

Message-Id: <4.2.0.58.J.20020124134620.02780048@sucaba.isl.ntt.co.jp>
Date: Thu, 24 Jan 2002 14:15:28 +0900
To: cryptrec-comment@ipa.go.jp
From: Masayuki KANDA <kanda@sucaba.isl.ntt.co.jp>
Subject: Camellia
=?ISO-2022-JP?B?GyRCJUYIOSVIVkILyVIJWskTjhtJGokSyREJCQbKEI=?=
=?ISO-2022-JP?B?GyRCJEYbKEI=?=
Cc: kanda@sucaba.isl.ntt.co.jp

CRYPTREC事務局 御中

日本電信電話株式会社の神田と申します。

このたび、弊社ならびに三菱電機株式会社よりCRYPTRECに継続提案しております、128ビットブロック暗号「Camellia」につきまして、2001年9月27日提出書類のうち、テストベクトル(t_camellia.txt)に誤りがあることが判明いたしました。そのため、弊社ならびに三菱電機(株)にて、原因の調査を行ったところ、テストベクトル生成プログラムに1箇所プログラムミスが含まれていることを確認いたしました。

本メールにて、提出書類のテストベクトルが誤っていることを報告いたしますと共に、その詳細ならびに正しいテストベクトル等の資料を添付いたします。なお、本メールに添付しました資料はCamelliaのホームページにも掲載いたします。

提出書類に誤りが含まれていましたことをお詫びいたしますと共に、今後の評価につきましては、訂正版のテストベクトル生成プログラムならびにテストベクトルファイルを利用いただきますようお願い申し上げます。

(添付書類の内訳)

- 1 . Attachedsheet.ppt : テストベクトルの正誤対応関係付図
- 2 . camellia.c : Camelliaリファレンスプログラム (2001年9月27日提出版と同一)
- 3 . correction.txt : 誤り箇所説明資料
- 4 . t_camellia.c : 修正したテストベクトル生成プログラム
- 5 . t_camellia.txt : 正しいテストベクトルファイル
- 6 . t_camellia_old.c : 2001年9月27日提出のテストベクトル生成プログラム

NTT 情報流通プラットフォーム研究所 情報セキュリティプロジェクト
セキュリティ基盤グループ
NTT Information Sharing Platform Laboratories - Security Project

神田 雅透 <KANDA Masayuki >
E-Mail: kanda@sucaba.isl.ntt.co.jp
〒239-0847 神奈川県横須賀市光の丘1-1-612A
TEL. 0468-59-2437 (Dial in) FAX. 0468-59-3858

テストベクトルの正誤対応関係

(参考付図)
日本電信電話株式会社
三菱電機株式会社

提出版テストベクトル
(2001年9月27日版)

この平文暗号文対の
データが一致している
ことを表しています

正しいテストベクトル
(今回の訂正版)

128ビット鍵	1番目 (K1利用と誤記) のデータ	K1利用時の正しいデータ	128ビット鍵
	2番目 (K2利用と誤記) のデータ	K2利用時の正しいデータ	
	3番目 (K3利用と誤記) のデータ	K3利用時の正しいデータ	
	4番目 (K4利用と誤記) のデータ	K4利用時の正しいデータ	
	5番目 (K5利用と誤記) のデータ	K5利用時の正しいデータ	
	6番目 (K6利用と誤記) のデータ	K6利用時の正しいデータ	
	7番目 (K7利用と誤記) のデータ	K7利用時の正しいデータ	
	8番目 (K8利用と誤記) のデータ	K8利用時の正しいデータ	
	9番目 (K9利用と誤記) のデータ	K9利用時の正しいデータ	
	10番目 (K10利用と誤記) のデータ	K10利用時の正しいデータ	

192ビット鍵	1番目 (K1利用と誤記) のデータ	K1利用時の正しいデータ	192ビット鍵
	2番目 (K2利用と誤記) のデータ	K2利用時の正しいデータ	
	3番目 (K3利用と誤記) のデータ	K3利用時の正しいデータ	
	4番目 (K4利用と誤記) のデータ	K4利用時の正しいデータ	
	5番目 (K5利用と誤記) のデータ	K5利用時の正しいデータ	
	6番目 (K6利用と誤記) のデータ	K6利用時の正しいデータ	
	7番目 (K7利用と誤記) のデータ	K7利用時の正しいデータ	
	8番目 (K8利用と誤記) のデータ	K8利用時の正しいデータ	
	9番目 (K9利用と誤記) のデータ	K9利用時の正しいデータ	
	10番目 (K10利用と誤記) のデータ	K10利用時の正しいデータ	

256ビット鍵	1番目 (K1利用と誤記) のデータ	K1利用時の正しいデータ	256ビット鍵
	2番目 (K2利用と誤記) のデータ	K2利用時の正しいデータ	
	3番目 (K3利用と誤記) のデータ	K3利用時の正しいデータ	
	4番目 (K4利用と誤記) のデータ	K4利用時の正しいデータ	
	5番目 (K5利用と誤記) のデータ	K5利用時の正しいデータ	
	6番目 (K6利用と誤記) のデータ	K6利用時の正しいデータ	
	7番目 (K7利用と誤記) のデータ	K7利用時の正しいデータ	
	8番目 (K8利用と誤記) のデータ	K8利用時の正しいデータ	
	9番目 (K9利用と誤記) のデータ	K9利用時の正しいデータ	
	10番目 (K10利用と誤記) のデータ	K10利用時の正しいデータ	

CRYPTREC 事務局御中

2001年度継続評価暗号に応募いたしました Camellia のテストベクトル生成プログラムに誤りがありましたのでここで訂正するとともに、正しいテストベクトル生成プログラムとテストデータを送付いたします。誤りはディレクトリ tv 内のファイル t_camellia.c の 57行目にあり、これによって鍵の対応が1つつずれるという現象が発生しました。

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

これを修正した t_camellia.c ならびにこれをもちいて作られた、正しいテストベクトルファイル(ディレクトリ tvect 内) t_camellia.txt を送付いたします。ご迷惑をおかけいたしますがよろしく差し替えをお願いいたします。

なおこの誤りは、提出いたしましたテストベクトル生成プログラムにのみ含まれるものであり、Camellia の仕様には一切変更がないことを付け加えさせていただきます。具体的には、Camellia 仕様書、Camellia リファレンスプログラム camellia.c、Camellia テストベクトル生成プログラム仕様書には変更はございません。

日本電信電話会社
三菱電機株式会社