Protected Communication System（CMLcrypt） Ver. 3

（C）宇山　靖政

ソフトウエアの名称　：　Protected Communication System（CMLcrypt）

１．ソフトの概要

この暗号ソフトは、Camellia を参考にして作成したものです。
(NTT 様と三菱電機様の御厚意により Camellia の暗号アルゴリズムを無料で利用させていただける事を感謝しております。)貿易管理令の規制によりソースコードを公開しないで､インターネットに掲載できるものは、最大で 56 ビットですので悪しからず。
"メールもビトマ"、"Cipher Web Mail" には、Camellia 暗号ソフトとそのためのもっと長い鍵を生成するソフトが付いています。 "メールもビトマ"、"Cipher Web Mail" で利用可能な暗号は、RSA（2048 ビット）AES(Rijndael),RSA,Camellia,Twofish などです。これらを用いた 5 段階の多重暗号化が可能です。

Camellia は NTT と三菱電機が共同開発した優れた暗号ソフトです。Camellia 紹介の HP では、

Camellia（カメリア）は、世界のトップクラスの暗号研究者を抱える NTT と三菱電機が共同で 2000 年に開発した共通鍵ブロック暗号です。技術的に高い安全性を有するのは当然のこと、効率性と実用性にも優れており、さまざまなプラットフォーム上でのソフトウェアにより高速に実装することができます。ハードウェア実装においても、高速実装はもとよりコンパクトかつ低消費電力型の実装が可能です。
これらの技術的優位性は、例えば欧州連合推奨暗号選定プロジェクト NESSIE において「米国政府標準暗号 AES と多くの点で同等の安全性と性能を有している」と評価されるなど、国際的にも認められています。現在では、AES と同等の安全性・処理性能を有しているほぼ唯一の暗号として国際的にも認知されつつあり、多くの国際的な標準暗号・推奨暗号に選定されています。
とりわけ、日本国産暗号としては、初めてインターネット標準暗号（IETF Standard Track RFC）として承認されました。
と紹介されています。

２．　作者への連絡先(メールアドレス、ホームページ)

メールアドレス：uyama33@yahoo.co.jp　　（宇山　靖政）
ホームページ　：http://uyama22.pa.land.to/　（ソースコード）

３．　取り扱い種別(フリーウエア)

４．　動作環境

Windows Vista Home Premium　32 ビット
Windows 7 Home Premium　　64 ビット
の上で動きます。

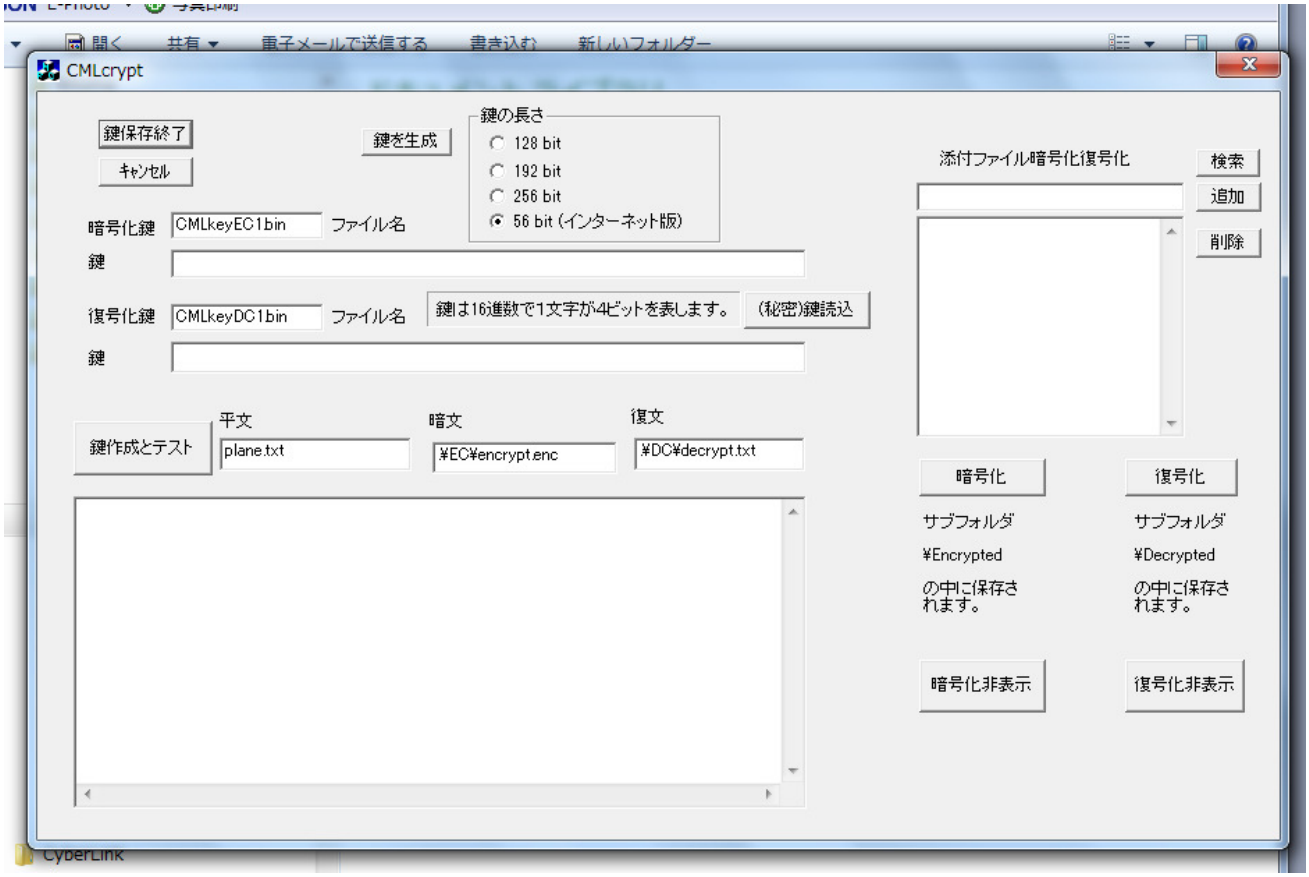
５．　別途必要なソフト：特になし（暗号ソフトとして単独で動きます。メール機能はありません。）

６．　インストール・アンインストール方法

インストール：CamelliaPac.zip を解凍すると、このマニュアルの他に、CamelliaSys.zip　（暗号ソフトと関連するフォルダ、ファイル）が現れます。
さらに、CamelliaSys.zip を解凍すると、“CamelliaSys”フォルダが出来ます。このフォルダをデスクトップ等の適当な場所に置き、その中にある
“CMLcrypt.exe”へのショートカットを作成してください。

７．アンインストール：作成したショートカットと、フォルダを削除してください。

使い方：



１．適当なフォルダをつくり、CMLcrypt.exe を置く。
２．暗号化したい添付ファイルを同じフォルダに入れる。
３．CMLcrypt.exe　を起動して、平文の所に暗号化したいファイル名を記入する。
　　暗号化されたものの所に暗号化されたファイルの名前を記入する。
　　復号化されたものの所に平文のファイル名とは別の名前を記入する。
４．＜鍵を作成＞のボタンをクリックする。
　　必要なら、５６ビット鍵（１４文字の所２カ所には同じ文字列を入れる）の所を好きな１６進数にする。
５．＜鍵のテスト＞ボタンをクリックして正常に暗号化、復号化出来るか確認
６．暗号化されたものを添付ファイルとして送信。
７．相手にもこのソフトをダウンロードしてもらって、鍵を教える。
８．相手は、＜鍵を作成＞のボタンをクリックする。
　　５６ビット鍵（2 箇所の１４文字は同じ文字列を入れる）の所を教えられた１６進数にする。
９．暗号化されたファイル名を正しく入力する。
１０．＜復号化のみ＞をクリックする。
１１．相手は添付ファイルを復号化できる。
となります。

暗号化鍵、復号化鍵を読み込んでから、暗号化するものを検索して、リストボックスにその一覧を表示しておけば、連続して暗号化、復号化が行えます。
暗号化したものが置かれるフォルダをしっかり確認してください。この暗号化されたものを復号化することになります。

非表示で、操作すれば Camellia 暗号の高速処理が確認できます。この処理速度ならば電子メールを送信する途中で本文や添付ファイルを暗号化できます。
電子メールでの扱いには、メールアドレスとの関連が問題になります。“メールもビトマ”、または“Cipher Web Mail” を利用すれば、送信アドレスごとに暗号化鍵、復号化鍵、暗号化アルゴリズムを 5 段階で設定できます。

電子メールの添付ファイルを暗号化するときは、復号化鍵を相手の方に前もって届けて置いてください。そのためには、RSA 暗号をご利用ください。フリーソフト Protected Communication System(AFCrypt) が利用できます。

参考：
Protected Communication System に関しては、ヨーロッパ、アメリカでの特許を取得いたしました。