Protected Communication System（AEScrypt） Ver. 3

（C）宇山　靖政

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

１．ソフトの概要

DES が制定されたのは 1977 年でありその後の暗号解読技術の発展、コンピュータの高性能化から、米国商務省標準技術局(NIST)によって新しい暗号技術の選定作業が行われました。
米国政府の次世代標準暗号化方式を決めることになり、NIST は DES に代わる次世代の暗号標準として、AES 候補となる暗号方式を全世界から公募しました。世界中から集まった 15 の方式が審査を受けていたが、2000 年 10 月に、ベルギーの暗号開発者 Joan Daemen 氏と Vincent Rijmen 氏が開発した「Rijndael」という方式が選ばれました。このアルゴリズムは、ロイヤリティーフリーで提供されていましたので、利用させていただきました。

この暗号ソフトは、下記の参考文献を使って作りましたので、AES として採用されているものよりも鍵およびブロックの長さの種類が多くなっています。鍵長、ブロック長は、それぞれ 128,160,192,224,256 ビットの 5 通りです。AES のものは、鍵長、ブロック長は、それぞれ、128,192,256 ビットの 3 通りです。

参考文献

The Design of Rijndael: Aes-The Advanced Encryption Standard (Information Security and Cryptography) (ハードカバー)
Joan Daemen
参考文献のミスプリント The Design Of Rijndael ? Errata

貿易管理令での制限については、鍵の長さを 56 ビットを超えないようにするか、ソースコードを公開するかのどちらかが必要です。HP でソースコードを公開するほうを選びました。

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：AesPac.zip を解凍すると、このマニュアルの他に、AesSys.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、AesSys.zip を解凍すると、“AesSys”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
“AEScrypt.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、AEScrypt.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．AEScrypt.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 AES 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。