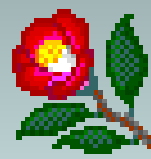
Camellia テストベクトル 生成プログラム訂正

日本電信電話株式会社
三菱電機株式会社

発表者：松井充



本発表の目的

- 継続評価128ビットブロック暗号Camelliaの2001年応募資料（2001年9月27日提出）のうち**テストベクトル生成プログラム**ならびにそれにより生成された**テストベクトル**に誤りがあったことを報告

- Camellia の仕様（書）ならびにそれを実現したリファレンスコードは変更なし

テストベクトル生成プログラム

- ﾘﾌｧﾚﾝｽﾌﾟﾛｸﾞﾗﾑ (暗号ｱﾙｺﾞﾘｽﾞﾑ本体) を呼び出し、平文・鍵・暗号文の組を自動的に生成
- テストベクトル生成プログラム自身は暗号演算には関与しない
- 2001年度応募提出資料として、暗号設計者自身が設計作成し提出することが求められた

訂正個所 (t_camellia.c)

```
for( k=0; k<3; k++ ){
        printf( "Camellia with %d-bit key¥n¥n", keysize[k] );

        for( i=0; i<10; i++ ){
                鍵 key[i][0] … key[i][(keysize[k]/8)-1] 生成ならびに出力

                Camellia_Ekeygen( keysize[k], key[i-1], ekey );

                for( j=0; j<128; j++ ){
                        平文 ptext[0] … ptext[15] 生成ならびに出力

                        Camellia_Encrypt( keysize[k], ptext, ekey, ctext );

                        暗号文 ctext[0] … ctext[15] 出力
                }
        }
}
```

(誤) key[i-1] => (正) key[i]

正誤対応付図


2001年9月27日提出版
テストベクトルファイル
平文暗号文対は同一
今回修正した正しい
テストベクトルファイル
1番目(K1利用と誤記)のデータ
2番目(K2利用と誤記)のデータ
3番目(K3利用と誤記)のデータ
4番目(K4利用と誤記)のデータ
5番目(K5利用と誤記)のデータ
6番目(K6利用と誤記)のデータ
7番目(K7利用と誤記)のデータ
8番目(K8利用と誤記)のデータ
9番目(K9利用と誤記)のデータ
10番目(K10利用と誤記)のデータ
K1利用時の正しいデータ
K2利用時の正しいデータ
K3利用時の正しいデータ
K4利用時の正しいデータ
K5利用時の正しいデータ
K6利用時の正しいデータ
K7利用時の正しいデータ
K8利用時の正しいデータ
K9利用時の正しいデータ
K10利用時の正しいデータ

まとめ

- Camellia のテストベクトル生成プログラムに誤りがあり、鍵の順序がずれて表示された
- この誤りの指摘ならびに修正されたファイル一式を CRYPTREC 事務局に送付済み
- Camellia の仕様 (書) ならびにそれを実現したリファレンスコードに変更なし