

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

DSA FIPS 186-2

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	DSA FIPS 186-2	4
2.1	パラメータファイル (*.par)	5
2.2	リクエストファイル (*.req)	7
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)	12

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 DSA FIPS 186-2

DSA FIPS 186-2 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。」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，ハッシュ関数識別子は下表の通りである。

表 1: 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

複数のドメインパラメータを記述する場合は，SEED 値，counter 値を，以下のように各ドメインパラメータ [PQG] の直後に記述する。

[PQG]

... # 1 つ目のドメインパラメータを記述する。

[SEED]

... # 1 つ目のドメインパラメータ生成に使用された SEED 値を記述する。

[counter]

... # 1 つ目のドメインパラメータ生成に使用された counter を記述する。

[PQG]

... # 2 つ目のドメインパラメータを記述する。

[SEED]

... # 2 つ目のドメインパラメータ生成に使用された SEED 値を記述する。

[counter]

... # 2 つ目のドメインパラメータ生成に使用された counter を記述する。

2.1 パラメータファイル (*.par)

表 2: DSA FIPS 186-2 パラメータファイル

機能	タグ	内容
(共通)	[Algorithm Name]	DSA FIPS 186-2
ドメインパラメータ 生成	[Function Name]	Domain Parameter Generation
	[Validation Method]	試験項目の指定 . 1 と記述すること .
	[Bitlength of p]	法 p のビット長
	[Bitlength of q]	q のビット長
	[Bitlength of SEED]	p, q 生成用乱数シードのビット長
	[Number of PQG Sets]	ドメインパラメータ (p, q, g) の個数
ドメインパラメータ 検証	[Function Name]	Domain Parameter Validation
	[Validation Method]	試験項目の指定 . 1 と記述すること .
	[Bitlength of p]	法 p のビット長
	[Bitlength of q]	q のビット長
	[Bitlength of SEED]	p, q 生成用乱数シードのビット長
	[Number of PQG Sets]	ドメインパラメータ (p, q, g) の個数
	[Seed S]	SEED 生成のための擬似乱数生成関数 用乱数シード
	[Bitlength of Seed S]	Seed S のビット長
	[Rate of Fail Data]	ドメインパラメータ検証が不合格になる 割合
鍵ペア生成	[Function Name]	Key Generation
	[Bitlength of p]	法 p のビット長
	[Bitlength of q]	q のビット長
	[Bitlength of SEED]	p, q 生成用乱数シードのビット長
	[Seed S]	SEED 生成のための擬似乱数生成関数 用乱数シード
	[Bitlength of Seed S]	Seed S のビット長
	[Number of XY Sets]	生成する x, y ペアの個数

表 3: DSA FIPS 186-2 パラメータファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	DSA FIPS 186-2
署名生成	[Function Name]	Sign
	[Bitlength of p]	法 p のビット長
	[Bitlength of q]	q のビット長
	[Bitlength of SEED]	p, q 生成用乱数シードのビット長
	[Seed S]	SEED 生成のための擬似乱数生成関数 用乱数シード
	[Bitlength of Seed S]	Seed S のビット長
	[Seed P]	ランダムな平文を生成するための擬似乱 数生成関数用乱数シード
	[Bitlength of Seed P]	Seed P のビット長
	[Seed K]	鍵ペア生成のための擬似乱数生成関数用 乱数シード
	[Bitlength of Seed K]	Seed K のビット長
	[Hash]	ハッシュ関数識別子 . 常に M_Hash_SHA1 と記述する .
	[Bitlength of Plaintexts]	平文のビット長
	[Number of Plaintexts]	平文の数
	[Number of Signatures for RGT]	RGT で生成する署名の個数 .
署名検証	[Function Name]	Verification
	[Bitlength of p]	署名生成と同じ
	[Bitlength of q]	
	[Bitlength of SEED]	
	[Seed S]	
	[Bitlength of Seed S]	
	[Seed P]	
	[Bitlength of Seed P]	
	[Seed K]	
	[Bitlength of Seed K]	
	[Hash]	
	[Bitlength of Plaintexts]	
	[Number of Plaintexts]	
	[Seed of Ephemeral Keys]	一時秘密鍵 k を生成するための擬似乱数 生成関数用乱数シード
	[Bitlength of Seed of Ephemeral Keys]	Seed of Ephemeral Keys のビット長
	[Rate of Fail Data]	署名検証が不合格になる割合

2.2 リクエストファイル (*.req)

表 4: DSA FIPS 186-2 リクエストファイル

機能	タグ	内容
(共通)	[Algorithm Name]	DSA FIPS 186-2
ドメインパラメータ生成	[Function Name]	Domain Parameter Generation
	[Validation Method]	試験項目の指定 [10 進数表記]
	[Bitlength of p]	法 p のビット長 [10 進数表記]
	[Bitlength of q]	q のビット長 [10 進数表記]
	[Bitlength of SEED]	SEED のビット長 [10 進数表記]
	[Number of PQG Sets]	ドメインパラメータ (p, q, g) の個数 [10 進数表記]
ドメインパラメータ検証	[Function Name]	Domain Parameter Validation
	[Validation Method]	試験項目の指定 [10 進数表記]
	[Bitlength of p]	法 p のビット長 [10 進数表記]
	[Bitlength of q]	q のビット長 [10 進数表記]
	[Bitlength of SEED]	SEED のビット長 [10 進数表記]
	[Number of PQG Sets]	ドメインパラメータ (p, q, g) の個数 [10 進数表記]
	[PQG] ¹	ドメインパラメータ p, q, g [16 進数表記]
	[SEED] ¹	p, q 生成用乱数シード [16 進数表記]
鍵ペア生成	[Function Name]	Key Generation
	[Bitlength of p]	法 p のビット長 [10 進数表記]
	[Bitlength of q]	q のビット長 [10 進数表記]
	[PQG]	ドメインパラメータ p, q, g [16 進数表記]
	[Number of XY Sets]	生成する x, y ペアの個数 [10 進数表記]
署名生成	[Function Name]	Sign
	[Bitlength of p]	法 p のビット長 [10 進数表記]
	[Bitlength of q]	q のビット長 [10 進数表記]
	[PQG]	ドメインパラメータ p, q, g [16 進数表記]
	[Hash]	ハッシュ関数識別子 . 常に M.Hash_SHA1 と記述する .
	[Private Key]	プライベート鍵 [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] ²	平文 [16 進数表記]
	[Number of Signatures for RGT]	RGT で生成する署名の個数 . [10 進数表記]
署名検証	[Function Name]	Verification
	[Bitlength of p]	署名生成と同じ
	[Bitlength of q]	
	[PQG]	
	[Hash]	
	[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]
	[Public Keys]	公開鍵 [16 進数表記]
	[Plaintexts] ²	平文 [16 進数表記]
	[Signatures] ²	署名. 1 つの署名を r と s の順に 1 行で記述する . [16 進数表記]

注

1. 前述のフォーマットにしたがって [Number of PQG Sets] 個の [PQG] , [SEED] , [counter] を記述する .
2. [Number of Plaintexts] 個の平文 (1 行につき 1 つの平文) および署名 (1 行につき 1 つの署名) を記述する .

2.3 Facts ファイル (*.fax)

表 5: DSA FIPS 186-2 Facts ファイル

機能	タグ	内容
(共通)	[Algorithm Name]	DSA FIPS 186-2
ドメインパラメータ生成	[Function Name]	Domain Parameter Generation
	[Validation Method]	試験項目の指定
	[Bitlength of p]	法 p のビット長
	[Bitlength of q]	q のビット長
	[Bitlength of SEED]	SEED のビット長
	[Number of PQG Sets]	ドメインパラメータ (p, q, g) の個数
ドメインパラメータ検証	[Function Name]	Domain Parameter Validation
	[Validation Method]	試験項目の指定
	[Bitlength of p]	法 p のビット長
	[Bitlength of q]	q のビット長
	[Bitlength of SEED]	SEED のビット長
	[Number of PQG Sets]	ドメインパラメータ (p, q, g) の個数
	[PQG] ¹	ドメインパラメータ p, q, g
	[SEED] ¹	p, q 生成用乱数シード
	[counter] ¹	p, q 生成用カウンタ
	[Result]	ドメインパラメータ検証結果．検証合格の時 0，不合格の時 1 と記述する．
鍵ペア生成	[Function Name]	Key Generation
	(鍵ペア生成リクエストファイルと同じ)	

注

1. 前述のフォーマットにしたがって [Number of PQG Sets] 個の [PQG] , [SEED] , [counter] , [Result] を記述する．

表 6: DSA FIPS 186-2 Facts ファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	DSA FIPS 186-2
署名生成	[Function Name]	Sign
	[Bitlength of p]	法 p のビット長
	[Bitlength of q]	q のビット長
	[PQG]	ドメインパラメータ p, q, g
	[Hash]	ハッシュ関数識別子 . 常に M.Hash_SHA1 と記述する .
	[Private Key]	プライベート鍵
	[Public Key]	公開鍵
	[Bitlength of Plaintexts]	平文のビット長
	[Number of Plaintexts]	平文の数
	[Plaintexts] ¹	平文
	[Number of Signatures for RGT]	RGT で生成する署名の個数 .
署名検証	[Function Name]	Verification
	[Bitlength of p]	署名生成と同じ
	[Bitlength of q]	
	[PQG]	
	[Hash]	
	[Private Key]	プライベート鍵
	[Bitlength of Plaintexts]	平文のビット長
	[Number of Plaintexts]	平文の数
	[Public Keys] ²	公開鍵
	[Plaintexts] ²	平文
	[Signatures] ²	署名. 1 つの署名を r と s の順に 1 行で記述する .
	[Results] ²	署名検証結果 . 検証合格の時 0 , 不合格の時 1 と記述する .

注

1. [Number of Plaintexts] 個の平文 (1 行につき 1 つの平文) を記述する .
2. [Number of Plaintexts] 個の公開鍵 (1 行につき 1 つの公開鍵) , 平文 (1 行につき 1 つの平文) , 署名 (1 行につき 1 つの署名) , および署名検証結果 (1 行につき 1 つの署名検証結果) を記述する .

2.4 レスponseファイル (*.rsp)

表 7: DSA FIPS 186-2 レスponseファイル

機能	タグ	内容
(共通)	[Algorithm Name]	DSA FIPS 186-2
ドメインパラメータ生成	[Function Name]	Domain Parameter Generation
	[Validation Method]	試験項目の指定 [10 進数表記]
	[Bitlength of p]	法 p のビット長 [10 進数表記]
	[Bitlength of q]	q のビット長 [10 進数表記]
	[Bitlength of SEED]	SEED のビット長 [10 進数表記]
	[Number of PQG Sets]	ドメインパラメータ (p, q, g) の個数 [10 進数表記]
	[PQG] ¹	【出力】ドメインパラメータ p, q, g [16 進数表記]
	[SEED] ¹	【出力】 p, q 生成用乱数シード [16 進数表記]
ドメインパラメータ検証	[Function Name]	Domain Parameter Validation
	[Validation Method]	試験項目の指定 [10 進数表記]
	[Bitlength of p]	法 p のビット長 [10 進数表記]
	[Bitlength of q]	q のビット長 [10 進数表記]
	[Bitlength of SEED]	SEED のビット長 [16 進数表記]
	[Number of PQG Sets]	ドメインパラメータ (p, q, g) の個数 [10 進数表記]
	[PQG] ²	ドメインパラメータ p, q, g [16 進数表記]
	[SEED] ²	p, q 生成用乱数シード [16 進数表記]
鍵ペア生成	[Function Name]	Key Generation
	[Bitlength of p]	法 p のビット長 [10 進数表記]
	[Bitlength of q]	q のビット長 [10 進数表記]
	[PQG]	ドメインパラメータ p, q, g [16 進数表記]
	[Number of XY Sets]	生成する x, y ペアの個数 [10 進数表記]
	[XY] ³	【出力】生成された x, y [16 進数表記]

注

1. 前述のフォーマットにしたがって [Number of PQG Sets] 個の [PQG] , [SEED] , [counter] を記述する .
2. 前述のフォーマットにしたがって [Number of PQG Sets] 個の [PQG] , [SEED] , [counter] , [Result] を記述する .
3. [Number of XY Sets] 個のタグ [XY] を記述し , 各タグ [XY] にはプライベート鍵 x と公開鍵 y を x, y の順に 2 行で記述する .

[XY]

... # 1 つ目のプライベート鍵 x を記述する .

... # 1 つ目の公開鍵 y を記述する .

[XY]

... # 2 つ目のプライベート鍵 x を記述する .

... # 2 つ目の公開鍵 y を記述する .

表 8: DSA FIPS 186-2 レスポンスファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	DSA FIPS 186-2
署名生成	[Function Name]	Sign
	[Bitlength of p]	法 p のビット長 [10 進数表記]
	[Bitlength of q]	q のビット長 [10 進数表記]
	[PQG]	ドメインパラメータ p, q, g [16 進数表記]
	[Hash]	ハッシュ関数識別子 . 常に M.Hash.SHA1 と記述すること .
	[Private Key]	プライベート鍵 [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]
	[Signatures] ¹	【出力】署名. 1 つの署名を r と s の順に 1 行で記述する . [16 進数表記]
	[Number of Signatures for RGT]	RGT で生成する署名の個数 . [10 進数表記]
	[Signatures for RGT] ²	【出力】RGT で生成された 署名. 1 つの署名を r と s の順に 1 行で記述する . [16 進数表記]
署名検証	[Function Name]	Verification
	[Bitlength of p]	署名生成と同じ
	[Bitlength of q]	
	[PQG]	
	[Hash]	
	[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]
	[Public Keys] ³	公開鍵 [16 進数表記]
	[Plaintexts] ³	平文 [16 進数表記]
	[Signatures] ³	署名. 1 つの署名を r と s の順に 1 行で記述する . [16 進数表記]
	[Results] ³	【出力】署名検証結果 . 検証合格の時 0 , 不合格の時 1 と記述する .

注

1. [Number of Plaintexts] 個の平文 (1 行につき 1 つの平文) , 署名 (1 行につき 1 つの署名) 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 Signatures for RGT] 個の署名データ .
3. [Number of Plaintexts] 個の公開鍵 (1 行につき 1 つの公開鍵) , 平文 (1 行につき 1 つの平文) , 署名 (1 行につき 1 つの署名) , および署名検証結果 (1 行につき 1 つの署名検証結果) を記述する . 例えば , [Number of Plaintexts] が 2 の場合 , [Public Keys] データの 1 番目 , [Plaintexts] データの 1 番目 , [Signatures] データの 1 番目を用いて署名検証した結果を , [Results] データの 1 番目に記述し , [Public Keys] データの 2 番目 , [Plaintexts] データの 2 番目 , [Signatures] データの 2 番目を用いて署名検証した結果を , [Results] データの 2 番目に記述する .

2.5 結果ファイル (*.out)

表 9: DSA FIPS 186-2 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，どの条件で不合格 (NG) となったかも表示される．
NG(#10 : $y = g^x \bmod p$?)
NG(#10 : $1 \leq x \leq q-1, 1 \leq y \leq p-2$?)
NG(#10 : $y^q = 1 \bmod p$?)
例えば，NG(#10 : $y = g^x \bmod p$?) は，公開鍵 y ，プライベート鍵 x ，ドメインパラメータ p, g が満たすべき条件 $y = g^x \bmod p$ を満たしていないことを意味する．詳細は別紙の試験項目を記述した文書を参照のこと．