

企業・個人の情報セキュリティ対策事業
暗号アルゴリズム実装試験ツールの機能追加

JCATT ファイルフォーマット仕様書

RSA-OAEP

2008 年 4 月

独立行政法人 情報処理推進機構

目 次

1	はじめに	3
2	RSA-OAEP	4
2.1	パラメータファイル (*.par)	6
2.2	リクエストファイル (*.req)	8
2.3	Facts ファイル (*.fax)	10
2.4	レスポンスファイル (*.rsp)	13
2.5	結果ファイル (*.out)	17

1 はじめに

暗号アルゴリズム実装試験ツール (以下 JCATT と略記する) が使用する各種ファイルのフォーマット規則を記述する。JCATT が使用するファイルには次のようなものがある。

ファイルの種類

- パラメータファイル (*.par)
試験項目の設定を記述する。JCATT を用いて作成する。
- リクエストファイル (*.req)
暗号モジュール開発ベンダに対する要求を記述する。JCATT を用いて作成する。
- Facts ファイル (*.fax)
テストベクタを記述する。JCATT を用いて作成する。
- レスponseファイル (*.rsp)
ベンダからの回答を記述する。リクエストファイルおよび本稿で指定するファイルフォーマットに基づいてベンダが作成する。
- 結果ファイル (*.out)
試験結果を記述する。JCATT を用いて作成する。

これらのファイルの名前は、次の規則に従ってつけること。

ファイル名の規則

- 拡張子は、上記 () 内に指定したものを使用すること。
- 拡張子以外の名前は、試験対象暗号モジュールごとに同じ名称をつけること。
リクエストファイル (*.req) と Facts ファイル (*.fax) の生成時には、リクエストファイル (*.req) と Facts ファイル (*.fax) に対してパラメータファイル (*.par) と同じ名称を JCATT が自動的につける。
試験実行時には、同じ名称のレスponseファイル (*.rsp) と Facts ファイル (*.fax) に対して試験が行われる。また、試験実行時は、結果ファイル (*.out) に対して、Facts ファイル (*.fax) と同じ名称を JCATT が自動的につける。

ファイルフォーマット詳細は次章以降に記述する。各ファイルに共通の規則は次の通りである。

共通規則

- [] で囲まれた“タグ”の次の行に値を記述する。
- タグは各ファイルフォーマットに記述した順番通りに記述すること。
- レスponseファイルにおいては【出力】と記述したタグが、試験対象モジュールが出力するデータを記述する箇所である。
- 半角英数字を用いること。
- タグおよび値は大文字小文字の区別をするので、大文字小文字を含めて正確に記述すること。ただし、数値を 16 進数で記述する場合は、大文字小文字は区別しない。
- 一文字目が # (半角) で始まるコメント行を自由に書き込むことができる。
- 平文、暗号文、鍵などのデータの区切り文字は改行 (CR+LF または LF) とする。
- 平文、暗号文、署名、鍵などのデータは 16 進表記とする。
- ビット数、個数などの数値は 10 進表記とする。
- ACSII コードを使用すること。
- 各行には必ず改行を入れること (最後のデータと EOF との間にも改行を入れること)。

2 RSA-OAEP

RSA-OAEP の暗号アルゴリズム実装試験のためのファイルフォーマットを記述する。各表において、試験方法に関する以下の略語を使用する。

- SMT: Short Messages Test
- SLMT: Selected Long Messages Test
- PGMT: Pseudorandomly Generated Messages Test
- RGT: Random Generation Test(「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。」に対する試験)

試験方法の詳細は，暗号アルゴリズム実装試験仕様書を参照のこと。

各表中，プライベート鍵識別子，公開鍵 e 識別子，擬似乱数生成関数識別子，マスク生成関数 (MGF) 識別子は下表の通りである。

表 1: プライベート鍵識別子

識別子	対応するプライベート鍵
TYPE1	プライベート鍵は $(p, q, dP, dQ, qInv)$
TYPE2	プライベート鍵は (d, n)

表 2: 公開鍵 e 識別子

識別子	対応する公開鍵 e
TYPE1	$e = 65,537$
TYPE2	e はランダム

表 3: 擬似乱数生成関数識別子

識別子	対応する擬似乱数生成関数
M_PRNG_ANSIX942_ANNEXC1_SHA1	PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1
M_PRNG_FIPS186_APPENDIX31_SHA1	PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1
M_PRNG_FIPS186_REVISIED_APPENDIX31_SHA1	PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1
M_PRNG_ISO18031_HASH	Hash_DRBG
M_PRNG_ISO18031_CTR	CTR_DRBG
M_PRNG_ISO18031_OFB	OFB_DRBG

表 4: マスク生成関数 (MGF) 識別子

MGF 識別子	対応する MGF
M_MGF_ANSI944_SHA1	ANSI X9.44 (SHA-1)
M_MGF_ANSI944_SHA256	ANSI X9.44 (SHA-256)
M_MGF_ANSI944_SHA384	ANSI X9.44 (SHA-384)
M_MGF_ANSI944_SHA512	ANSI X9.44 (SHA-512)

擬似乱数生成関数のパラメータ

擬似乱数生成関数のパラメータは、タグ [Parameter of PRNG] の下に、4 行 (各パラメータにつき 1 行) で以下の順で 16 進表記で記述する。ただし、*reseed counter* は 10 進数表記で記述する。

- PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1

- 1 行目：空行
- 2 行目：*XSEED*
- 3 行目：空行
- 4 行目：空行

- ISO18031 HASH DRBG

- 1 行目：ハッシュ関数識別子 (下表を参照のこと)
- 2 行目：*C*
- 3 行目：*additional input*
- 4 行目：*reseed counter*

- ISO18031 OFB DRBG

- 1 行目：ブロック暗号識別子 (下表を参照のこと)
- 2 行目：*KEY*
- 3 行目：*additional input*
- 4 行目：*reseed counter*

表 5: ハッシュ関数識別子

ハッシュ関数識別子	対応するハッシュ関数
M_Hash_SHA1	SHA-1
M_Hash_SHA256	SHA-256
M_Hash_SHA384	SHA-384
M_Hash_SHA512	SHA-512

表 6: ブロック暗号識別子

ブロック暗号識別子	対応するブロック暗号
M_BlockCipher_TDES	3-key Triple DES
M_BlockCipher_AES	AES

2.1 パラメータファイル (*.par)

表 7: RSA-OAEP パラメータファイル

機能	タグ	内容
(共通)	[Algorithm Name]	RSA-OAEP
暗号化	[Function Name]	Encryption
	[Bitlength of Modulus]	法 n のビット長
	[Secret Key Type]	プライベート鍵識別子
	[Public Key Type]	公開鍵 e 識別子
	[Seed P]	ランダムな平文を生成するための乱数シード
	[Bitlength of Seed P]	ランダムな平文を生成するための乱数シードのビット長
	[Seed K]	鍵ペア生成用乱数シード
	[Bitlength of Seed K]	鍵ペア生成用乱数シードのビット長
	[Hash]	ハッシュ関数識別子
	[MGF]	マスク生成関数識別子
	[Seed S]	変数 <i>seed</i> を生成するための擬似乱数生成関数用シード値 . <i>seed</i> とは , PKCS#1 v2.1 に記述されている EME-OAEP エンコーディングにおけるランダムオクテットストリングのことである .
	[Bitlength of Seed S] ¹	Seed S のビット長
	[L]	ラベル (L)
	[Bitlength of L]	ラベル (L) のビット長
	[Bitlength of S] ¹	変数 <i>seed</i> のビット長
	[Bitlength of Plaintexts]	平文のビット長
	[Number of Plaintexts]	平文の数
	[Number of Ciphertexts for RGT]	RGT で生成する暗号文の個数 .
	[PRNG]	擬似乱数生成関数識別子 (このタグは試験 2 の場合のみ記述する.)
	[Parameter of PRNG]	擬似乱数生成関数パラメータ (このタグは試験 2 の場合のみ記述する.)
復号	[Function Name]	Decryption
	[Bitlength of Modulus]	暗号化と同じ
	[Secret Key Type]	
	[Public Key Type]	
	[Seed P]	
	[Bitlength of Seed P]	
	[Seed K]	
	[Bitlength of Seed K]	
	[Hash]	
	[MGF]	
	[Seed S]	
	[Bitlength of Seed S]	
	[L]	
	[Bitlength of L]	
	[Bitlength of Plaintexts]	
	[Number of Ciphertexts]	
	[Rate of Fail Data]	復号失敗用データの割合

注

- この 2 つのタグで試験 1 , 2 , 3 のいずれを行うかを識別する .
 試験 1 を行う場合: [Bitlength of Seed S] と [Bitlength of S] 共に 0 の場合
 試験 2 を行う場合: [Bitlength of Seed S] が 0 でなく [Bitlength of S] が 0 の場合
 試験 3 を行う場合: [Bitlength of Seed S] と [Bitlength of S] 共に 0 でない場合
 上記以外の場合はエラーとする .

表 8: RSA-OAEP パラメータファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	RSA-OAEP
鍵ペア生成	[Function Name]	Key Generation
	[Bitlength of Modulus]	法 n のビット長
	[Secret Key Type]	プライベート鍵識別子
	[Public Key Type]	公開鍵 e 識別子
	[Number of Keys]	鍵の数

2.2 リクエストファイル (*.req)

表 9: RSA-OAEP リクエストファイル

機能	タグ g	内容
(共通)	[Algorithm Name]	RSA-OAEP
暗号化	[Function Name]	Encryption
	[Bitlength of Modulus]	法 n のビット長 [10 進数表記]
	[Hash]	ハッシュ関数識別子
	[MGF]	マスク生成関数識別子
	[n]	法 n [16 進数表記]
	[e]	公開鍵 e [16 進数表記]
	[L]	ラベル (L) [16 進数表記]
	[Bitlength of L]	ラベル (L) のビット長 [10 進数表記]
	[Seed S]	変数 $seed$ を生成するための擬似乱数生成関数用シード値 . $seed$ とは, PKCS#1 v2.1 に記述されている EME-OAEP エンコーディングにおけるランダムオクテットストリングのことである . [16 進数表記]
	[Bitlength of Seed S]	Seed S のビット長 [10 進数表記]
	[PRNG]	擬似乱数生成関数識別子 (このタグは試験 2 の場合のみ記述する.)
	[Parameter of PRNG]	擬似乱数生成関数パラメータ (このタグは試験 2 の場合のみ記述する.)
	[Bitlength of Plaintexts]	平文のビット長 [10 進数表記]
	[Bitlength of Ss]	変数 $seed$ のビット長 [10 進数表記]
	[Number of Plaintexts]	平文の数 [10 進数表記]
	[Plaintexts] ¹	平文 [16 進数表記]
	[Ss] ²	変数 $seed$ [16 進数表記]
	[Number of Ciphertexts for RGT]	RGT で生成する暗号文の個数 . このタグは試験 1 の場合のみ記述する . [10 進数表記]
復号	[Function Name]	Decryption
	[Bitlength of Modulus]	法 n のビット長 [10 進数表記]
	[Hash]	ハッシュ関数識別子
	[MGF]	マスク生成関数識別子
	[Secret Key Type]	プライベート鍵識別子
	[p] ³	素数 p [16 進数表記]
	[q] ³	素数 q [16 進数表記]
	[d] ³	プライベート鍵 d [16 進数表記]
	[n] ³	法 n [16 進数表記]
	[dP] ³	$d \bmod p - 1$ [16 進数表記]
	[dQ] ³	$d \bmod q - 1$ [16 進数表記]
	[qInv] ³	$q^{-1} \bmod p$ [16 進数表記]
	[L]	ラベル (L) [16 進数表記]
	[Bitlength of L]	ラベル (L) のビット長 [10 進数表記]
	[Bitlength of Plaintexts]	平文のビット長 [10 進数表記]
	[Number of Ciphertexts]	暗号文の数 [10 進数表記]
	[Ciphertexts] ⁴	暗号文 [16 進数表記]

注

1. [Number of Plaintexts] 個の平文を記述する .
2. 試験 3 の時のみ , [Number of Plaintexts] 個の変数 $seed$ を記述する .
3. プライベート鍵のタイプに応じて , ($[d],[n]$) の組または ($[p],[q],[dP],[dQ],[qInv]$) の組いずれか一方を記述する .
4. [Number of Ciphertexts] 個の暗号文を記述する .

表 10: RSA-OAEP リクエストファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	RSA-OAEP
鍵ペア生成	[Function Name]	Key Generation
	[Bitlength of Modulus]	法 n のビット長 [10 進数表記]
	[Secret Key Type]	プライベート鍵識別子
	[Public Key Type]	公開鍵 e 識別子
	[Number of Keys]	鍵の数 [10 進数表記]

2.3 Facts ファイル (*.fax)

表 11: RSA-OAEP Facts ファイル

機能	タグ	内容
(共通)	[Algorithm Name]	RSA-OAEP
暗号化	[Function Name]	Encryption
	[Bitlength of Modulus]	法 n のビット長
	[Hash]	ハッシュ関数識別子
	[MGF]	マスク生成関数識別子
	[Secret Key Type]	プライベート鍵識別子
	[Public Key Type]	公開鍵 e 識別子
	[p] ¹	素数 p
	[q] ¹	素数 q
	[d] ¹	プライベート鍵 d
	[n] ¹	法 n
	[dP] ¹	$d \bmod p - 1$
	[dQ] ¹	$d \bmod q - 1$
	[qInv] ¹	$q^{-1} \bmod p$
	[e]	公開鍵 e
	[L]	ラベル (L)
	[Bitlength of L]	ラベル (L) のビット長
	[Seed S]	変数 <i>seed</i> を生成するための擬似乱数生成関数用シード値 . <i>seed</i> とは , PKCS#1 v2.1 に記述されている EME-OAEP エンコーディングにおけるランダムオクテットストリングのことである .
	[Bitlength of Seed S]	Seed S のビット長
	[PRNG]	擬似乱数生成関数識別子 (このタグは試験 2 の場合のみ記述する.)
	[Parameter of PRNG]	擬似乱数生成関数パラメータ (このタグは試験 2 の場合のみ記述する.)
	[Bitlength of Plaintexts]	平文のビット長
	[Bitlength of Ss]	変数 <i>seed</i> のビット長
	[Number of Plaintexts]	平文の数
	[Plaintexts] ²	平文
	[Ss] ³	変数 <i>seed</i>
	[Ciphertexts] ²	暗号文
	[Number of Ciphertexts for RGT]	RGT で生成する暗号文の個数 . このタグは試験 1 の場合のみ記述する .

注

1. プライベート鍵識別子に応じて , ([d],[n]) の組または ([p],[q],[n],[dP],[dQ],[qInv]) の組いずれか一方を記述する .
2. [Number of Plaintexts] 個の平文および暗号文を記述する . ただし , 試験 1 の場合 , 暗号文は記述されない .
3. 試験 3 の時のみ , [Number of Plaintexts] 個の変数 *seed* を記述する .

表 12: RSA-OAEP Facts ファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	RSA-OAEP
復号	[Function Name]	Decryption
	[Bitlength of Modulus]	法 n のビット長
	[Hash]	ハッシュ関数識別子
	[MGF]	マスク生成関数識別子
	[Secret Key Type]	プライベート鍵識別子
	[Public Key Type]	公開鍵 e 識別子
	[p] ¹	素数 p
	[q] ¹	素数 q
	[d] ¹	プライベート鍵 d
	[n] ¹	法 n
	[dP] ¹	$d \bmod p - 1$
	[dQ] ¹	$d \bmod q - 1$
	[qInv] ¹	$q^{-1} \bmod p$
	[e]	公開鍵 e
	[L]	ラベル (L)
	[Bitlength of L]	ラベル (L) のビット長
	[Bitlength of Plaintexts]	平文のビット長
	[Number of Ciphertexts]	暗号文の数
	[Ciphertexts] ²	暗号文
	[Plaintexts] ²	平文

注

1. プライベート鍵識別子に応じて, $([d],[n])$ の組または $([p],[q],[n],[dP],[dQ],[qInv])$ の組いずれか一方を記述する .
2. [Number of Ciphertexts] 個の暗号文および平文を記述する . 復号に失敗した場合は, [Plaintexts] データの該当行に decryption error と記述する .

表 13: RSA-OAEP Facts ファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	RSA-OAEP
鍵ペア生成	[Function Name]	Key Generation
	[Bitlength of Modulus]	法 n のビット長
	[Secret Key Type]	プライベート鍵識別子
	[Public Key Type]	公開鍵 e 識別子
	[Number of Keys]	鍵の数

2.4 レスポンスファイル (*.rsp)

表 14: RSA-OAEP レスポンスファイル

機能	タグ	内容
(共通)	[Algorithm Name]	RSA-OAEP
暗号化	[Function Name]	Encryption
	[Bitlength of Modulus]	法 n のビット長 [10 進数表記]
	[Hash]	ハッシュ関数識別子
	[MGF]	マスク生成関数識別子
	[n]	法 n [16 進数表記]
	[e]	公開鍵 e [16 進数表記]
	[L]	ラベル (L) [16 進数表記]
	[Bitlength of L]	ラベル (L) のビット長 [10 進数表記]
	[Seed S]	変数 $seed$ を生成するための擬似乱数生成関数用シード値 . $seed$ とは , PKCS#1 v2.1 に記述されている EME-OAEP エンコーディングにおけるランダムオクテットストリングのことである . [16 進数表記]
	[Bitlength of Seed S]	Seed S のビット長 [10 進数表記]
	[PRNG]	擬似乱数生成関数識別子 (このタグは試験 2 の場合のみ記述する.)
	[Parameter of PRNG]	擬似乱数生成関数パラメータ (このタグは試験 2 の場合のみ記述する.)
	[Bitlength of Plaintexts]	平文のビット長 [10 進数表記]
	[Bitlength of Ss]	変数 $seed$ のビット長 [10 進数表記]
	[Number of Plaintexts]	平文の数 [10 進数表記]
	[Plaintexts] ¹	平文 [16 進数表記]
	[Ss] ²	変数 $seed$ [16 進数表記]
	[Ciphertexts] ¹	【出力】暗号文 [16 進数表記]
	[Number of Ciphertexts for RGT]	RGT で生成する暗号文の個数 . このタグは試験 1 の場合のみ記述する .
	[Ciphertexts for RGT] ³	【出力】RGT で生成された暗号文 . このタグは試験 1 の場合のみ記述する . [16 進数表記]

注

1. [Number of Plaintexts] 個の平文および暗号文を記述する .
2. 試験 3 の時のみ , [Number of Plaintexts] 個の変数 $seed$ を記述する .
3. [Plaintexts] データの 1 番目の平文を用いて生成した [Number of Ciphertexts for RGT] 個の暗号文 .

表 15: RSA-OAEP レスponseファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	RSA-OAEP
復号	[Function Name]	Decryption
	[Bitlength of Modulus]	法 n のビット長 [10 進数表記]
	[Hash]	ハッシュ関数識別子
	[MGF]	マスク生成関数識別子
	[Secret Key Type]	プライベート鍵識別子
	$[p]^2$	素数 p [16 進数表記]
	$[q]^2$	素数 q [16 進数表記]
	$[d]^2$	プライベート鍵 d [16 進数表記]
	$[n]^2$	法 n [16 進数表記]
	$[dP]^2$	$d \bmod p - 1$ [16 進数表記]
	$[dQ]^2$	$d \bmod q - 1$ [16 進数表記]
	$[qInv]^2$	$q^{-1} \bmod p$ [16 進数表記]
	[L]	ラベル (L) [16 進数表記]
	[Bitlength of L]	ラベル (L) のビット長 [10 進数表記]
	[Bitlength of Plaintexts]	平文のビット長 [10 進数表記]
	[Number of Ciphertexts]	暗号文の数 [10 進数表記]
	$[Ciphertexts]^2$	暗号文 [16 進数表記]
	$[Plaintexts]^2$	【出力】平文 [16 進数表記]

注

1. プライベート鍵識別子に応じて, $([d],[n])$ の組または $([p],[q],[dP],[dQ],[qInv])$ の組いずれか一方を記述する.
2. [Number of Ciphertexts] 個の暗号文および平文. 復号に失敗した場合は, [Plaintexts] データの該当行に decryption error と記述する.

表 16: RSA-OAEP レスポンスファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	RSA-OAEP
鍵ペア生成	[Function Name]	Key Generation
	[Bitlength of Modulus]	法 n のビット長 [10 進数表記]
	[Secret Key Type]	プライベート鍵識別子
	[Number of Keys]	鍵の数 [10 進数表記]
	$[p]^1$	【出力】素数 p [16 進数表記]
	$[q]^1$	【出力】素数 q [16 進数表記]
	$[d]^1$	【出力】プライベート鍵 d [16 進数表記]
	$[e]^1$	【出力】公開鍵 e [16 進数表記]
	$[n]^1$	【出力】法 n [16 進数表記]
	$[dP]^1$	【出力】 $d \bmod p - 1$ [16 進数表記]
	$[dQ]^1$	【出力】 $d \bmod q - 1$ [16 進数表記]
	$[qInv]^1$	【出力】 $q^{-1} \bmod p$ [16 進数表記]

注

1. プライベート鍵のタイプに応じて、 $([p], [q], [d], [e], [n])$ の組または $([p], [q], [dP], [dQ], [qInv], [e], [n])$ の組いずれか一方を [Number of Keys] 個記述する。

プライベート鍵識別子に TYPE1 が指定されているとき、鍵 $([p], [q], [dP], [dQ], [qInv], [e], [n])$ は次の例に従って記述すること。すなわち、2 組以上の鍵を記述する時は、まず 1 組目の $([p], [q], [dP], [dQ], [qInv], [e], [n])$ をこの順番で記述し、次に 2 組目の $([p], [q], [dP], [dQ], [qInv], [e], [n])$ をこの順番で記述する。(以降同様)

$[p]$

... # 1 組目の素数 p を記述する。

$[q]$

... # 1 組目の素数 q を記述する。

$[dP]$

... # 1 組目の $d \bmod p - 1$ を記述する。

$[dQ]$

... # 1 組目の $d \bmod q - 1$ を記述する。

$[qInv]$

... # 1 組目の $q^{-1} \bmod p$ を記述する。

$[e]$

... # 1 組目の公開鍵 e を記述する。

$[n]$

... # 1 組目の法 n を記述する。

$[p]$

... # 2 組目の素数 p を記述する。

$[q]$

... # 2 組目の素数 q を記述する。

$[dP]$

... # 2 組目の $d \bmod p - 1$ を記述する。

[dQ]
... # 2 組目の $d \bmod q - 1$ を記述する .

[qInv]
... # 2 組目の $q^{-1} \bmod p$ を記述する .

[e]
... # 2 組目の公開鍵 e を記述する .

[n]
... # 2 組目の法 n を記述する .

2.5 結果ファイル (*.out)

表 17: RSA-OAEP 結果ファイル

タグ	内容
[Algorithm Name]	暗号名
[Function Name]	試験対象機能名
[Results]	試験結果

注

- 試験合格の場合，[Results] に OK と表示される．
- 試験不合格の場合，[Results] に何らかの形式で NG と表示される．また，[Results] には，レスポンスファイル内の不合格となったデータが記述されているタグ名と，そのタグ内の何番目 (No.，#等の記号で番号を表す) のデータが不合格となったかが表示される．不合格となったデータが記述されているタグ名は，前記のレスポンスファイル仕様に【出力】と記述したタグである．ただし【出力】と記述したタグが1つしかない場合，タグ名は省略することがある．
- 鍵ペア生成機能に対する試験において試験不合格の場合，下記のようにどの条件が合格 (ok) でどの条件が不合格 (NG) となったかも表示される．
NG(#1 : p is prime ?)
ok(#1 : q is prime ?)
例えば，ok(#1 : q is prime ?) は， q は素数であるという条件を満たしていることを示し，NG(#1 : p is prime ?) は， p は素数であるという条件を満たしていないことを示す．詳細は別紙の試験項目を記述した文書を参照のこと．