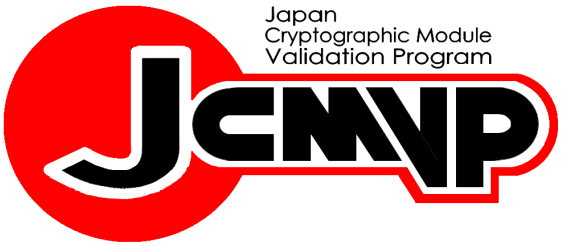


暗号アルゴリズム実装試験仕様書
– 公開鍵 –

令和 4 年 8 月 10 日

IPA

ATR-01-A

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) に実装された公開鍵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.

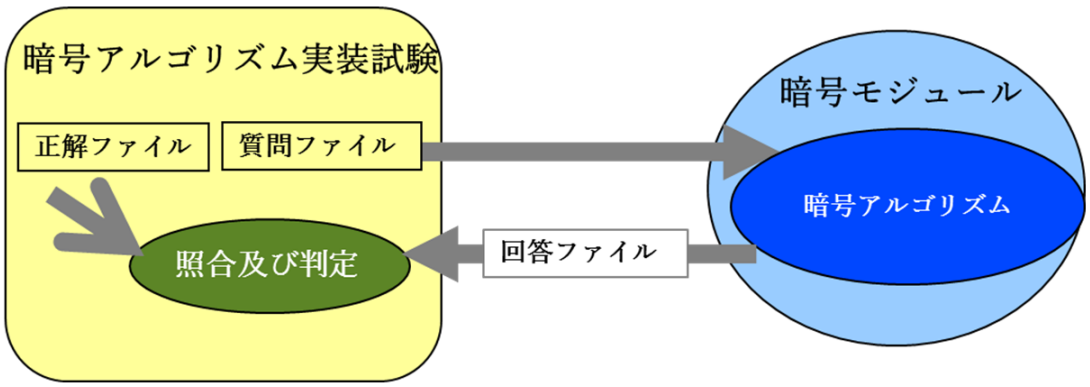
1.1　暗号アルゴリズム実装試験ツールの概要

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.
- 例えばディジタル署名の場合は署名生成機能, 署名検証機能, 鍵ペア生成機能など, 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 [3], サンプルファイルは文献 [4] を参照.
暗号アルゴリズム実装試験の流れ 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



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: 暗号アルゴリズム実装試験ツールが試験の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

本書が試験対象とする暗号アルゴリズムを次に示す.

2.1　公開鍵

2.1.1　署名

- DSA (FIPS 186-4)
- ECDSA
- RSASSA-PKCS1-v1_5
- RSASSA-PSS

2.1.2　守秘

- RSA-OAEP

3　暗号アルゴリズム実装試験仕様 – 公開鍵 –

3.1　署名

ディジタル署名 DSA (FIPS 186-4), ECDSA, RSASSA-PKCS1-v1_5, RSASSA-PSS の各暗号アルゴリズム試験項目を記述する.

3.1.1　DSA (FIPS 186-4)

DSA (FIPS 186-4) の試験対象機能は次の通りである.

- ドメインパラメータ生成機能
- ドメインパラメータ検証機能
- 鍵ペア生成機能
- 署名生成機能
- 署名検証機能

3.1.1.1　ドメインパラメータ生成機能試験

ドメインパラメータのうち p と q については,

- FIPS 186-4 Appendix A 1.1.2 “Generation of the Probable Primes p and q Using an Approved Hash Function”

又は

- FIPS 186-4 Appendix A 1.2.1 “Generation of the Primes p and q Using the Shawe-Taylor Algorithm”

に記述されているドメインパラメータ生成法に従って p と q が生成されていることを試験する.
また, ドメインパラメータ g については,

- FIPS 186-4 Appendix A 2.1 “Unverifiable Generation of the Generator g”

又は

- FIPS 186-4 Appendix A 2.3 “Verifiable Canonical Generation of the Generator g”

に記述されているドメインパラメータ生成法に従って g が生成されていることを試験する.
ドメインパラメータ生成機能は, 次の暗号アルゴリズムを組み合わせて使用する.

- FIPS 180-4 で規定されたハッシュ関数

ドメインパラメータ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.

3.1.1.1.1　p, q の生成試験

3.1.1.1.1.1　FIPS 186-4 A.1.1.2 に基づく確率的素数 p, q の生成

FIPS 186-4 Appendix A に記述されているドメインパラメータ $p, q, counter, domain\_parameter\_seed$ の正当性も試験する.

- 指定された FFC パラメータセット及びハッシュ関数に対して，IUT が生成した *domain_parameter_seed* 及び *counter* を JCATT に入力し, JCATT は FIPS 186-4 A.1.1.2 のアルゴリズムに従って 2 つの素数 p', q' を計算する. この p', q' と, IUT が生成した p, q がそれぞれ等しいこと.
- IUT が生成した複数 (別途規定する数) のドメインパラメータ (p,q) が全て異なるものであること.

3.1.1.1.1.2 FIPS 186-4 A.1.2.1 に基づく素数 p, q の生成

- 指定された FFC パラメータセット及びハッシュ関数に対して, IUT が生成した *firstseed* を JCATT に入力し, JCATT は FIPS 186-4 A.1.2.1 のアルゴリズムに従って p', q', *pseed*′, *qseed*′, *pgen_counter*′ 及び *qgen_counter*′ を計算する. この p', q', *pseed*′, *qseed*′, *pgen_counter*′ 及び *qgen_counter*′ と, IUT が生成した p, q, *pseed*, *qseed*, *pgen_counter* 及び *qgen_counter* とがそれぞれ等しいこと.
- IUT が生成した複数 (別途規定する数) のドメインパラメータ (p,q) が全て異なるものであること.

3.1.1.1.2 g の生成試験

3.1.1.1.2.1 FIPS 186-4 A.2.1 に基づく g の生成

- p 及び q に対して, IUT が生成した g を JCATT に入力し, JCATT は FIPS 186-4 A.2.2 のアルゴリズムに従って $2 \leq g \leq p-1$ かつ $g^q \equiv 1 \mod p$ を満たすか試験する.

3.1.1.1.2.2 FIPS 186-4 A.2.3 に基づく g の生成

- p 及び q, *domain_parameter_seed*, 及び *index* に対して, IUT が生成した g を JCATT に入力し, JCATT は FIPS 186-4 A.2.3 のアルゴリズムに従って g' を計算する. この g' と IUT が生成した g とが等しいこと. (なお, p 及び q を FIPS 186-4 A.1.2.1 に基づいて生成する場合, *firstseed*, *pseed*, 及び *qseed* を連結したものを *domain_parameter_seed* として扱う.)

3.1.1.2 ドメインパラメータ検証機能試験

ドメインパラメータのうち p と q については,

- FIPS 186-4 Appendix A 1.1.3 “Validation of the Probable Primes p and q that were Generated Using an Approved Hash Function”

又は

- FIPS 186-4 Appendix A 1.2.2 “Validation of the DSA Primes p and q that were Constructed Using the Shawe-Taylor Algorithm”

に従って p と q を検証する機能を試験する.
また, ドメインパラメータ g については,

- FIPS 186-4 Appendix A 2.2 “Assurance of the Validity of the Generator g”

又は

- FIPS 186-4 Appendix A 2.4 “Validation Routine when the Canonical Generation of the Generator g Routine Was Used”

に従って g が検証する機能を試験する.

ドメインパラメータ検証機能は, 次の暗号アルゴリズムを組み合わせて使用する.

- FIPS 180-4 で規定されたハッシュ関数

ドメインパラメータ検証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.

3.1.1.2.1 p, q の検証試験

3.1.1.2.1.1 FIPS 186-4 A.1.1.3 に基づく p, q の検証

- 3.1.1.1.1.1 節に記述した p, q 生成機能に対する試験に適合するような p, q, *domain_parameter_seed*, *counter* に対して, IUT が “合格”と判定すること.
- 3.1.1.1.1.1 節に記述した p, q 生成機能に対する試験に違反するような p, q, *domain_parameter_seed*, *counter* に対して, IUT が “不正”と判定すること.

3.1.1.2.1.2 FIPS 186-4 A.1.2.2 に基づく p, q の検証

- 3.1.1.1.1.2 節に記述した p, q 生成機能に対する試験に適合するような p, q, *first_seed*, *pseed*, *qseed*, *pgen_counter*, *qgen_counter* に対して, IUT が “合格”と判定すること.
- 3.1.1.1.1.2 節に記述した p, q 生成機能に対する試験に違反するような p, q, *first_seed*, *pseed*, *qseed*, *pgen_counter*, *qgen_counter* に対して, IUT が “不正”と判定すること.

3.1.1.2.2 g の検証試験

3.1.1.2.2.1 FIPS 186-4 A.2.2 に基づく g の検証

- 3.1.1.1.2.1 節に記述した g 生成機能に対する試験に適合するような p, q, g に対して, IUT が “合格”と判定すること.
- 3.1.1.1.2.1 節に記述した g 生成機能に対する試験に違反するような p, q, g に対して, IUT が “不正”と判定すること.

3.1.1.2.2.2 FIPS 186-4 A.2.4 に基づく g の検証

- 3.1.1.1.2.2 節に記述した g 生成機能に対する試験に適合するような p, q, g, *domain_parameter_seed*, 及び *index* に対して, IUT が “合格”と判定すること.
- 3.1.1.1.2.2 節に記述した g 生成機能に対する試験に違反するような p, q, g, *domain_parameter_seed*, 及び *index* に対して, IUT が “不正”と判定すること.

3.1.1.3 鍵ペア生成機能試験

鍵ペア生成機能試験の試験項目は次の通りである. なお, プライベート鍵を x, 公開鍵を y とする.

- $y \equiv g^x \pmod{p}$ であること
- $1 \leq x \leq q-1, 2 \leq y \leq p-2$ であること
- $y^q \equiv 1 \pmod{p}$ であること
- IUT が生成した複数 (別途規定する数) の鍵ペアが全て異なるものであること.

鍵ペア生成機能は, 次の暗号アルゴリズムを組み合わせて使用する.

- NIST SP800-90A で規定された決定論的乱数生成器

鍵ペア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.

3.1.1.4 署名生成機能試験

署名生成機能試験の試験項目は, 試験 1 又は試験 2 である. 既定は試験 1 である.

試験 1(既定の試験. JCMVP 推奨の試験)

- JCATT が与えたプライベート鍵 x , ドメインパラメータ 及び平文 , 並びに指定されたハッシュ関数に対して, IUT が生成した署名を, JCATT が署名検証した時に署名検証合格となること.
- 同じ平文, 同じプライベート鍵に対して複数 (別途規定する数) 署名を生成させた時, IUT が同じ署名を生成しないこと.

試験 2(DSA2VS 互換 (CAVP 互換) の試験)

- JCATT が与えた平文, 及び指定されたハッシュ関数に対して, IUT が生成した署名, それに対応するドメインパラメータ及び公開鍵を, JCATT が署名検証した時に署名検証合格となること.

署名生成機能は, 次の暗号アルゴリズムを組み合わせて使用する.

- FIPS 180-4 で規定されたハッシュ関数 (SHA-1 を除く)
- NIST SP800-90A で規定された決定論的乱数生成器

署名生成機能試験に先立って, これら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.

3.1.1.5 署名検証機能試験

署名検証機能試験の試験項目は次の通りである.

- JCATT が与えた正しい公開鍵 y, ドメインパラメータ, 平文及び署名, 並びに指定されたハッシュ関数に対して, IUT が正しく署名検証合格と判定すること.
- JCATT が改竄した平文, 署名, 又は公開鍵に対して, IUT が署名検証不合格と判定すること.

署名検証機能は, 次の暗号アルゴリズムを組み合わせて使用する.

- FIPS 180-4 で規定されたハッシュ関数 (SHA-1 を除く)

署名検証機能試験に先立って, これら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 ECDSA

ECDSA の試験対象機能は次の通りである.

- ドメインパラメータ生成機能
- ドメインパラメータ検証機能
- 鍵ペア生成機能
- 公開鍵検証機能
- 署名生成機能
- 署名検証機能

3.1.2.1 ドメインパラメータ生成機能試験

ドメインパラメータ生成機能試験の試験項目は次の通りである.

3.1.2.1.1 標数 p の場合

検証可能なランダム曲線であるかどうかに応じて試験 1, 2 のいずれかを実行する. 既定は試験 1 である.

試験 1(既定の試験)

$\mathbb{F}_p$ 上楕円曲線の場合

- セキュリティレベルを s として, n が $\max(2s, 224)$ ビット以上であること.
- $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$ であること.
- a, b, x_G, y_G が 0 以上 $p-1$ 以下の整数であること.
- $y_G^2 \equiv x_G^3 + ax_G + b \pmod{p}$ であること.
- n が素数であること.
- p が素数であること.
- $h \leq 2^{s/8}$ かつ $h = \lfloor (\sqrt{p}+1)^2/n \rfloor$ であること.
- $nG = \mathcal{O}$ であること.
- すべての $1 \leq B < 100$ に対して $p^B \not\equiv 1 \pmod{n}$ であること.
- $nh \neq p$ であること.
- IUT が生成した複数 (別途規定する数) のドメインパラメータが全て異なるものであること.

試験 2(検証可能なランダム曲線に対する試験)

$\mathbb{F}_p$ **上楕円曲線の場合**

- IUT が SEED を出力する場合, ANS X9.62 A.3.3 に記述された “Verifiably random”な方法で生成された曲線であることを検証する.
- セキュリティレベルを s として, n が $\max(2s, 224)$ ビット以上であること.
- $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$ であること.
- a, b, x_G, y_G が 0 以上 $p-1$ 以下の整数であること.
- $y_G^2 \equiv x_G^3 + ax_G + b \pmod{p}$ であること.
- n が素数であること.
- p が素数であること.
- $h \leq 2^{s/8}$ かつ $h = \lfloor (\sqrt{p}+1)^2/n \rfloor$ であること.
- $nG = \mathcal{O}$ であること.
- すべての $1 \leq B < 100$ に対して $p^B \not\equiv 1 \pmod{n}$ であること.
- $nh \neq p$ であること.
- IUT が生成した複数 (別途規定する数) のドメインパラメータが全て異なるものであること.

3.1.2.1.2 標数 2 の場合

検証可能なランダム曲線であるかどうかに応じて試験 1, 2 のいずれかを実行する. 既定は試験 1 である.

試験 1(既定の試験)

$\mathbb{F}_{2^m}$ **上楕円曲線の場合**

- セキュリティレベルを s として, n が $\max(2s, 224)$ ビット以上であること.
- $f(x)$ が次数 m の $\mathbb{F}_2$ 上既約多項式であること.
- a, b, x_G, y_G が次数 $m-1$ 以下の $\mathbb{F}_2$ 上多項式であること.
- $b \neq 0$ in $\mathbb{F}_{2^m}$ であること.
- $y_G^2 + x_G y_G \equiv x_G^3 + ax_G^2 + b$ in $\mathbb{F}_{2^m}$ であること.
- n が素数であること.
- $h \leq 2^{s/8}$ かつ $h = \lfloor (\sqrt{2^m}+1)^2/n \rfloor$ であること.
- $nG = \mathcal{O}$ であること.
- すべての $1 \leq B < 100$ に対して $2^{mB} \not\equiv 1 \pmod{n}$ であること.
- $nh \neq 2^m$ であること.
- IUT が生成した複数 (別途規定する数) のドメインパラメータが全て異なるものであること.

試験 2(検証可能なランダム曲線に対する試験)

$\mathbb{F}_{2^m}$ **上楕円曲線の場合**

- IUT が SEED を出力する場合, ANS X9.62 A.3.3 に記述された “Verifiably random”な方法で生成された曲線であることを検証する.
- セキュリティレベルを s として, n が $\max(2s, 224)$ ビット以上であること.
- $f(x)$ が次数 m の $\mathbb{F}_2$ 上既約多項式であること.
- a, b, x_G, y_G が次数 $m-1$ 以下の $\mathbb{F}_2$ 上多項式であること.
- $b \neq 0$ in $\mathbb{F}_{2^m}$ であること.
- $y_G^2 + x_G y_G \equiv x_G^3 + a x_G^2 + b$ in $\mathbb{F}_{2^m}$ であること.
- n が素数であること.
- $h \leq 2^{s/8}$ かつ $h = \lfloor (\sqrt{2^m}+1)^2/n \rfloor$ であること.
- $nG = \mathcal{O}$ であること.
- すべての $1 \leq B < 100$ に対して $2^{mB} \not\equiv 1 (\mod n)$ であること.
- $nh \neq 2^m$ であること.
- IUT が生成した複数 (別途規定する数) のドメインパラメータが全て異なるものであること.

3.1.2.2 ドメインパラメータ検証機能試験

ドメインパラメータ検証機能試験の試験項目は次の試験 1 又は試験 2 である. 既定は試験 1 である.

試験 1(既定の試験)

- JCATT が与えた前節に記述したドメインパラメータ生成機能試験項目に適合するようなドメインパラメータに対して, IUT が “合格”と判定すること.
- JCATT が与えた前節に記述したドメインパラメータ生成機能試験項目に違反するようなドメインパラメータに対して, IUT が “不正”と判定すること.

試験 2(検証可能なランダム曲線に対する試験)

- IUT が ANS X9.62 A.3.3 に記述された “Verifiably random”な方法で生成された曲線であることを検証する機能を持つ場合, JCATT が与えた正しいドメインパラメータ (SEED を含む) に対して “合格”と判定し, JCATT が与えた不正なドメインパラメータに対して “不正”と判定すること.

3.1.2.3 鍵ペア生成機能試験

鍵ペア生成機能は, 次の暗号アルゴリズムを組み合わせて使用する.

- NIST SP800-90A で規定された決定論的乱数生成器

鍵ペア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.

鍵ペア生成機能試験の試験項目は次の通りである.

3.1.2.3.1 標数 p の場合

- $Q \neq \mathcal{O}$ であること.
- $y_Q^2 \equiv x_Q^3 + ax_Q + b(\mod p)$ であること.
- $nQ = \mathcal{O}$ であること.
- $Q = dG$ であること.
- IUT が生成した複数 (別途規定する数) の鍵ペアが全て異なるものであること.

3.1.2.3.2 標数 2 の場合

- $Q \neq \mathcal{O}$ であること.
- $y_Q^2 + x_Q y_Q \equiv x_Q^3 + ax_Q^2 + b$ in $\mathbb{F}_{2^m}$ であること.
- $nQ = \mathcal{O}$ であること.
- $Q = dG$ であること.
- IUT が生成した複数 (別途規定する数) の鍵ペアが全て異なるものであること.

3.1.2.4 公開鍵検証機能試験

公開鍵検証機能試験の試験項目は次の通りである.

- JCATT が与えた前節に記述した鍵ペア生成機能試験項目に適合するような公開鍵に対して, IUT が “合格”と判定すること.
- JCATT が与えた前節に記述した鍵ペア生成機能試験項目に違反するような公開鍵に対して, IUT が “不正”と判定すること.

3.1.2.5 署名生成機能試験

署名生成機能試験の試験項目は, 試験 1 又は試験 2 である. 既定は試験 1 である.

ハッシュ関数は, SHA-224, SHA-256, SHA-384, SHA-512 , SHA-512/224, SHA-512/256 の中から指定する.

署名生成機能は, 次の暗号アルゴリズムを組み合わせて使用する.

- 上述の使用するハッシュ関数
- NIST SP800-90A で規定された決定論的乱数生成器

署名生成機能試験に先立って, これら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.

試験 1(既定の試験. JCMVP 推奨の試験)

- JCATT が与えたプライベート鍵 d 及び平文に対して, IUT が生成した署名を, JCATT が署名検証した時に署名検証合格となること.
- 同じ平文, 同じプライベート鍵に対して複数 (別途規定する数) 署名を生成させた時, IUT が同じ署名が生成されないこと.

試験 2(ECDSA2VS 互換 (CAVP 互換) の試験)

- JCATT が与えた平文に対して, IUT が生成した署名及びそれに対応する公開鍵を, JCATT が署名検証した時に署名検証合格となること.

3.1.2.6 署名検証機能試験

署名検証機能試験の試験項目は次の通りである.

- JCATT が与えた正しい公開鍵 Q, 平文及び署名, 並びに指定されたハッシュ関数に対して, IUT が署名検証合格と判定すること.
- JCATT が改竄した平文, 署名, 又は公開鍵に対して, IUT が署名検証不合格と判定すること.

ハッシュ関数は, SHA-224, SHA-256, SHA-384, SHA-512 , SHA-512/224, SHA-512/256 の中から指定する.

署名検証機能試験に先立って, 使用するハッシュ関数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 RSASSA-PKCS1-v1_5

RSASSA-PKCS1-v1_5 の試験対象機能は次の通りである.

- 鍵ペア生成機能
- 署名生成機能
- 署名検証機能

3.1.3.1 鍵ペア生成機能試験

文献 [1] に記載された RSA アルゴリズム (RSA-OAEP, RSASSA-PKCS1-v1_5, RSASSA-PSS) のプライベート鍵は, プライベート鍵演算 (復号及び署名生成) において Chinese Remainder Theorem (CRT) を用いるかどうかによって, 2 種類に分かれる. CRT を用いない場合, プライベート鍵は (n,d) の組であり, CRT を用いる場合は $(p,q,dP,dQ,qInv)$ の組である. したがって, 試験対象の鍵ペア生成機能が CRT 用の $dP,dQ,qInv$ を出力するかどうかによって, 試験項目を 2 通りに分けることとする. それぞれ試験項目は次の通りである.

CRT を用いない場合の鍵ペア生成機能試験項目

- n が指定されたビット長であること.
- p と q のビット長が等しいこと.
- p は素数であること.
- q は素数であること.
- $n = pq$ を満たすこと.
- $e \cdot d \equiv 1 \mod \lambda(n)$ を満たすこと.
- 生成された複数 (別途規定する数) の鍵ペアが全て異なるものであること.

CRT を用いる場合の鍵ペア生成機能試験項目

- n が指定されたビット長であること.
- p と q のビット長が等しいこと.
- p は素数であること.
- q は素数であること.
- $n = pq$ を満たすこと.
- $e \cdot dP \equiv 1 \mod p-1$ を満たすこと.
- $e \cdot dQ \equiv 1 \mod q-1$ を満たすこと.
- $q \cdot qInv \equiv 1 \mod p$ を満たすこと.
- 生成された複数 (別途規定する数) の鍵ペアが全て異なるものであること.

ここで, $\lambda(n)$ は $p-1$ と $q-1$ の最小公倍数である.

鍵ペア生成機能は, 次の暗号アルゴリズムを組み合わせて使用する.

- NIST SP800-90A で規定された決定論的乱数生成器

鍵ペア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.

3.1.3.2 署名生成機能試験

署名生成機能試験の試験項目は次の通りである.

- JCATT が与えたプライベート鍵 (n,d) 又は $(p,q,dP,dQ,qInv)$, 及び平文, 並びに指定されたハッシュ関数に対して IUT が正しい署名を生成すること.

ハッシュ関数は, SHA-224, SHA-256, SHA-384, SHA-512 , SHA-512/224, SHA-512/256 の中から指定する.

署名生成機能試験に先立って, 使用するハッシュ関数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.

3.1.3.3 署名検証機能試験

署名検証機能試験の試験項目は次の通りである.

- JCATT が与えた公開鍵 (n,e), 平文及び署名, 並びに指定されたハッシュ関数に対して, IUT が署名検証合格と判定すること.
- JCATT が改竄した平文, 署名, 又は公開鍵に対して, IUT が署名検証不合格と判定すること.

ハッシュ関数は, SHA-224, SHA-256, SHA-384, SHA-512 , SHA-512/224, SHA-512/256 の中から指定する.

署名検証機能試験に先立って, 使用するハッシュ関数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 RSASSA-PSS

RSASSA-PSS の試験対象機能は次の通りである.

- 鍵ペア生成機能
- 署名生成機能
- 署名検証機能

3.1.4.1 鍵ペア生成機能試験

3.1.3 節に記述した鍵ペア生成機能試験項目と同じである.

3.1.4.2 署名生成機能試験

署名生成機能試験の試験項目は次の試験 1 又は試験 3 である. 既定は試験 1 である.

試験 1

- JCATT が与えたプライベート鍵 (n,d) 又は $(p,q,dP,dQ,qInv)$, 平文に対して IUT が生成した署名を, JCATT が署名検証した時に署名検証合格となること.
- *salt* 長が 0 でない場合, 同じ平文, 同じプライベート鍵に対して, 複数 (別途規定する数) 署名を生成させた時, IUT が同じ署名を生成しないこと.

試験 3(任意で実施する試験. *salt* を指定して行う既知入出力試験)

- JCATT が与えたプライベート鍵 (n,d) 又は $(p,q,dP,dQ,qInv)$, 平文, 並びに指定されたハッシュ関数, *salt* に対して IUT が正しい署名を生成すること.

ハッシュ関数は, SHA-224, SHA-256, SHA-384, SHA-512 , SHA-512/224, SHA-512/256 の中から指定する.

署名生成機能は, 次の暗号アルゴリズムを組み合わせて使用する.

- 上述の使用するハッシュ関数
- NIST SP800-90A で規定された決定論的乱数生成器

署名生成機能試験に先立って, これら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.

3.1.4.3 署名検証機能試験

3.1.3 節に記述した RSASSA-PKCS1-v1_5 の署名検証機能試験項目と同じである.

3.2 守秘

公開鍵暗号 (守秘) RSA-OAEP の各暗号アルゴリズム試験項目を記述する.

3.2.1 RSA-OAEP

RSA-OAEP の試験対象機能は次の通りである.

- 鍵ペア生成機能
- 暗号化機能
- 復号機能

3.2.1.1 鍵ペア生成機能試験

鍵ペア生成機能試験の試験項目は 3.1.3 節に記述した試験項目と同じである.

3.2.1.2 暗号化機能試験

暗号化機能試験の試験項目は次の試験 1 又は試験 3 である. 既定は試験 1 である.

試験 1(既定の試験)

- JCATT が与えた公開鍵 (n,e) 及び平文, 並びに指定されたハッシュ関数及びマスク生成関数 *MGF* 及びラベル L に対して IUT が生成した暗号文を, JCATT が復号した時に, もとの平文に復号されること.
- 同じ平文, 同じ公開鍵, 同じラベル値に対して, 複数 (別途規定する数) 暗号文を生成させた時, 同じ暗号文が生成されないこと.

試験 3(任意で実施する試験. 中間値 *seed* を指定して行う既知入出力試験)

- JCATT が与えた公開鍵 (n,e), 平文及びラベル L, 並びに指定されたハッシュ関数, マスク生成関数 *MGF* 及び中間値 *seed* 対して正しい暗号文を IUT が生成すること.

ハッシュ関数は, SHA-224, SHA-256, SHA-384, SHA-512 , SHA-512/224, SHA-512/256 の中から指定する.

マスク生成関数 *MGF* は, ANSI X9.44 に記載の SHA-224, SHA-256, SHA-384, SHA-512 , SHA-512/224, SHA-512/256 ベースの関数の中から指定する.

暗号化機能は, 次の暗号アルゴリズムを組み合わせて使用する.

- 上述の使用するハッシュ関数
- NIST SP800-90A で規定された決定論的乱数生成器

暗号化機能試験に先立って, これら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.

3.2.1.3 復号機能試験

復号機能の試験項目は次の通りである.

- 与えられたプライベート鍵 (n,d) 又は $(p,q,dP,dQ,qInv)$ と, 与えられたラベル L と, 指定されたハッシュ関数及びマスク生成関数 MGF と, 与えられた暗号文に対して, もとの平文に復号できること.
- 与えられたプライベート鍵 (n,d) 又は $(p,q,dP,dQ,qInv)$ と, 与えられたラベル L と, 指定されたハッシュ関数及びマスク生成関数 MGF と, 改竄された暗号文に対して不正検出を正しく行うこと.

ハッシュ関数は, SHA-224, SHA-256, SHA-384, SHA-512 , SHA-512/224, SHA-512/256 の中から指定する.

マスク生成関数 MGF は, ANSI X9.44 に記載の SHA-224, SHA-256, SHA-384, SHA-512 , SHA-512/224, SHA-512/256 ベースの関数の中から指定する.

復号機能試験に先立って, 使用するハッシュ関数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.

4 確認書発行条件

4.1 パラメータについて

公開鍵暗号アルゴリズムにおいて, 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 4.6 に記載する値とする.

4.1.1 DSA (FIPS 186-4)

表 4.1: DSA 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
ドメインパラメータ生成	(L, N)=(p のビット長 , q のビット長)		(3072, 256)	次のいずれか • (2048, 224) • (2048, 256) • (3072, 256)
	FIPS 186-4 A.1.1.2 に基づく p, q の生成	ハッシュ関数識別子	SHA-256	• $N = 224$ の場合, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256 のいずれか • $N = 256$ の場合, SHA-256, SHA-384, SHA-512, SHA-512/256 のいずれか
		domain_parameter_seed のビット長	256	8 の倍数かつ N 以上かつ 16000 以下
		生成する p, q の数	10	5 以上
	FIPS 186-4 A.1.2.1 に基づく p, q の生成	ハッシュ関数識別子	SHA-256	• $N = 224$ の場合, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256 のいずれか • $N = 256$ の場合, SHA-256, SHA-384, SHA-512, SHA-512/256 のいずれか
		first_seed のビット長	256	8 の倍数かつ N 以上かつ 16000 以下
		生成する p, q の数	10	5 以上
	FIPS 186-4 A.2.1 に基づく g の生成	生成する g の数	10	5 以上
	FIPS 186-4 A.2.3 に基づく g の生成	*domain_parameter_seed* のビット長	256	• FIPS 186-4 A.1.1.2 に基づく p, q の生成の選択時 – 8 の倍数かつ N 以上かつ 16000 以下 • FIPS 186-4 A.1.2.1 に基づく p, q の生成の選択時 – 8 の倍数かつ $3N$ 以上かつ 16000 以下
		生成する g の数	10	5 以上
ドメインパラメータ検証	(L, N)=(p のビット長 , q のビット長)		(3072, 256)	次のいずれか • (2048, 224) • (2048, 256) • (3072, 256)
	FIPS 186-4 A.1.1.3 に基づく p, q の検証	ハッシュ関数識別子	SHA-256	• $N = 224$ の場合, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256 のいずれか • $N = 256$ の場合, SHA-256, SHA-384, SHA-512, SHA-512/256 のいずれか
		domain_parameter_seed のビット長	256	8 の倍数かつ N 以上かつ 16000 以下
		生成個数	10	5 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

	FIPS 186-4 A.1.2.2 に基づく p, q の検証	ハッシュ関数識別子	SHA-256	• $N = 224$ の場合, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256 のいずれか • $N = 256$ の場合, SHA-256, SHA-384, SHA-512, SHA-512/256 のいずれか
		first_seed, *pseed*, *qseed* のビット長	256	8 の倍数かつ N 以上かつ 16000 以下
		生成する p, q の数	10	5 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
	FIPS 186-4 A.2.2 に基づく g の検証	生成する g の数	10	5 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
	FIPS 186-4 A.2.4 に基づく g の検証	*domain_parameter_seed* のビット長	256	• FIPS 186-4 A.1.1.2 に基づく p, q の生成の選択時 – 8 の倍数かつ N 以上かつ 16000 以下 • FIPS 186-4 A.1.2.1 に基づく p, q の生成の選択時 – 8 の倍数かつ $3N$ 以上かつ 16000 以下
		生成する g の数	10	5 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
鍵ペア生成	(L, N)=(p のビット長 , q のビット長)		(3072, 256)	次のいずれか • (2048, 224) • (2048, 256) • (3072, 256)
	生成個数		10	10 以上
署名生成	(L, N)=(p のビット長 , q のビット長)		(3072, 256)	次のいずれか • (2048, 224) • (2048, 256) • (3072, 256)
	ハッシュ関数		SHA-256	SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256 のいずれか
	平文のビット長		1024	8 の倍数かつ 16000 以下
	試験 1	平文の数	20	10 以上
		いつも異なる署名が生成されることを検証するための署名の個数	2048	10 以上
	試験 2	平文の数	20	10 以上
署名検証	(L, N)=(p のビット長 , q のビット長)		(3072, 256)	次のいずれか • (2048, 224) • (2048, 256) • (3072, 256)
	ハッシュ関数		SHA-256	SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256 のいずれか
	平文のビット長		1024	8 の倍数かつ 16000 以下
	平文の数		100	50 以上
	改ざんするデータの割合 (パーセント)		50	1 以上 99 以下

4.1.2 ECDSA

表 4.2: 素体上 ECDSA 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
ドメインパラメータ生成	p のビット長		256	8 の倍数 かつ 16000 以下
	曲線のランダム性検証用 SEED のビット長		256	8 の倍数 かつ 16000 以下
	生成個数		10	10 以上
ドメインパラメータ検証	なし		–	–
鍵ペア生成	鍵の個数		10	10 以上
公開鍵検証	鍵の個数		12	12 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
署名生成	ハッシュ関数		SHA-256	SHA-224, SHA-256, SHA-384, SHA-512 , SHA-512/224 , SHA-512/256 のいずれか
	平文のビット長		1024	8 の倍数かつ 16000 以下
	試験 1	平文の数	20	10 以上
		いつも異なる署名が生成されることを検証するための署名の個数	2048	10 以上
	試験 2	平文の数	20	10 以上
署名検証	ハッシュ関数		SHA-256	SHA-224, SHA-256, SHA-384, SHA-512 , SHA-512/224 , SHA-512/256 のいずれか
	平文のビット長		1024	8 の倍数かつ 16000 以下
	平文の数		100	50 以上
	改ざんするデータの割合 (パーセント)		50	1 以上 99 以下

表 4.3: 標数 2 の体上 ECDSA 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
ドメインパラメータ生成	既約多項式の次数		283	16000 以下
	曲線のランダム性検証用 SEED のビット長		256	8 の倍数 かつ 16000 以下
	生成個数		10	10 以上
ドメインパラメータ検証	なし		–	–
鍵ペア生成	鍵の個数		10	10 以上
公開鍵検証	鍵の個数		12	12 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
署名生成	ハッシュ関数		SHA-256	SHA-224, SHA-256, SHA-384, SHA-512 , SHA-512/224 , SHA-512/256 のいずれか
	平文のビット長		1024	8 の倍数かつ 16000 以下
	試験 1	平文の数	15	15 以上
		いつも異なる署名が生成されることを検証するための署名の個数	2048	10 以上
	試験 2	平文の数	20	10 以上
署名検証	ハッシュ関数		SHA-256	SHA-224, SHA-256, SHA-384, SHA-512 , SHA-512/224 , SHA-512/256 のいずれか
	平文のビット長		1024	8 の倍数かつ 16000 以下
	平文の数		100	50 以上
	改ざんするデータの割合 (パーセント)		50	1 以上 99 以下

4.1.3 RSASSA-PKCS1-v1_5

表 4.4: RSASSA-PKCS1-v1_5 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
鍵ペア生成	鍵長	2048	2048 以上 16000 以下
	プライベート鍵のタイプ選択	CRT あり	CRT あり, CRT なし のいずれか
	公開鍵 e のタイプ選択	65537	65537, ランダム のいずれか
	鍵の個数	10	10 以上
署名生成	鍵長	2048	2048 以上 16000 以下
	プライベート鍵のタイプ選択	CRT あり	CRT あり, CRT なし のいずれか
	ハッシュ関数	SHA-256	SHA-224, SHA-256, SHA-384, SHA-512 , SHA-512/224, SHA-512/256 のいずれか
	平文のビット長	1024	8 の倍数かつ 16000 以下
	平文の数	2048	10 以上
署名検証	鍵長	2048	2048 以上 16000 以下
	公開鍵 e のタイプ選択	65537	65537, ランダム のいずれか
	ハッシュ関数	SHA-256	SHA-224, SHA-256, SHA-384, SHA-512 , SHA-512/224, SHA-512/256 のいずれか
	平文のビット長	1024	8 の倍数かつ 16000 以下
	平文の数	100	10 以上
	改ざんするデータの割合 (パーセント)	60	1 以上 99 以下

4.1.4 RSASSA-PSS

表 4.5: RSASSA-PSS 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
鍵ペア生成	鍵長	2048	2048 以上 16000 以下
	プライベート鍵のタイプ選択	CRT あり	CRT あり, CRT なし のいずれか
	公開鍵 *e* のタイプ選択	65537	65537, ランダム のいずれか
	鍵の個数	10	10 以上
署名生成	鍵長	2048	2048 以上 16000 以下
	プライベート鍵のタイプ選択	CRT あり	CRT あり, CRT なし のいずれか
	ハッシュ関数	SHA-256	SHA-224, SHA-256, SHA-384, SHA-512 , SHA-512/224, SHA-512/256 のいずれか
	マスク生成関数 *MGF*	ANSI X9.44 SHA-256	ANSI X9.44 SHA-224, SHA-256, SHA-384, SHA-512 , SHA-512/224, SHA-512/256 のいずれか
	salt のビット長	256	8 の倍数かつ 16000 以下
	平文のビット長	1024	8 の倍数かつ 16000 以下
	平文の数	2048	10 以上
	いつも異なる署名が生成されることを検証するための署名の個数	10	10 以上
署名検証	鍵長	2048	2048 以上 16000 以下
	公開鍵 *e* のタイプ選択	65537	65537, ランダム のいずれか
	ハッシュ関数	SHA-256	SHA-224, SHA-256, SHA-384, SHA-512 , SHA-512/224, SHA-512/256 のいずれか
	マスク生成関数 *MGF*	ANSI X9.44 SHA-256	ANSI X9.44 SHA-224, SHA-256, SHA-384, SHA-512 , SHA-512/224, SHA-512/256 のいずれか
	salt のビット長	256	8 の倍数かつ 16000 以下
	平文のビット長	1024	8 の倍数かつ 16000 以下
	平文の数	100	10 以上
	改ざんするデータの割合 (パーセント)	80	1 以上 99 以下

4.1.5 RSA-OAEP

表 4.6: RSA-OAEP 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
鍵ペア生成	鍵長	2048	2048 以上 16000 以下
	プライベート鍵のタイプ選択	CRT あり	CRT あり, CRT なし のいずれか
	公開鍵 e のタイプ選択	65537	65537, ランダム のいずれか
	鍵の個数	10	10 以上
暗号化	鍵長	2048	2048 以上 16000 以下
	公開鍵 e のタイプ選択	65537	65537, ランダム のいずれか
	ハッシュ関数	SHA-256	SHA-224, SHA-256, SHA-384, SHA-512 , SHA-512/224, SHA-512/256 のいずれか
	マスク生成関数 *MGF*	ANSI X9.44 SHA-256	ANSI X9.44 SHA-224, SHA-256, SHA-384, SHA-512 , SHA-512/224, SHA-512/256 のいずれか
	ラベル L のビット長	0	8 の倍数かつ 16000 以下
	平文のビット長	64	8 の倍数かつ 16000 以下
	平文の数	2048	10 以上
	暗号文の数	10	10 以上
復号	鍵長	2048	2048 以上 16000 以下
	プライベート鍵のタイプ選択	CRT あり	CRT あり, CRT なし のいずれか
	ハッシュ関数	SHA-256	SHA-224, SHA-256, SHA-384, SHA-512 , SHA-512/224, SHA-512/256 のいずれか
	マスク生成関数 *MGF*	ANSI X9.44 SHA-256	ANSI X9.44 SHA-224, SHA-256, SHA-384, SHA-512 , SHA-512/224, SHA-512/256 のいずれか
	ラベル L のビット長	0	8 の倍数かつ 16000 以下
	平文のビット長	64	8 の倍数かつ 16000 以下
	暗号文の数	100	10 以上
	改ざんするデータの割合 (パーセント)	60	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.

附 則
この手順は, 令和 4 年 8 月 10 日から施行し, 令和 4 年 8 月 10 日から適用する.

参考文献

[1] Internet Engineering Task Force (IETF), *PKCS #1: RSA Cryptography Specifications Version 2.2*, November, 2016. https://tools.ietf.org/html/rfc8017

[2] Accredited Standards Committee X9, Inc., *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*, ANS X9.62-2005, November 26, 2005.

[3] JCATT ファイルフォーマット仕様書 – 公開鍵 –, https://www.ipa.go.jp/security/jcmvp/documents/open/jcatt/format/jcatt_fileformat_a.zip

[4] JCATT サンプルファイル – 公開鍵 –, https://www.ipa.go.jp/security/jcmvp/documents/open/jcatt/sample/jcatt_sample_a.zip

改版履歴

識別番号	ATR-01-A

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 (選択可能な擬似乱数生成関数を記載, 及び誤植の訂正)
平成 30 年 6 月 22 日	櫻井・江口	一部改正 (承認されたセキュリティ機能の改正に伴い, DSA (FIPS 186-2) を DSA (FIPS 186-4) に変更すると共に,RSAES-PKCS1-v1_5 を削除し,RSASSA-PSS 及び RSA-OAEP の試験 2 を削除. DSA (FIPS 186-4) に対応して, 指定できるハッシュ関数に SHA-512/224, SHA-512/256 を追加. PKCS#1 v2.2 に対応して, 指定できるハッシュ関数に SHA-512/224, SHA-512/256 を追加. 確認書発行条件のうち, RSASSA-PKCS1-v1_5 及び RSASSA-PSS の署名生成及び署名検証, 並びに RSA-OAEP の暗号化及び復号の定量性パラメータを変更.)
令和元年 7 月 11 日	櫻井・江口	一部改正 (依存関係のある暗号アルゴリズムを記載及び誤植を訂正)
令和 4 年 8 月 10 日	佐伯・板垣・富田	一部改正 (承認されたセキュリティ機能の改正に伴い, RSASSA-PKCS1-v1_5 及び RSASSA-PSS における署名検証の鍵長を 2048 ビット以上へ変更すると共に, 署名及び守秘で使用するハッシュ関数から SHA-1 を削除. PKCS#1 v2.2 の参照先 URL を変更.)