2007 情財第 866 号

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

DH(dhStatic, dhEphem, dhOneFlow)

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

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 DH(dhStatic, dhEphem, dhOneFlow)

dhStatic，dhEphem，dhOneFlow 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．これらの DH に対するファイルフォーマットは，`Algorithm Name` の他は同じである．

`Algorithm Name` は，それぞれ下記の通り．

- DH dhStatic
- DH dhEphem
- DH dhOneFlow

各表中，鍵導出関数識別子は下表の通りである．

表 1: 鍵導出関数識別子

識別子	対応する鍵導出関数
M_Kdf_ANSI942_771SHA1	ANSI X9.42 KDF with SHA-1 based on ASN.1
M_Kdf_ANSI942_771SHA224	ANSI X9.42 KDF with SHA-224 based on ASN.1
M_Kdf_ANSI942_771SHA256	ANSI X9.42 KDF with SHA-256 based on ASN.1
M_Kdf_ANSI942_771SHA384	ANSI X9.42 KDF with SHA-384 based on ASN.1
M_Kdf_ANSI942_771SHA512	ANSI X9.42 KDF with SHA-512 based on ASN.1
M_Kdf_ANSI942_772SHA1	ANSI X9.42 KDF with SHA-1 based on Concatenation
M_Kdf_ANSI942_772SHA224	ANSI X9.42 KDF with SHA-224 based on Concatenation
M_Kdf_ANSI942_772SHA256	ANSI X9.42 KDF with SHA-256 based on Concatenation
M_Kdf_ANSI942_772SHA384	ANSI X9.42 KDF with SHA-384 based on Concatenation
M_Kdf_ANSI942_772SHA512	ANSI X9.42 KDF with SHA-512 based on Concatenation

複数のドメインパラメータを記述する場合は，$SEED$ 値，pgenCounter 値，および h 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． [16 進数表記]
[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． [16 進数表記]
[pgenCounter]
. . . ♯ 1 つ目のドメインパラメータ生成に使用された pgenCounter を記述する． [10 進数表記]
[h]
. . . ♯ 1 つ目のドメインパラメータ生成に使用された h を記述する． [16 進数表記]
[PQG]
. . . ♯ 2 つ目のドメインパラメータを記述する． [16 進数表記]
[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． [16 進数表記]
[pgenCounter]
. . . ♯ 2 つ目のドメインパラメータ生成に使用された pgenCounter を記述する． [10 進数表記]
[h]
. . . ♯ 2 つ目のドメインパラメータ生成に使用された h を記述する． [16 進数表記]

2.1 パラメータファイル (*.par)

表 2: DH(dhStatic, dhEphem, dhOneFlow) パラメータファイル

機能	タグ	内容
(共通)	[Algorithm Name]	(アルゴリズム名)
鍵共有	[Function Name]	Key Sharing
	[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 x]	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 x]	Seed x のビット長
	[KDF]	鍵導出関数識別子
	[Otherinfo for KDF]	鍵導出関数への入力用データ Otherinfo
	[Bitlength of Otherinfo for KDF]	鍵導出関数への入力用データ Otherinfo のビット長
	[Bitlength of Keying Data]	共有する鍵のビット長
	[Number of Keying Datas]	共有する鍵の個数
公開鍵検証	[Function Name]	Public Key Validation
	[Bitlength of p]	鍵共有と同じ
	[Bitlength of q]	
	[Bitlength of SEED]	
	[Seed S]	
	[Bitlength of Seed S]	
	[Seed x]	
	[Bitlength of Seed x]	
	[Number of Public Keys]	生成する公開鍵の個数
	[Rate of Fail Data]	公開鍵検証が不合格になる割合
鍵ペア生成	[Function Name]	Key Generation
	[Bitlength of p]	鍵共有と同じ
	[Bitlength of q]	
	[Bitlength of SEED]	
	[Seed S]	
	[Bitlength of Seed S]	
	[Number of XY Sets]	生成するプライベート鍵 x と公開鍵 y ペアの個数

表 3: DH(dhStatic, dhEphem, dhOneFlow) パラメータファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	(アルゴリズム名)
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, 2 のいずれか 1 つを記述する.
	[Bitlength of p]	鍵共有と同じ
	[Bitlength of q]	
	[Bitlength of SEED]	
	[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, 2 のいずれか 1 つを記述する.
	[Bitlength of p]	鍵共有と同じ
	[Bitlength of q]	
	[Bitlength of SEED]	
	[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]	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: DH(dhStatic, dhEphem, dhOneFlow) リクエストファイル

機能	タグ	内容
(共通)	[Algorithm Name]	(アルゴリズム名)
鍵共有	[Function Name]	Key Sharing
	[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]
	[KDF]	鍵導出関数識別子
	[Otherinfo for KDF]	鍵導出関数への入力用データ Otherinfo [16 進数表記]
	[Bitlength of Otherinfo for KDF]	鍵導出関数への入力用データ Otherinfo のビット長 [10 進数表記]
	[Bitlength of Keying Data]	共有する鍵のビット長 [10 進数表記]
	[Number of Keying Datas]	共有する鍵の個数 [10 進数表記]
	[x][1]	鍵共有者のプライベート鍵 x [16 進数表記]
	[y][1]	鍵共有対象者の公開鍵 y [16 進数表記]
公開鍵検証	[Function Name]	Public Key Validation
	[Bitlength of p]	鍵共有と同じ
	[Bitlength of q]	
	[PQG]	
	[Number of Public Keys]	生成する公開鍵の個数 [10 進数表記]
	[y][2]	公開鍵 y [16 進数表記]
鍵ペア生成	[Function Name]	Key Generation
	[Bitlength of p]	鍵共有と同じ
	[Bitlength of q]	
	[PQG]	
	[Number of XY Sets]	生成するプライベート鍵 x と公開鍵 y ペアの個数 [10 進数表記]
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．1，2 のいずれか 1 つを記述する．
	[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]

注

1. [Number of Keying Datas] 個の各鍵を以下のように記述する.

   [x]
   . . . ♯ 1 つ目のプライベート鍵を記述する.

   [y]
   . . . ♯ 1 つ目の公開鍵を記述する.

   [x]
   . . . ♯ 2 つ目のプライベート鍵を記述する.

   [y]
   . . . ♯ 2 つ目の公開鍵を記述する.

2. [Number of Public Keys] 個の公開鍵 y を以下のように記述する.

   [y]
   . . . ♯ 1 つ目の公開鍵を記述する.

   [y]
   . . . ♯ 2 つ目の公開鍵を記述する.

表 5: DH(dhStatic, dhEphem, dhOneFlow) リクエストファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	(アルゴリズム名)
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．1，2 のいずれか 1 つを記述する．
	[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][1]	ドメインパラメータ (p, q, g) の個数 [10 進数表記]
	[PQG]	ドメインパラメータ p, q, g [16 進数表記]
	[SEED]	p, q 生成用乱数シード [16 進数表記]
	[pgenCounter]	p, q 生成用カウンタ [10 進数表記]
	[h]	h [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]，[pgenCounter]，[h] を記述する．ただし，[h] は試験 2 を行う時のみ記述する．

2.3 Facts ファイル (*.fax)

表 6: DH(dhStatic, dhEphem, dhOneFlow) Facts ファイル

機能	タグ	内容
(共通)	[Algorithm Name]	(アルゴリズム名)
鍵共有	[Function Name]	Key Sharing
	[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
	[KDF]	鍵導出関数識別子
	[Otherinfo for KDF]	鍵導出関数への入力用データ Otherinfo
	[Bitlength of Otherinfo for KDF]	鍵導出関数への入力用データ Otherinfo のビット長
	[Bitlength of Keying Data]	共有する鍵のビット長
	[Number of Keying Datas]	共有する鍵の個数
	[x][1]	鍵共有者のプライベート鍵 x
	[y][1]	鍵共有対象者の公開鍵 y
	[Keying Data][1]	共有鍵
公開鍵検証	[Function Name]	Public Key Validation
	[Bitlength of p]	鍵共有と同じ
	[Bitlength of q]	
	[PQG]	
	[Number of Public Keys]	検証する公開鍵の個数
	[y][2]	公開鍵 y
	[Result][2]	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]	鍵共有と同じ
	[Bitlength of q]	
	[PQG]	
	[Number of XY Sets]	生成するプライベート鍵 x と公開鍵 y ペアの個数
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．1，2 のいずれか 1 つを記述する．
	[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]	生成されるドメインパラメータ p, q, g の個数

注

1. [Number of Keying Datas] 個の各鍵と [Keying Data] を以下のように記述する．

   [x]
   . . . ♯ 1 つ目のプライベート鍵を記述する．

   [y]
   . . . ♯ 1 つ目の公開鍵を記述する

   [Keying Data]
   . . . ♯ 1 つ目の共有鍵を記述する．

[x]
. . . ♯ 2 つ目のプライベート鍵を記述する.

[y]
. . . ♯ 2 つ目の公開鍵を記述する

[Keying Data]
. . . ♯ 2 つ目の共有鍵を記述する.

2. [Number of Public Keys] 個の公開鍵 [y] と公開鍵検証結果 [Result] を以下のように記述する.

[y]
. . . ♯ 1 つ目の公開鍵を記述する

[Result]
. . . ♯ 1 つ目の公開鍵検証結果を記述する

[y]
. . . ♯ 2 つ目の公開鍵を記述する

[Result]
. . . ♯ 2 つ目の公開鍵検証結果を記述する

表 7: DH(dhStatic, dhEphem, dhOneFlow) Facts ファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	(アルゴリズム名)
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．1，2 のいずれか 1 つを記述する．
	[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
	[pgenCounter]	p, q 生成用カウンタ
	[h]	h
	[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．

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]，[pgenCounter]，[h]，[Result] を記述する．ただし，[h] は試験 2 を行う時のみ記述する．

2.4 レスポンスファイル (*.rsp)

表 8: DH(dhStatic, dhEphem, dhOneFlow) レスポンスファイル

機能	タグ	内容
(共通)	[Algorithm Name]	(アルゴリズム名)
鍵共有	[Function Name]	Key Sharing
	[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]
	[KDF]	鍵導出関数識別子
	[Otherinfo for KDF]	鍵導出関数への入力用データ Otherinfo [16 進数表記]
	[Bitlength of Otherinfo for KDF]	鍵導出関数への入力用データ Otherinfo のビット長 [16 進数表記]
	[Bitlength of Keying Data]	共有する鍵のビット長 [16 進数表記]
	[Number of Keying Datas]	共有する鍵の個数 [10 進数表記]
	[x][1]	鍵共有者のプライベート鍵 x [16 進数表記]
	[y][1]	鍵共有対象者の公開鍵 y [16 進数表記]
	[Keying Data][1]	【出力】共有鍵 [16 進数表記]
公開鍵検証	[Function Name]	Public Key Validation
	[Bitlength of p]	鍵共有と同じ
	[Bitlength of q]	
	[PQG]	
	[Number of Public Keys]	公開鍵の個数 [10 進数表記]
	[y][2]	公開鍵 y [16 進数表記]
	[Result][2]	【出力】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]	鍵共有と同じ
	[Bitlength of q]	
	[PQG]	
	[Number of XY Sets]	生成するプライベート鍵 x と公開鍵 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]
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．1，2 のいずれか 1 つを記述する．
	[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][4]	ドメインパラメータ p, q, g の個数 [10 進数表記]
	[PQG]	【出力】ドメインパラメータ p, q, g [16 進数表記]
	[SEED]	【出力】p, q 生成用乱数シード [16 進数表記]
	[pgenCounter]	【出力】p, q 生成用カウンタ [10 進数表記]
	[h]	【出力】h [16 進数表記]

注

1. [Number of Keying Datas] 個の各鍵と [Keying Data] を以下のように記述する．

   [x]
   . . . ♯ 1 つ目のプライベート鍵を記述する．

   [y]
   . . . ♯ 1 つ目の公開鍵を記述する

   [Keying Data]
   . . . ♯ 1 つ目の共有鍵を記述する．

   [x]
   . . . ♯ 2 つ目のプライベート鍵を記述する．

   [y]
   . . . ♯ 2 つ目の公開鍵を記述する

   [Keying Data]
   . . . ♯ 2 つ目の共有鍵を記述する．

2. [Number of Public Keys] 個の公開鍵 [y] と公開鍵検証結果 [Result] を以下のように記述する．

   [y]
   . . . ♯ 1 つ目の公開鍵を記述する

   [Result]
   . . . ♯ 1 つ目の公開鍵検証結果を記述する

   [y]
   . . . ♯ 2 つ目の公開鍵を記述する

   [Result]
   . . . ♯ 2 つ目の公開鍵検証結果を記述する

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．

4. 前述のフォーマットにしたがって [Number of PQG Sets] 個のタグ [PQG]，[SEED]，[pgenCounter]，[h] を，実行した試験項目が 1〜2 のいずれであるかに応じて以下に示す必要なタグを記述する．

実行した試験項目	記述が必要なタグ
試験 1	[PQG], [SEED], [pgenCounter]
試験 2	[PQG], [SEED], [pgenCounter], [h]

表 9: DH(dhStatic, dhEphem, dhOneFlow) レスポンスファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	(アルゴリズム名)
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．1，2 のいずれか 1 つを記述する．
	[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][1]	ドメインパラメータ (p, q, g) の個数 [10 進数表記]
	[PQG]	ドメインパラメータ p, q, g [16 進数表記]
	[SEED]	p, q 生成用乱数シード [16 進数表記]
	[pgenCounter]	p, q 生成用カウンタ [10 進数表記]
	[h]	h [16 進数表記]
	[Result]	【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．

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]，[pgenCounter]，[h]，[Result] を記述する．ただし，[h] は試験 2 を行う時のみ記述する．

2.5 結果ファイル (*.out)

表 10: DH(dhStatic, dhEphem, dhOneFlow) 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．

- 鍵ペア生成機能やドメインパラメータ検証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で不合格 (NG) となったかも表示される．
  NG(#10 : y = g∧x mod p ?)
  この例では y，g，x，p が $y = g^x \bmod p$ 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．