Protected Communication System（AFCrypt）　　Ver. 1.0

（C）宇山　靖政

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

１．ソフトの概要

公開鍵暗号 RSA のソフトです。“メールもビトマ”、"Cipher Web Mail” における共通鍵の交換のために作成しました。公開鍵の作成、交換、暗号化、復号化が可能です。電子メールでの添付ファイルの暗号化、復号化にご利用ください。

鍵の長さは、512 ビット、1024 ビット、1536 ビット、2048 ビットから選択できます。（鍵を作成するのに要する時間はそれぞれ、30 秒、10 分、40 分、2 時間です。メモリーの量や CPU の性能で異なる。）もちろん貿易管理令に違反しないようにソースコードを HP で公開しています。

特徴は、複素数の配列と多倍長整数の変換を適宜行う方法で全体を扱っていることです。さらに、3 通りの乗法（複素数の普通の乗法、DFT による乗法、FFT による乗法）を用意して、扱う数の大きさによって切り替えて計算しています。除法と剰余は自分で考えた方法で計算しています。最大公約数と逆数の計算は Menezes の Handbook of Applied Cryptography (Discrete Mathematics and Its Applications) にあった方法を少し変形して使っています。べき乗計算は FFT を主に利用しています。

全体的な流れは、橋本晋之介　氏の
”RSA 暗号技術の基礎から C++による実装まで”
の流れに沿って作成しました。ご指導いただいたことを感謝しております。

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：AFCryptPac.zip を解凍すると、このマニュアルの他に、
AFCryptSys.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、AFCryptSys.zip を解凍すると、“AFCryptSys”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
“AFCrypt.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、４つのフォルダを削除してください。

使い方：

１．適当な場所に、“AFCryptSys”フォルダをつくり、AFCrypt.exe へのショートカットをつくる。

２．暗号化したいファイルを同じフォルダに入れる。

３．AFCrypt.exe　を起動して、
平文の所に暗号化したいテキストファイル名を記入する。

暗文の所に暗号化されたファイルの名前を記入する。
”ec¥encrypt.enc”とするとサブフォルダ”EC”の中に作成される。

復文の所に平文のテキストファイル名とは別の名前を記入する。
”dc¥decrypt.txt”とするとサブフォルダ”DC”の中に作成される。

４．鍵の長さ（512～2048）ビットを指定する。

５．鍵を作る　ボタンをクリックする。

６．暗号化と復号化のテスト　ボタンをクリックする、

７．鍵を保存して終了。

が基本操作です。

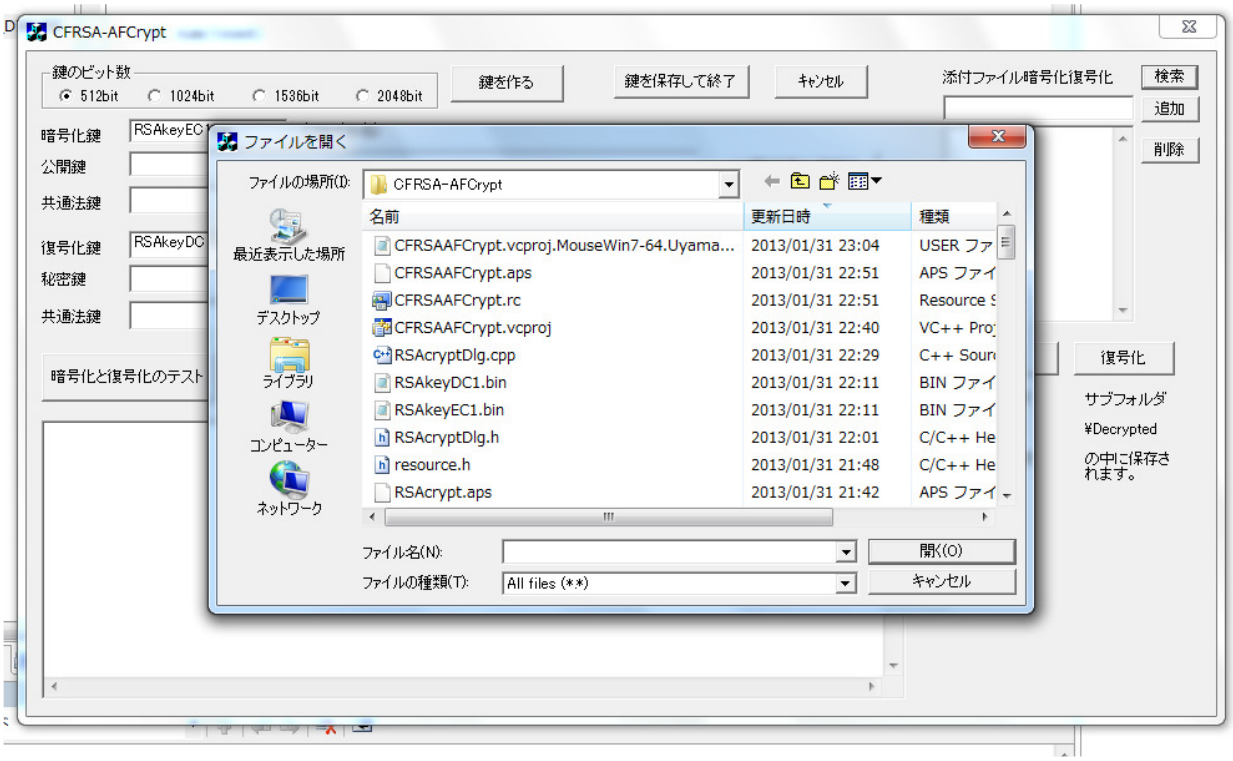
電子メールの場合

添付ファイルの暗号化するときの作成した鍵の使い方

１．作成した公開鍵をお互いに相手におくる。

２．受け取った公開鍵を、（公開）暗号化鍵読込　ボタンをクリックして読込む。

３．平文の所に、暗号化して相手に送るデータ名を記入する。
　　または､右上の　検索　ボタンをクリックして暗号化した添付ファイルとして相手に送るファイルを選択する。これを繰り返す。



余分なものは削除する。

４．暗文のところは、もし文書名を同じにしたいなら、”ec¥test.txt”のようにしてサブフォルダ EC の中に作成するように設定する。

右上のボタンで操作すると、ファイル名は同じで、内容が暗号化されたものが、¥Encrypted サブフォルダの中に作成される。

５．暗号化　または　暗号化非表示　ボタンをクリックする。

６．作成した暗号文をメールソフトに添付して送信。

７．受け取った人は、自分の秘密鍵を、（秘密）復号化鍵読込　ボタンをクリックして読み込む。

８．暗文　の所に受け取った暗号文を設定する。復文の名前を”dc¥test.enc”のように設定する。

　または、自分の公開鍵によって暗号化されて送られてきたファイルを、¥Encrypted の中において、右上の検索ボタンで、次々に選んでゆく。

９．復号化　または　復号化非表示　をクリックして元に戻す。

　右上のボタンの操作では、復号化されたものは　¥Decrypted のなかに保存されます。

ファイルは、基本的には上書きされます。

必要なデータを無くさないように十分注意してください。

あまり長い公開鍵を相手に送ると、相手の PC によっては、かなり時間がかかりますので迷惑します。
お互いによく相談してください。

８G バイト以上のメモリーを持っている PC をお勧めします。

鍵を作成するほどではないのですが、暗号化、復号化にも時間がかかります。

あらかじめ十分テストしてください。

参考：

安全保障貿易に係る機微技術管理ガイダンス
（大学・研究機関用）
改訂版
平成２２年２月
経済
Ⅱ―５．規制の許可例外について
貿易関係貿易外取引等に関する省令（平成１０年通商産業省令第８号。以下「貿易外省令」という。）第９条において、安全保障貿易管理の観点から特に支障が無いと認められるため許可を必要としない技術提供が規定されています。代表的なものとしては以下のようなものがあります。
○ 公知の技術を提供する取引又は技術を公知とするために当該技術を提供する取引であって、以下のいずれかに該当するもの（第２項第９号）
－ 新聞、書籍、雑誌、カタログ、電気通信ネットワーク上のファイルなどにより、既に不特定多数の者に対して公開されている技術を提供する取引
－ 学会誌、公開特許情報、公開シンポジウムの議事録など不特定多数の者が入手可能な技術を提供する取引
－ 工場の見学コース、講演会、展示会などにおいて不特定多数の者が入手又は聴講可能な技術を提供する取引
－ ソースコードが公開されているプログラムを提供する取引
－ 学会発表用の原稿又は展示会などでの配布資料の送付、雑誌への投稿など、当該技術を不特定多数の者が入手又は閲覧可能とすることを目的とする取引

RSA アルゴリズムは特許が切れて自由に使えるようです。皆さんも自由に作ってみてください。
暗号メールの国内での使用については法律的な問題はありませんが、
１、異なるアルゴリズムで多重暗号化可能。
２、鍵は利用者が好きな長さで作れる。
３、異なる暗号化方式を簡単に使える。
などが可能なために、HP にソースコードを掲載してます。

著作権、特許権を放棄してはいませんのでご注意ください。貿易管理令にあわせるために公開しているだけです。メールソフト“メールもビトマ”、“Cipher Web Mail”では、AES（Rijndael）,Twofish　なども利用できます。これらの暗号による多重暗号化が可能です。

* 詳しくはホームページをご覧下さい。

特許：
暗号通信の方式に関してはヨーロッパ、アメリカで特許を取得しました。