JCATTファイルフォーマット仕様書

DSA

２００８年1月１８日

独立行政法人　情報処理推進機構

目 次

1　はじめに

暗号アルゴリズム試験ツール (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

DSA アルゴリズム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

試験方法の詳細は，暗号アルゴリズム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 パラメータファイル

機能	タグ	内容
(共通)	[Algorithm Name]	DSA
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 パラメータファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	DSA
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 リクエストファイル

機能	タグ	内容
(共通)	[Algorithm Name]	DSA
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][1]	ドメインパラメータ (p, q, g) の個数
	[PQG]	ドメインパラメータ p, q, g
	[SEED]	p, q 生成用乱数シード
	[counter]	p, q 生成用カウンタ
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
	[PQG]	ドメインパラメータ p, q, g
	[Number of XY Sets]	生成する x, y ペアの個数
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
	[Bitlength of Plaintexts]	平文のビット長
	[Number of Plaintexts]	平文の数
	[Plaintexts][2]	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]	
	[Bitlength of Plaintexts]	平文のビット長
	[Number of Plaintexts]	平文の数
	[Public Keys]	公開鍵
	[Plaintexts][2]	平文
	[Signatures][2]	署名

注

1. 前述のフォーマットにしたがって [Number of PQG Sets] 個のドメインパラメータを記述する．
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 Facts ファイル

機能	タグ	内容
(共通)	[Algorithm Name]	DSA
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][1]	ドメインパラメータ (p, q, g) の個数
	[PQG]	ドメインパラメータ p, q, g
	[SEED]	p, q 生成用乱数シード
	[counter]	p, q 生成用カウンタ
	[Results]	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] 個のドメインパラメータおよび [Results] を記述する．

表 6: DSA Facts ファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	DSA
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
	[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 レスポンスファイル (*.rsp)

表 7: DSA レスポンスファイル

機能	タグ	内容
(共通)	[Algorithm Name]	DSA
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][1]	ドメインパラメータ (p, q, g) の個数
	[PQG]	ドメインパラメータ p, q, g
	[SEED]	p, q 生成用乱数シード
	[counter]	p, q 生成用カウンタ
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][1]	ドメインパラメータ (p, q, g) の個数
	[PQG]	ドメインパラメータ p, q, g
	[SEED]	p, q 生成用乱数シード
	[counter]	p, q 生成用カウンタ
	[Results]	【出力】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
	[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
	[Number of XY Sets]	生成する x, y ペアの個数
	[XY][2]	【出力】生成された x, y

注

1. 前述のフォーマットにしたがって [Number of PQG Sets] 個のドメインパラメータおよび [Results] を記述する.
2. [Number of Keys] 個の鍵 (1 行につき 1 つの鍵) を記述する.

表 8: DSA レスポンスファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	DSA
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 と記述すること．
	[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
	[Plaintexts][1]	平文
	[Signatures][1]	【出力】署名
	[Number of Signatures for RGT][2]	RGT で生成する署名の個数.
	[Signatures for RGT]	【出力】RGT で生成された署名
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
	[Number of Plaintexts]	平文の数
	[Public Keys][3]	公開鍵
	[Plaintexts][3]	平文
	[Signatures][3]	署名
	[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) 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．

2.5 結果ファイル (*.out)

表 9: DSA 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 mod p ?)
  NG(#10 : 1 <= x <= q-1, 1 <= y <= p-2 ?)
  NG(#10 : y∧q = 1 mod p ?)
  例えば，NG(#10 : y = g∧x mod 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．