JCATT ファイルフォーマット仕様書

HMAC

2018 年 8 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，試験対象実装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

- JCATT 互換ファイルフォーマットの選択時, [　　] で囲まれた “タグ” の次の行に値を記述する．
- CAVS 準互換ファイルフォーマットの選択時, 〈 タグ 〉=〈 値 〉 の形式で 1 行で記述する．
- ヘッダ部分については各行について [〈 タグ 〉=〈 値 〉] の形式で 1 行で記述する．
- レスポンスファイルにおいては，【出力】と記述したタグが，試験対象実装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 HMAC

HMAC 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

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．
各表におけるハッシュ関数の識別子は次表の通り．

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
M_Hash_SHA224	SHA-224
M_Hash_SHA256	SHA-256
M_Hash_SHA384	SHA-384
M_Hash_SHA512	SHA-512

2.1 JCATT2 互換ファイルフォーマット

JCATT2 互換ファイルフォーマットは, 暗号アルゴリズム実装試験仕様書に記載された試験 1 に対応する．

2.1.1 パラメータファイル (*.par)

表2　HMAC パラメータファイル

機能	タグ	内容
(共通)	[Algorithm Name]	HMAC
メッセージ認証	[Function Name]	MAC
	[Key]	メッセージ認証用鍵
	[Bitlength of Key]	メッセージ認証用鍵のビット長
	[Seed]	SMT および SLMT においてランダムメッセージを生成するための擬似乱数生成関数用シード値
	[Bitlength of Seed]	Seed のビット長
	[Hash]	HMAC 内部で使用するハッシュ関数の識別子
	[Data Format]	メッセージデータが byte oriented であることを示す識別子．M_Hash_Byte と記述すること．
	[Upperbound of SLMT]	SLMT で使用されるメッセージの最大ビット長を規定するパラメータ．“メッセージの最大ビット長” = [Upperbound of SLMT]×“ハッシュ関数のブロック長 (ビット)” となる．ハッシュ関数のブロック長は，SHA-1，SHA-224，SHA-256 が 512 ビット，SHA-384 と SHA-512 が 1,024 ビットである．
	[Number of Inner-loop for PGMT]	PGMT の内側ループの回数
	[Number of Outer-loop for PGMT]	PGMT の外側ループの回数
	[Initial Data for PGMT]	PGMT 用初期値
	[Bitlength of Initial Data for PGMT]	PGMT 用初期値のビット長

2.1.2 リクエストファイル (*.req)

表3 HMAC リクエストファイル

機能	タグ	内容
(共通)	[Algorithm Name]	HMAC
メッセージ認証	[Function Name]	MAC
	[Key]	メッセージ認証用鍵 [16 進数表記]
	[Bitlength of Key]	メッセージ認証用鍵のビット長 [10 進数表記]
	[Hash]	ハッシュ関数識別子
	[Data of SMT]	SMT 用メッセージ [16 進数表記]
	[Upperbound of SLMT]	SLMT で使用されるメッセージの最大ビット長を規定するパラメータ．“メッセージの最大ビット長” = [Upperbound of SLMT]×“ハッシュ関数のブロック長 (ビット)” となる．ハッシュ関数のブロック長は，SHA-1，SHA-224，SHA-256 が 512 ビット，SHA-384 と SHA-512 が 1,024 ビットである．[10 進数表記]
	[Data of SLMT]	SLMT 用メッセージ
	[Number of Inner-loop for PGMT]	PGMT の内側ループの回数 [10 進数表記]
	[Number of Outer-loop for PGMT]	PGMT の外側ループの回数 [10 進数表記]
	[Initial Data for PGMT]	PGMT 用初期値 [16 進数表記]
	[Bitlength of Initial Data for PGMT]	PGMT 用初期値のビット長 [10 進数表記]

2.1.3 Facts ファイル (*.fax)

表4 HMAC Facts ファイル

機能	タグ	内容
(共通)	[Algorithm Name]	HMAC
メッセージ認証	[Function Name]	MAC
	[Key]	メッセージ認証用鍵
	[Bitlength of Key]	メッセージ認証用鍵のビット長
	[Hash]	ハッシュ関数識別子
	[Data of SMT]	SMT 用メッセージ
	[MAC of SMT]	SMT で生成された MAC 値
	[Upperbound of SLMT]	SLMT で使用されるメッセージの最大ビット長を規定するパラメータ．“メッセージの最大ビット長” = [Upperbound of SLMT]× “ハッシュ関数のブロック長 (ビット)” となる．ハッシュ関数のブロック長は，SHA-1, SHA-224, SHA-256 が 512 ビット，SHA-384 と SHA-512 が 1,024 ビットである．
	[Data of SLMT]	SLMT 用メッセージ
	[MAC of SLMT]	SLMT で生成された MAC 値
	[Number of Inner-loop for PGMT]	PGMT の内側ループの回数
	[Number of Outer-loop for PGMT]	PGMT の外側ループの回数
	[Initial Data for PGMT]	PGMT 用初期値
	[Bitlength of Initial Data for PGMT]	PGMT 用初期値のビット長
	[MAC of PGMT]	PGMT で生成された MAC 値

2.1.4 レスポンスファイル (*.rsp)

表5 HMAC レスポンスファイル

機能	タグ	内容
(共通)	[Algorithm Name]	HMAC
メッセージ認証	[Function Name]	MAC
	[Key]	メッセージ認証用鍵 [16 進数表記]
	[Bitlength of Key]	メッセージ認証用鍵のビット長 [10 進数表記]
	[Hash]	ハッシュ関数識別子
	[Data of SMT]	SMT 用メッセージ [16 進数表記]
	[MAC of SMT]	【出力】SMT で生成された MAC 値 [16 進数表記]
	[Upperbound of SLMT]	SLMT で使用されるメッセージの最大ビット長を規定するパラメータ．“メッセージの最大ビット長” = [Upperbound of SLMT]×“ハッシュ関数のブロック長 (ビット)” となる．ハッシュ関数のブロック長は，SHA-1，SHA-224，SHA-256 が 512 ビット，SHA-384 と SHA-512 が 1,024 ビットである．[10 進数表記]
	[Data of SLMT]	SLMT 用メッセージ [16 進数表記]
	[MAC of SLMT]	【出力】SLMT で生成された MAC 値 [16 進数表記]
	[Number of Inner-loop for PGMT]	PGMT の内側ループの回数 [10 進数表記]
	[Number of Outer-loop for PGMT]	PGMT の外側ループの回数 [10 進数表記]
	[Initial Data for PGMT]	PGMT 用初期値 [16 進数表記]
	[Bitlength of Initial Data for PGMT]	PGMT 用初期値のビット長 [10 進数表記]
	[MAC of PGMT]	【出力】PGMT で生成された MAC 値 [16 進数表記]

2.2 CAVS 準互換ファイルフォーマット

CAVS 準互換ファイルフォーマットは, 暗号アルゴリズム実装試験仕様書に記載された試験 2 に対応する. この節で取り扱うファイルフォーマットでは, メッセージ認証アルゴリズム識別子として, 表6に記載された表現を用いる.

表6 メッセージ認証アルゴリズム識別子

メッセージ認証アルゴリズム識別子	メッセージ認証アルゴリズム
HMAC-SHA1	HMAC-SHA-1
HMAC-SHA224	HMAC-SHA-224
HMAC-SHA256	HMAC-SHA-256
HMAC-SHA384	HMAC-SHA-384
HMAC-SHA512	HMAC-SHA-512
HMAC-SHA512/224	HMAC-SHA-512/224
HMAC-SHA512/256	HMAC-SHA-512/256
HMAC-SHA3-256	HMAC-SHA3-256
HMAC-SHA3-384	HMAC-SHA3-384
HMAC-SHA3-512	HMAC-SHA3-512

2.2.1 パラメータファイル (*.par)

表7: HMAC パラメータファイル

機能	分類	タグ	内容	値の表記	例示
メッセージ認証	ヘッダ	AlgorithmName	メッセージ認証アルゴリズム識別子.	文字列	[AlgorithmName = HMAC-SHA512]
		〈 メッセージ認証子のビット長 〉	メッセージ認証子のビット長	10 進表記	[L = 256]
		BitLengthOfMessage	メッセージのビット長	10 進表記	[BitLengthOfMessage = 1024]
		BitLengthOfKeyForKSltB	$\|K\| < B$ なる K を IUT がサポートする場合, そのビット長の代表値	10 進表記	[BitLengthOfKeyForKSltB = 256]
		NumberOfTrialsForKSltB	$\|K\| < B$ なる K を使う試験の数	10 進表記	[NumberOfTrialsForKSltB = 30]
		BitLengthOfKeyForKSeqB	$\|K\| = B$ なる K を IUT がサポートする場合, そのビット長	10 進表記	[BitLengthOfKeyForKSeqB = 1024]
		NumberOfTrialsForKSeqB	$\|K\| = B$ なる K を使う試験の数	10 進表記	[NumberOfTrialsForKSeqB = 15]
		BitLengthOfKeyForKSgtB	$\|K\| > B$ なる K を IUT がサポートする場合, そのビット長の代表値	10 進表記	[BitLengthOfKeyForKSgtB = 2048]
		NumberOfTrialsForKSgtB	$\|K\| > B$ なる K を使う試験の数	10 進表記	[NumberOfTrialsForKSgtB = 30]

2.2.2 リクエストファイル (*.req)

表8: HMAC リクエストファイル

機能	分類	タグ	内容	値の表記	例示
メッセージ認証	ヘッダ	AlgorithmName	メッセージ認証アルゴリズム識別子.	文字列	[AlgorithmName = HMAC-SHA512]
		〈 メッセージ認証子のビット長 〉	メッセージ認証子のビット長	10 進表記	[L = 256]
		BitLengthOfMessage	メッセージのビット長	10 進表記	[BitLengthOfMessage = 1024]
		BitLengthOfKeyForKSltB	$\|K\| < B$ なる K を IUT がサポートする場合, そのビット長の代表値	10 進表記	[BitLengthOfKeyForKSltB = 256]
		NumberOfTrialsForKSltB	$\|K\| < B$ なる K を使う試験の数	10 進表記	[NumberOfTrialsForKSltB = 30]
		BitLengthOfKeyForKSeqB	$\|K\| = B$ なる K を IUT がサポートする場合, そのビット長	10 進表記	[BitLengthOfKeyForKSeqB = 1024]
		NumberOfTrialsForKSeqB	$\|K\| = B$ なる K を使う試験の数	10 進表記	[NumberOfTrialsForKSeqB = 15]
		BitLengthOfKeyForKSgtB	$\|K\| > B$ なる K を IUT がサポートする場合, そのビット長の代表値	10 進表記	[BitLengthOfKeyForKSgtB = 2048]
		NumberOfTrialsForKSgtB	$\|K\| > B$ なる K を使う試験の数	10 進表記	[NumberOfTrialsForKSgtB = 30]
	本体 *1	COUNT	0 以上 (NumberOfTrialsForKSltB + NumberOfTrialsForKSeqB + NumberOfTrialsForKSgtB) 未満の整数	10 進表記	COUNT = 0
		Klen	HMAC 鍵のバイト長	10 進表記	Klen = 16
		Tlen	メッセージ認証子のバイト長	10 進表記	Tlen = 32
		Msg	メッセージ認証アルゴリズムへの入力メッセージ	16 進表記	Msg = 5a09 . . . 8e80
		Mac	メッセージ認証子	16 進表記	Mac = ?

∗1 〈 NumberOfTrialsForKSltB + NumberOfTrialsForKSeqB + NumberOfTrialsForKSgtB 〉個の各データの組を以下のように記述する.

```
COUNT = 0                       ♯ i = 0 のデータの組について記述する.
Klen = 32                       ♯ i = 0 に対応する HMAC 鍵のバイト長を記述する.
Tlen = 64                       ♯ i = 0 に対応するメッセージ認証子のバイト長を記述する.
Msg = a677 ... e038             ♯ i = 0 に対応する入力メッセージを記述する.
Mac = ?                         ♯ i = 0 に対応するメッセージ認証子のプレースホルダ.


COUNT = 1                       ♯ i = 1 のデータの組について記述する.
Klen = 32                       ♯ i = 1 に対応する HMAC 鍵のバイト長を記述する.
Tlen = 64                       ♯ i = 1 に対応するメッセージ認証子のバイト長を記述する.
Msg = 30                        ♯ i = 1 に対応する入力メッセージを記述する.
Mac = ?                         ♯ i = 1 に対応するメッセージ認証子のプレースホルダ.
.
.
.

COUNT = 〈                       ♯ i = 〈 NumberOfTrialsForKSltB + NumberOfTrialsForKSeqB + NumberOfTrialsForKS-
NumberOfTrialsForKSltB          gtB - 1 〉のデータの組について記述する.
+ NumberOfTrialsForKSeqB
+ NumberOfTrialsForKSgtB - 1 〉
Klen = 128                      ♯ i = 〈 NumberOfTrialsForKSltB + NumberOfTrialsForKSeqB + NumberOfTrialsForKS-
                                gtB - 1 〉に対応する HMAC 鍵のバイト長を記述する.
Tlen = 64                       ♯ i = 〈 NumberOfTrialsForKSltB + NumberOfTrialsForKSeqB + NumberOfTrialsForKS-
                                gtB - 1 〉に対応するメッセージ認証子のバイト長を記述する.
Msg = dc6f ... c8f2             ♯ i = 〈 NumberOfTrialsForKSltB + NumberOfTrialsForKSeqB + NumberOfTrialsForKS-
                                gtB - 1 〉に対応する入力メッセージを記述する.
Mac = ?                         ♯ i = 〈 NumberOfTrialsForKSltB + NumberOfTrialsForKSeqB + NumberOfTrialsForKS-
                                gtB - 1 〉に対応するメッセージ認証子のプレースホルダ.
```

2.2.3 Facts ファイル (*.fax)

表9: HMAC Facts ファイル

機能	分類	タグ	内容	値の表記	例示
メッセージ認証	ヘッダ	AlgorithmName	メッセージ認証アルゴリズム識別子.	文字列	[AlgorithmName = HMAC-SHA512]
		〈 メッセージ認証子のビット長 〉	メッセージ認証子のビット長	10 進表記	[L = 256]
		BitLengthOfMessage	メッセージのビット長	10 進表記	[BitLengthOfMessage = 1024]
		BitLengthOfKeyForKSltB	$\|K\| < B$ なる K を IUT がサポートする場合, そのビット長の代表値	10 進表記	[BitLengthOfKeyForKSltB = 256]
		NumberOfTrialsForKSltB	$\|K\| < B$ なる K を使う試験の数	10 進表記	[NumberOfTrialsForKSltB = 30]
		BitLengthOfKeyForKSeqB	$\|K\| = B$ なる K を IUT がサポートする場合, そのビット長	10 進表記	[BitLengthOfKeyForKSeqB = 1024]
		NumberOfTrialsForKSeqB	$\|K\| = B$ なる K を使う試験の数	10 進表記	[NumberOfTrialsForKSeqB = 15]
		BitLengthOfKeyForKSgtB	$\|K\| > B$ なる K を IUT がサポートする場合, そのビット長の代表値	10 進表記	[BitLengthOfKeyForKSgtB = 2048]
		NumberOfTrialsForKSgtB	$\|K\| > B$ なる K を使う試験の数	10 進表記	[NumberOfTrialsForKSgtB = 30]
	本体 *1	COUNT	0 以上 (NumberOfTrialsForKSltB + NumberOfTrialsForKSeqB + NumberOfTrialsForKSgtB) 未満の整数	10 進表記	COUNT = 0
		Klen	HMAC 鍵のバイト長	10 進表記	Klen = 16
		Tlen	メッセージ認証子のバイト長	10 進表記	Tlen = 32
		Msg	メッセージ認証アルゴリズムへの入力メッセージ	16 進表記	Msg = 5a09 . . . 8e80
		Mac	メッセージ認証子	16 進表記	Mac = aa77 . . . 3c78

∗1 〈 NumberOfTrialsForKSltB + NumberOfTrialsForKSeqB + NumberOfTrialsForKSgtB 〉個の各データの組を以下のように記述する.

```
COUNT = 0                    ♯ i = 0 のデータの組について記述する.
Klen = 32                    ♯ i = 0 に対応する HMAC 鍵のバイト長を記述する.
Tlen = 64                    ♯ i = 0 に対応するメッセージ認証子のバイト長を記述する.
Msg = a677 ... e038          ♯ i = 0 に対応する入力メッセージを記述する.
Mac = aa77 ... 3c78          ♯ i = 0 に対応するメッセージ認証子の期待値を記述する.


COUNT = 1                    ♯ i = 1 のデータの組について記述する.
Klen = 32                    ♯ i = 1 に対応する HMAC 鍵のバイト長を記述する.
Tlen = 64                    ♯ i = 1 に対応するメッセージ認証子のバイト長を記述する.
Msg = 30                     ♯ i = 1 に対応する入力メッセージを記述する.
Mac = aa77 ... 3c78          ♯ i = 1 に対応するメッセージ認証子の期待値を記述する.
.
.
.

COUNT = 〈                    ♯ i = 〈 NumberOfTrialsForKSltB + NumberOfTrialsForKSeqB + NumberOfTrialsForKS-
NumberOfTrialsForKSltB       gtB - 1 〉のデータの組について記述する.
+ NumberOfTrialsForKSeqB
+ NumberOfTrialsForKSgtB - 1 〉
Klen = 128                   ♯ i = 〈 NumberOfTrialsForKSltB + NumberOfTrialsForKSeqB + NumberOfTrialsForKS-
                             gtB - 1 〉に対応する HMAC 鍵のバイト長を記述する.
Tlen = 64                    ♯ i = 〈 NumberOfTrialsForKSltB + NumberOfTrialsForKSeqB + NumberOfTrialsForKS-
                             gtB - 1 〉に対応するメッセージ認証子のバイト長を記述する.
Msg = dc6f ... c8f2          ♯ i = 〈 NumberOfTrialsForKSltB + NumberOfTrialsForKSeqB + NumberOfTrialsForKS-
                             gtB - 1 〉に対応する入力メッセージを記述する.
Mac = aa77 ... 3c78          ♯ i = 〈 NumberOfTrialsForKSltB + NumberOfTrialsForKSeqB + NumberOfTrialsForKS-
                             gtB - 1 〉に対応するメッセージ認証子の期待値を記述する.
```

2.2.4 レスポンスファイル (*.rsp)

表10: HMAC レスポンスファイル

機能	分類	タグ	内容	値の表記	例示
メッセージ認証	ヘッダ	AlgorithmName	メッセージ認証アルゴリズム識別子.	文字列	[AlgorithmName = HMAC-SHA512]
		〈 メッセージ認証子のビット長 〉	メッセージ認証子のビット長	10 進表記	[L = 256]
		BitLengthOfMessage	メッセージのビット長	10 進表記	[BitLengthOfMessage = 1024]
		BitLengthOfKeyForKSltB	$\|K\| < B$ なる K を IUT がサポートする場合, そのビット長の代表値	10 進表記	[BitLengthOfKeyForKSltB = 256]
		NumberOfTrialsForKSltB	$\|K\| < B$ なる K を使う試験の数	10 進表記	[NumberOfTrialsForKSltB = 30]
		BitLengthOfKeyForKSeqB	$\|K\| = B$ なる K を IUT がサポートする場合, そのビット長	10 進表記	[BitLengthOfKeyForKSeqB = 1024]
		NumberOfTrialsForKSeqB	$\|K\| = B$ なる K を使う試験の数	10 進表記	[NumberOfTrialsForKSeqB = 15]
		BitLengthOfKeyForKSgtB	$\|K\| > B$ なる K を IUT がサポートする場合, そのビット長の代表値	10 進表記	[BitLengthOfKeyForKSgtB = 2048]
		NumberOfTrialsForKSgtB	$\|K\| > B$ なる K を使う試験の数	10 進表記	[NumberOfTrialsForKSgtB = 30]
	本体 *1	COUNT	0 以上 (NumberOfTrialsForKSltB + NumberOfTrialsForKSeqB + NumberOfTrialsForKSgtB) 未満の整数	10 進表記	COUNT = 0
		Klen	HMAC 鍵のバイト長	10 進表記	Klen = 16
		Tlen	メッセージ認証子のバイト長	10 進表記	Tlen = 32
		Msg	メッセージ認証アルゴリズムへの入力メッセージ	16 進表記	Msg = 5a09 . . . 8e80
		Mac	【出力】メッセージ認証子	16 進表記	Mac = aa77 . . . 3c78

∗1 〈 NumberOfTrialsForKSltB + NumberOfTrialsForKSeqB + NumberOfTrialsForKSgtB 〉個の各データの組を以下のように記述する.

```
COUNT = 0                       ♯ i = 0 のデータの組について記述する.
Klen = 32                       ♯ i = 0 に対応する HMAC 鍵のバイト長を記述する.
Tlen = 64                       ♯ i = 0 に対応するメッセージ認証子のバイト長を記述する.
Msg = a677 ... e038             ♯ i = 0 に対応する入力メッセージを記述する.
Mac = aa77 ... 3c78             ♯ i = 0 に対応して, IUT が生成したメッセージ認証子.


COUNT = 1                       ♯ i = 1 のデータの組について記述する.
Klen = 32                       ♯ i = 1 に対応する HMAC 鍵のバイト長を記述する.
Tlen = 64                       ♯ i = 1 に対応するメッセージ認証子のバイト長を記述する.
Msg = 30                        ♯ i = 1 に対応する入力メッセージを記述する.
Mac = aa77 ... 3c78             ♯ i = 1 に対応して, IUT が生成したメッセージ認証子.
.
.
.

COUNT = 〈                       ♯ i = 〈 NumberOfTrialsForKSltB + NumberOfTrialsForKSeqB + NumberOfTrialsForKS-
NumberOfTrialsForKSltB          gtB - 1 〉のデータの組について記述する.
+ NumberOfTrialsForKSeqB
+ NumberOfTrialsForKSgtB - 1 〉
Klen = 128                      ♯ i = 〈 NumberOfTrialsForKSltB + NumberOfTrialsForKSeqB + NumberOfTrialsForKS-
                                gtB - 1 〉に対応する HMAC 鍵のバイト長を記述する.
Tlen = 64                       ♯ i = 〈 NumberOfTrialsForKSltB + NumberOfTrialsForKSeqB + NumberOfTrialsForKS-
                                gtB - 1 〉に対応するメッセージ認証子のバイト長を記述する.
Msg = dc6f ... c8f2             ♯ i = 〈 NumberOfTrialsForKSltB + NumberOfTrialsForKSeqB + NumberOfTrialsForKS-
                                gtB - 1 〉に対応する入力メッセージを記述する.
Mac = aa77 ... 3c78             ♯ i = 〈 NumberOfTrialsForKSltB + NumberOfTrialsForKSeqB + NumberOfTrialsForKS-
                                gtB - 1 〉に対応して, IUT が生成したメッセージ認証子.
```

2.2.5 結果ファイル (*.out)

表11: HMAC 結果ファイル

機能	分類	タグ	内容	値の表記	例示
メッセージ認証	ヘッダ	AlgorithmName	メッセージ認証アルゴリズム識別子.	文字列	[AlgorithmName = HMAC-SHA512]
		〈 メッセージ認証子のビット長 〉	メッセージ認証子のビット長	10 進表記	[L = 256]
		BitLengthOfMessage	メッセージのビット長	10 進表記	[BitLengthOfMessage = 1024]
		BitLengthOfKeyForKSltB	$\|K\| < B$ なる K を IUT がサポートする場合, そのビット長の代表値	10 進表記	[BitLengthOfKeyForKSltB = 256]
		NumberOfTrialsForKSltB	$\|K\| < B$ なる K を使う試験の数	10 進表記	[NumberOfTrialsForKSltB = 30]
		BitLengthOfKeyForKSeqB	$\|K\| = B$ なる K を IUT がサポートする場合, そのビット長	10 進表記	[BitLengthOfKeyForKSeqB = 1024]
		NumberOfTrialsForKSeqB	$\|K\| = B$ なる K を使う試験の数	10 進表記	[NumberOfTrialsForKSeqB = 15]
		BitLengthOfKeyForKSgtB	$\|K\| > B$ なる K を IUT がサポートする場合, そのビット長の代表値	10 進表記	[BitLengthOfKeyForKSgtB = 2048]
		NumberOfTrialsForKSgtB	$\|K\| > B$ なる K を使う試験の数	10 進表記	[NumberOfTrialsForKSgtB = 30]
		〈 Results 〉	OK 又は NG	文字列	OK

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何番目 (COUNT, # 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.