長		96	96
	Salt のビット長		96	96
	Authentication Tag のビット長		128	128
	改ざんするデータの割合 (パーセント)		30	1 以上 99 以下

附 則
この手順は, 平成 21 年 1 月 23 日から施行し, 平成 21 年 1 月 8 日から適用する.

附 則
この手順は, 平成 21 年 7 月 1 日から施行し, 平成 21 年 7 月 10 日から適用する.

附 則
この手順は, 平成 24 年 2 月 29 日から施行し, 平成 24 年 6 月 1 日から適用する.

附 則
この手順は, 平成 30 年 6 月 22 日から施行し, 平成 30 年 6 月 22 日から適用する.

附 則
この手順は, 令和元年 7 月 11 日から施行し, 令和元年 7 月 11 日から適用する.

参考文献

[1] National Institute of Standards and Technology, *The Keyed-Hash Message Authentication Code (HMAC)*, FIPS PUB 198-1, July, 2008.

[2] Sharon S. Keller, Lawrence E. Bassham III, Timothy A. Hall, *The Keyed-Hash Message Authentication Code Validation System (HMACVS)*, National Institute of Standards and Technology, May 6, 2016.

[3] Sharon S. Keller, *The CMAC Validation System (CMACVS)*, National Institute of Standards and Technology, August 23, 2011.

[4] L. E. Bassham III, *The secure hash algorithm validation system (SHAVS)*, National Institute of Standards and Technology, May 21, 2014.

[5] L. E. Bassham III, *The CCM validation system (CCMVS)*, National Institute of Standards and Technology, January 9, 2012.

[6] Sharon S. Keller,Timothy A. Hall, *The Galois/Counter Mode (GCM) and GMAC Validation System (GCMVS) with the Addition of XPN Validation Testing*, National Institute of Standards and Technology, June 15, 2016.

[7] Morris Dworkin, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*, NIST SP 800-38D, National Institute of Standards and Technology, November, 2007.

[8] IEEE Standards Association, *Standard for Local and metropolitan area networks, Media Access Control (MAC) Security, Amendment 2: Extended Packet Numbering*, 802.1AEbw-2013, February 12, 2013.

[9] JCATT ファイルフォーマット仕様書 – メッセージ認証 –, `https://www.ipa.go.jp/security/jcmvp/documents/open/jcatt/format/jcatt_fileformat_d.zip`

[10] JCATT サンプルファイル – メッセージ認証 –, `https://www.ipa.go.jp/security/jcmvp/documents/open/jcatt/sample/jcatt_sample_d.zip`

改版履歴

識別番号	ATR-01-D

改訂年月日	作成者・承認者	改訂内容
平成 21 年 1 月 23 日	橋本・仲田	新規制定
平成 21 年 7 月 1 日	櫻井・仲田	一部改正 (HMAC-RIPEMD-160 を削除)
平成 24 年 2 月 29 日	橋本・仲田	一部改正 (GCM/GMAC に関する記述を追加)
平成 30 年 6 月 22 日	櫻井・江口	一部改正 (HMAC について, HMACVS 互換の試験, 及び SHA-3 と組み合わせる記述を追加)
令和元年 7 月 11 日	櫻井・江口	一部改正 (GCM-AES-XPN の記述を追加. 依存関係のある暗号アルゴリズムを記載 及び CCM 及び GCM の記述を訂正)