

JCATT ファイルフォーマット仕様書

RSAES-PKCS1-v1_5

2 0 0 8 年 4 月 1 1 日

独立行政法人 情報処理推進機構

目 次

1	はじめに	1
2	RSAES-PKCS1-v1_5	2
2.1	パラメータファイル (*.par)	4
2.2	リクエストファイル (*.req)	6
2.3	Facts ファイル (*.fax)	8
2.4	レスポンスファイル (*.rsp)	10
2.5	結果ファイル (*.out)	13

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。
- レスポンスファイル (*.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、同じ名称のレスポンスファイル (*.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。
- レスポンス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 RSAES-PKCS1-v1_5

RSAES-PKCS1-v1_5 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。

- RGT: Random Generation Test(「同じ平文、同じ公開鍵に対して、複数(別途規定する数)暗号文を生成させた時、IUT が同じ暗号文を生成しないこと。」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。

識別子

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

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、*resseed 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：*resseed 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：*resseed counter*

表 4: 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 5: 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 6: RSAES-PKCS1-v1.5 パラメータファイル

機能	タグ	内容
(共通)	[Algorithm Name]	RSAES-PKCS1-v1.5
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．関数 M_RSA_Keygen の入力 x_{key} に対応する．関数 M_RSA_Keygen の仕様はモジュールインタフェース仕様書を参照のこと．
	[Bitlength of Seed K]	鍵ペア生成用乱数シードのビット長
	[Bitlength of PS] ¹	パディング列のビット長
	[Seed PS]	パディング列用乱数シード
	[Bitlength of Seed PS] ¹	パディング列用乱数シードのビット長
	[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.)

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 PS] と [Bitlength of PS] が共に 0 の場合
 試験 2 を行う場合: [Bitlength of Seed PS] が 0 でなく [Bitlength of PS] が 0 の場合
 試験 3 を行う場合: [Bitlength of Seed PS] と [Bitlength of PS] が共に 0 でない場合
 上記以外の場合はエラーとする．

表 7: RSAES-PKCS1-v1.5 パラメータファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	RSAES-PKCS1-v1.5
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]	
	[Seed PS]	
	[Bitlength of Seed PS]	
	[Bitlength of Plaintexts]	
	[Number of Ciphertexts]	
	[Rate of Fail Data]	復号失敗用データの割合
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 8: RSAES-PKCS1-v1_5 リクエストファイル

機能	タグ	内容
(共通)	[Algorithm Name]	RSAES-PKCS1-v1_5
暗号化	[Function Name]	Encryption
	[Bitlength of Modulus]	法 n のビット長 [10 進数表記]
	[n]	法 n [16 進数表記]
	[e]	公開鍵 e [16 進数表記]
	[Bitlength of Plaintexts]	平文のビット長 [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]
	[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]
	[PS]	パディング列 [16 進数表記]
	[Bitlength of PS]	パディング列のビット長 [10 進数表記]
	[Seed PS]	パディング列用乱数シード [16 進数表記]
	[Bitlength of Seed PS]	パディング列用乱数シードのビット長 [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.)

注

1. [Number of Plaintexts] 個の平文を記述する .

表 9: RSAES-PKCS1-v1.5 リクエストファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	RSAES-PKCS1-v1.5
復号	[Function Name]	Decryption
	[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
	[p] ¹	素数 p [16 進数表記]
	[q] ¹	素数 q [16 進数表記]
	[d] ¹	プライベート鍵 d [16 進数表記]
	[n] ¹	法 n [16 進数表記]
	[dP] ¹	$d \bmod p - 1$ [16 進数表記]
	[dQ] ¹	$d \bmod q - 1$ [16 進数表記]
	[qInv] ¹	$q^{-1} \bmod p$ [16 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]
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]

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] 個の暗号文を記述する.

2.3 Facts ファイル (*.fax)

表 10: RSAES-PKCS1-v1_5 Facts ファイル

機能	タグ	内容
(共通)	[Algorithm Name]	RSAES-PKCS1-v1_5
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
	[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
	[Bitlength of Plaintexts]	平文のビット長
	[Number of Plaintexts]	平文の数
	[Plaintexts] ²	平文
	[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.)
	[PS]	パディング列
	[Bitlength of PS]	パディング列のビット長
	[Seed PS]	パディング列用乱数シード
	[Bitlength of Seed PS]	パディング列用乱数シードのビット長
	[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.)

注

1. プライベート鍵のタイプに応じて, $([d],[n])$ 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.

表 11: RSAES-PKCS1-v1_5 Facts ファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	RSAES-PKCS1-v1_5
復号	[Function Name]	Decryption
	[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
	[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
	[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
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

注

1. プライベート鍵のタイプに応じて, $([d],[n])$ 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] 個の平文および暗号文を記述する. 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.

2.4 レスポンスファイル (*.rsp)

表 12: RSAES-PKCS1-v1.5 レスポンスファイル

機能	タグ	内容
(共通)	[Algorithm Name]	RSAES-PKCS1-v1.5
暗号化	[Function Name]	Encryption
	[Bitlength of Modulus]	法 n のビット長 [10 進数表記]
	[n]	法 n [16 進数表記]
	[e]	公開鍵 e [16 進数表記]
	[Bitlength of Plaintexts]	平文のビット長 [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]
	[Ciphertexts] ¹	【出力】暗号文 [16 進数表記]
	[PS]	パディング列 [16 進数表記]
	[Bitlength of PS]	パディング列のビット長 [10 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]
	[Ciphertexts for RGT] ²	【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]
	[Seed PS]	パディング列用乱数シード [16 進数表記]
	[Bitlength of Seed PS]	パディング列用乱数シードのビット長 [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.)

注

1. [Number of Plaintexts] 個の平文および暗号文を記述する .
2. [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 13: RSAES-PKCS1-v1_5 レスponseファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	RSAES-PKCS1-v1_5
復号	[Function Name]	Decryption
	[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
	$[p]^1$	素数 p [16 進数表記]
	$[q]^1$	素数 q [16 進数表記]
	$[d]^1$	プライベート鍵 d [16 進数表記]
	$[n]^1$	法 n [16 進数表記]
	$[dP]^1$	$d \bmod p - 1$ [16 進数表記]
	$[dQ]^1$	$d \bmod q - 1$ [16 進数表記]
	$[qInv]^1$	$q^{-1} \bmod p$ [16 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]
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]
	$[p]^3$	【出力】素数 p [16 進数表記]
	$[q]^3$	【出力】素数 q [16 進数表記]
	$[d]^3$	【出力】プライベート鍵 d [16 進数表記]
	$[e]^3$	【出力】公開鍵 e [16 進数表記]
	$[n]^3$	【出力】法 n [16 進数表記]
	$[dP]^3$	【出力】 $d \bmod p - 1$ [16 進数表記]
	$[dQ]^3$	【出力】 $d \bmod q - 1$ [16 進数表記]
	$[qInv]^3$	【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、 $([d], [n])$ 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] 個の平文および暗号文。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。
3. 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 14: RSAES-PKCS1-v1.5 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．