スマホでニャン語(Protected Communication System)

ソフトウェアの名称：スマホでニャン語(Protected Communication System)
（シェアレジ番号 ： SR381760 ）

１．ソフトの概要
Android スマホで、ニャン語メールを送受信するソフトです。また、本格的な暗号化も可能です。
暗号方式を Neko, AES、Camellia、Misty、Twofish、Serpent、Mars、Bitoma、Bmp56 から自由に選んで、５段階の多重暗号化ができます。暗号化鍵、復号化鍵の作成は PC で行います。
貿易管理令の例外適用を受けるために、ソースコードをホームページで公開し、公知の技術とします。ソースコードは自由に閲覧できますが、特許権と著作権は宇山靖政が所有しますので、複製を作って所持してはいけません。
特許(Protected Communication System)については、米国、欧州の特許庁 HP をご覧ください。

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://www.asahi-net.or.jp/~cq4y-uym/index.html
貿易管理令があるので、暗号関連の質問に直接答えることは出来ません。質問と回答を HP に掲載する形になります。

３．取り扱い種別(シェアウェア)
金額：3348 円（本体価格 3000 円＋税＋ベクターの手数料　となります。）
送金方法：ベクターレジサービス
試用制限：試用期間中は、復号化ソフトと復号化鍵は自由に設定できますが、暗号化ソフトと暗号化鍵は Bmp56EC.exe と“K1234567.bin”に制限されます。
試用期限：期限無し。
試用制限を解除するには、送金後にベクターから送られてくるライセンスキー、“userkey.dat”で、スマホの SD カードの中のものを上書きする。
　購入したライセンスキーは、同時に 1 台のマシンにおいてのみ使用を許可します。複数台のマシンにおいて本ソフトウェアのライセンスキーを登録する場合は、マシンの台数分のライセンスキーを購入してください。

４．動作環境
Android スマホ　（SD カード装着。Android　Ver. 4.1 以上）
機種によって、SD カードのフォルダ名が異なるので、動かない機種もあります。
Bmp56EC.exe　による、暗号化が可能であることを必ず確認してください。

PC（スマホへのインストール、暗号化鍵、復号化鍵の作成で使います。）
Windows Vista Home Premium　 32 ビット
Windows 7 Home Premium　　64 ビット

５．別途必要なソフト、機材：Android スマホと PC をつなぐ USB ケーブル

６．インストール・アンインストール方法
インストール：PC で SN5mailPac.zip を解凍すると、このマニュアルの他に、
SN5mailSys.zip　（暗号メールソフトと関連するフォルダ、ファイル）
鍵の見本.zip　　（暗号化鍵と復号化鍵の見本）
鍵作成ソフト.zip　（暗号化鍵と復号化鍵を作成するソフト）
が現れます。さらに、SN5mailSys.zip を解凍すると、“SN5mailSys”フォルダが出来ます。この中のファイルを対応する、スマホの SD カード、スマホ本体の Download フォルダにコピーしてください。
スマホ起動後に“SN5mail.apk”をインストールしてご利用ください。
最初に、メールサーバーとアドレス帳の設定をします。
アンインストール：スマホの操作で削除できます。PC のデータはフォルダごと削除できます。

スマホでニャン語(Protected Communication System)

目次

スマホでニャン語(Protected Communication System)

特許権、著作権：宇山　靖政

１．保証および法的責任の放棄

このソフトウエアの名称は、”スマホでニャン語(Protected Communication System)”です。
暗号メールに関する特許(Protected Communication System)の内容を実現したものです。

1.1　ご利用は自己責任です。

このソフトウエアに関する本文書の内容には信頼性があり、また正確であるものと確信しております。しかし、著者　宇山靖政　は、いかなる誤り、抜け落ち、また不正確さに対しても、その責任を負うことはありません。

著者　宇山靖政　は本マニュアルの内容およびそこに記述するソフトウエアに関して特定の機能に対する市場性および適合性の保証を始めとして、いかなる、またあらゆる明示的または暗黙の保証を放棄します。

本製品の品質および性能に関する危険（リスク）は本製品の購入者またはユーザーに帰属することになります。著者　宇山靖政　が事前にその可能性について通知を受けている場合においても、かような情報およびソフトウエアの使用に起因するような特殊なまたは結果的な損害を始めとして、いかなる損害に対しても法的責任を負うことはありません。

1.2　日本国内でのみご利用ください。

このメールソフトは、暗号技術の扱いに関する基本技術を特許内容として公開しています。更に次のホームページ（http://www.asahi-net.or.jp/~cq4y-uym/index.html）でメールソフトのソースファイルや暗号ソフトのソースファイルを公開し、その内容を“公知の技術”としています。

“経済産業省の安全保障貿易管理の手引き”では、

2. 技術の提供の場合の主な例（関係法令：貿易外省令第9条）

ア. 公知の技術（※1）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）

a. 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

b. 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

c. 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

d.　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

e.　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

※1　貿易外省令第9条第2項第9号でいう「公知の技術」とは、「不特定多数の者に公開されている技術又は不特定多数の者が入手可能な技術」と規定されています。これは安全保障貿易管理の観点から定義しているものであり、守秘義務の有無にかかわらず、特定少数の者しか知り得ない場合は「公知である」と判断されません。なお、例えば特許法では、社会に対する技術の新規性の観点から「公知」について規定しており、特定少数の者しか知り得ない場合でも、その者に守秘義務が無ければ「公知である」と判断されることとなります。

となっています。したがって、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になります。

しかしながら、暗号通信に関する法律的な規制は国によって異なります。日本国内に住んでいられる皆様が日本国内でご利用になるのは自由に出来ます。したがって、日本に住んでおられる方々の情報は強力に保護できます。

海外出張のためパソコン(外為法の暗号機能に該当のもの)を持ち出す場合、自分が使用するためだけに持ってゆき、他人に売ったり譲渡したりせずに持ち帰る場合は、経済産業省の許可を得なくてもよいという特例があります。ヤマハのヘリコプターの事件もありましたので、**事前に経済産業省に確認**を取ったほうが安全です。

国によっては、全ての通信を傍受して内容をチェックするために、暗号通信の利用に強い制限がかかっている場合もありますので、外国での使用に関しては、その国の法律に従ってください。

日本では、憲法に

第２１条〔表現の自由〕
１　集会、結社及び言論、出版その他一切の表現の自由は、これを保障する。
２　検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。

とあります。このメールソフトを使うと、“通信の秘密は、これを侵してはならない。“の部分が実現できる可能性が強まります。

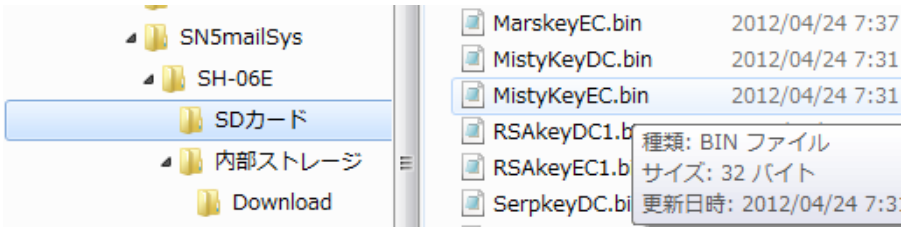
質問がありましたら、作者（宇山靖政）（uyama33@yahoo.co.jp）まで、お問い合わせください。
ただし、貿易管理令により、暗号技術に関する質問には個別にはお答え出来ません。
ホームページに質問内容と回答を掲載します。

２．インストールと起動

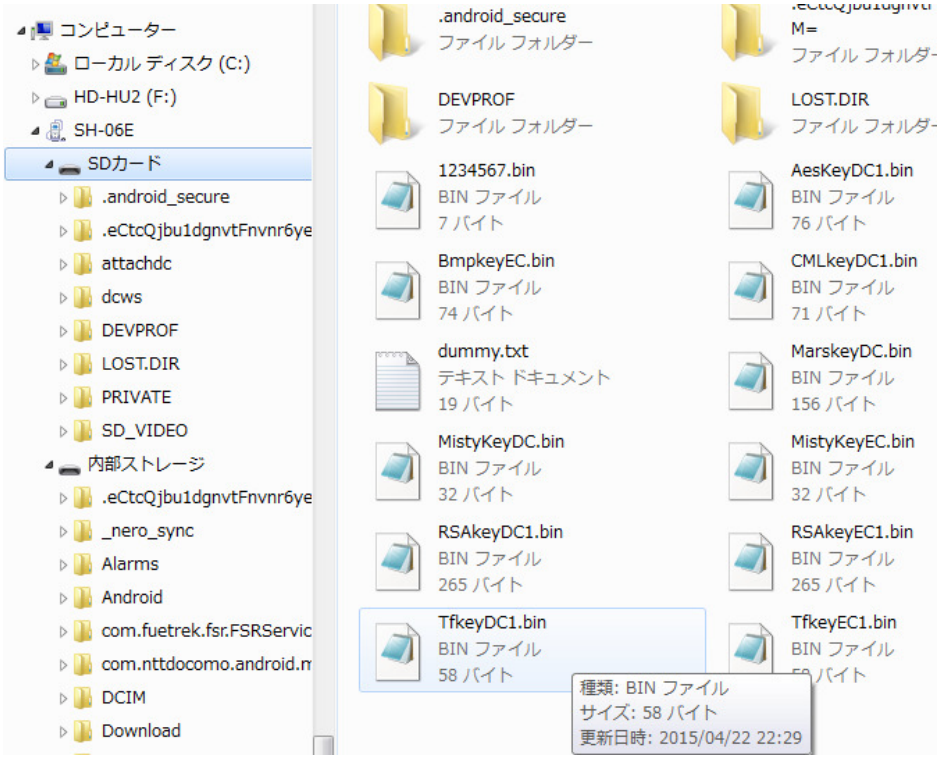
2.1　解凍

インストール：PC で SN5mailPac.zip を解凍すると、このマニュアルの他に、
SN5mailSys.zip　（暗号メールソフトと関連するフォルダ、ファイル）
鍵の見本.zip　（暗号化鍵と復号化鍵の見本）
鍵作成ソフト.zip　（暗号化鍵と復号化鍵を作成するソフト）
が現れます。さらに、SN5mailSys.zip を解凍すると、“SN5mailSys”フォルダが出来ます。この中のファイルを対応する、スマホの SD カード、本体の Download フォルダにコピーしてください。

SN5mailSys　フォルダの中は、次のようになっています。必要なファイルは SD カードフォルダと　Download フォルダの中に入っています。



スマホと PC を USB ケーブルで接続すると、下の図のようにスマホのフォルダが見えます。SD カードのフォルダに PC のほうの SD カードフォルダに入っているのものを全てコピー貼り付けします。
内部ストレージの Download フォルダへは PC の Download フォルダに入っている、SN5mail.apk ファイルをコピー貼り付けします。



スマホと PC を切り離して、スマホで次のような操作をします。

SH ツール（エクスプローラのようなもの）⇒　コンテンツマネージャ　⇒　保存先
⇒　ファイル管理　⇒　Download フォルダ　⇒　SN5mail をダブルタップ

この結果、

このアプリケーションをインストールしてもよろしいですか？このアプリケーションは下記にアクセスるる場合があります：

と言うようなメッセージが出ますが、

インストールを選択　⇒　完了

として下さい。（不安な方は、ソースコードを読んでください。）

スマホ内部でファイルはグループ化されているので、
スマホのダウンロードアプリ　の所を見ると、SN5mail があります。
ダブルタップすれば起動します。

2.2　メールサーバーの設定（SMTP-AUTH、IMAP、POP　設定）

他のメールソフトの、アカウント設定を参考にすると楽に出来ます。サンダーバードなどのアカウント設定などを見ながら設定してください。

ダブルタップで起動すると、次の図になります。

　起動したら、本体のメニューキーをタップして下さい。
下の図の、赤丸のところです。

すると、次の画面になります。

右の、受信設定をタップして下さい。

最初の項目をタップして、展開して様子を見たら、編集中止をタップして下さい。

編集を継続できないのは、次の理由です。

いったん登録したものは、アドレスの部分を修正できない。

従って、あなたの利用するメールサーバーを設定するには、
１．新規作成をタップして、新しくサーバーの設定をする。
２．見本で入っている仮の設定は、
　　項目タップ　⇒　編集　⇒　削除
　　として、削除してください。

アドレス以外の部分はあとから編集できます。

新規作成をタップしてから、あなたが利用している、メールサーバーの設定に従って設定してください。ここで設定される、SMTP サーバーが送信のときに使われます。あなたがメールを送信するときの発信者のアドレスは、ここで設定したメールアドレスの一つでなくてはいけません。なお、SMTP-AUTH 接続ですので、SMTP のポート番号は 587 になります。

設定のときは、必要ない項目は、必ず空欄にして下さい。

以下、具体例を示します。

１． G メールの場合は、次のようになります。
G メールアドレスが、tarou@gmail.com 、 パスワードが、password の場合

User-ID は tarou （@の左の部分）
アドレスは tarou@gmail.com
P W は password
IMAP-H は imap.gmail.com
IMAP-P は 993
SMTP-H は smtp.gmail.com
SMTP-P は 587
POP-H は 空欄
POP-P は 空欄
DL は 3（一度にダウンロードするメール数）
Memo は memo（そのまま）

これで、G メールのサーバーに、IMAP 接続します。

２． Yahoo メールを追加するには、新規作成をタップして、次のように記述します。
Yahoo メールアドレスが、tarou@yahoo.co.jp 、 パスワードが、password の場合

User-ID は tarou （@の左の部分）
アドレスは tarou@yahoo.co.jp
P W は password

IMAP-H は　imap.mail.yahoo.co.jp
IMAP-P は　993
SMTP-H は　smtp.mail.yahoo.co.jp
SMTP-P は　587　　（SMTP-AUTH 接続なので 587 です。）
POP-H は　　空欄
POP-P は　　空欄
DL は　　3（一度にダウンロードするメール数）
Memo は　　空欄（そのまま）

これで、Yahoo メールのサーバーに、IMAP 接続します。

３．POP 接続の追加。

　ASAHI ネットの場合は、新規作成をタップして、次のように記述します。
ASAHI ネットでメールアドレスが、xxxxxxx123@asahinet.jp 、 パスワードが、password の場合

User-ID は　bb77-aaa　　（ASAHI ネット ID、メールのアカウント）
アドレスは　xxxxxxx123@asahinet.jp
P W は　　password　　（プロバイダーから来た書類を見てください。）
IMAP-H は　空欄
IMAP-P は　空欄
SMTP-H は　mail.asahi-net.or.jp（送信メールサーバー）
SMTP-P は　587　　（プロバイダーの指示が無いときは、587　）
POP-H は　　pop.asahi-net.or.jp（受信メールサーバー）
POP-P は　　110　　（プロバイダーの指示が無いときは、110　）
DL は　　3　　（一度にダウンロードするメール数、5 とか 10 でもよい。）
Memo は　　空欄

これで、ASAHI ネットのサーバーに、接続できます。

プロバイダーによって、用語が異なるので注意して下さい。

2.3　アドレス帳の設定

本体のメニューのところをタップして、赤丸の、送信 AD　の部分をタップします。

さらに、一番上の項目をタップすると、次のような画面になります。

ここで、確認したら、もどる　をタップして下さい。

いったん保存したものは、メールアドレスの部分を変更できません。

新規作成をタップして、新しく作成した後に、見本を削除して下さい。
見本の削除は、
削除対象をタップ　⇒　編集　⇒　削除
とします。

試用期間中は、暗号化ソフト(Bmp56EC.exe)、復号化ソフト(Bmp56DC.exe)の組み合わせで暗号化と復号化が体験できます。この場合は暗号化、復号化の鍵は K1234567.bin　から変更はできません。**また、暗号化、復号化の鍵 K1234567.bin の内容を変更しても、無意味です。実際にはその値を使っていないからです。**

ただし、復号化化だけは自由に設定できます。ベクターから正規のユーザーキーを購入すれば、制限が解除されて全ての項目が自由に設定できるようになります。

設定例を示します。

伊藤さんから山田さんに暗号化したメールを送るには、伊藤さんのアドレス帳で

氏名　山田
電子メールアドレス　yamada@yahoo.jp
暗号化ソフト　Bmp56EC.exe
暗号化鍵　K1234567.bin
とします。

山田さんから伊藤さん宛てに暗号化されて送られてきたものを伊藤さんが受け取るには
伊藤さんのアドレス帳で、山田さんのところに

復号化ソフト　Bmp56DC.exe
復号化鍵　K1234567.bin
とします。(試用期間中は自動的に入力されます。)

さらに、山田さんのアドレス帳では
　氏名　伊藤
　電子電子メールアドレス　itou@goo.jp
　暗号化ソフト　Bmp56EC.exe
　暗号化鍵　K1234567.bin
　復号化ソフト　Bmp56DC.exe
　復号化鍵　K1234567.bin
のように設定します。

これで暗号通信ができます。最初は自分宛に、そして自分のフリーメールアドレス宛に送ってみましょう。

削除方法

削除したい項目をタップしてから、編集をタップ。編集画面で削除をタップします。

2.4　暗号メール作成と送信

メール作成は、3 通りの方法があります。

０．　初期画面で、新規作成　を選択。
１．　メールを読んでから、返信　を選択
２．　アドレス帳から、メール　を選択。

初期画面から、メールを作成するには、

右端の、新規作成をタップすると、次のようになります。

発信の部分で使うメールアドレスは、受信設定で使ったアドレスのうちの 1 つではくてはなりません。

宛先のメールアドレス、件名、発信者（自分）のメールアドレスを記入し、内容を記述してください。

右下の送信ボタンをタップすれば送信されます。送信が終了すると前の画面に戻ります。

　添付ファイルを追加することもできます。確認は、添付一覧で行います。
添付追加をタップすると、ファイル検索が出来て、ファイルをタップすれば、添付ファイルとして扱うことが出来ます。実際にどれが添付されるのかは、添付一覧から確認できます。

　メールを読んだ後での返信では、宛先が入力済みの、メール用のエディタが現れます。
件名の入力と、その下の部分に本文を入力します。その後、メニューのメールから送信をタップすれば、送信されます。また、暗号プログラム、暗号化鍵がアドレス帳にセットされているときは、メール本文および添付ファイルが暗号化されて送信されます。

アドレス帳で、暗号化設定がされているときに、
本文の内容は暗号化されますが、件名は暗号化されません。
添付ファイルの内容は暗号化されますが、そのファイル名は暗号化されません。

　暗号化されたときのデータ形式は、一連の暗号化の最後に NekoEC.exe、BmpEC.exe、 Bmp56EC.exe を使ったときはビットマップ形式になります。それ以外は、バイナリデータです。

2.5　（暗号）メールの受信

　起動したときに、あなたのメールサーバーのアドレスが幾つか設定されていれば、一番上の項目あてに送られてきたメールを、幾つか受信した形になっています。

　DL をタップして、次の画面になります。

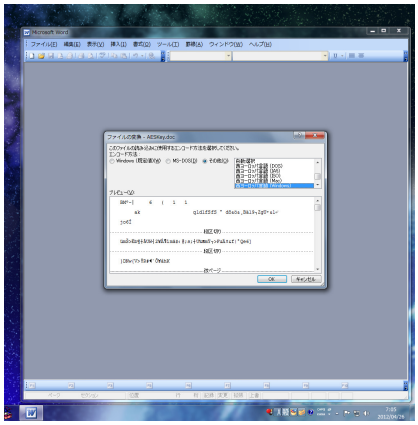
あなたが、メールの受信で使っているアドレスの一覧です。どれかをタップしてから、
メール DL　をタップすれば、設定された個数だけのメールがダウンロードされます。
アドレスにタップしないで、**単に　メール DL　をタップすると、一番上のアドレスについてのメールがダウンロードされます。**
　もう一度、メール DL をタップすれば追加でダウンロードされます。

　ダウンロードしたメールを、タップすれば、読むことが出来ます。
暗号化されていないものはそのまま**（内容：）**と表示されます。
暗号化されて送信されてきたものは**（復号：）**と表示されます。

暗号化されているメールを、ほかのメールソフトで受信すると、ダミーテキストが表示されます。

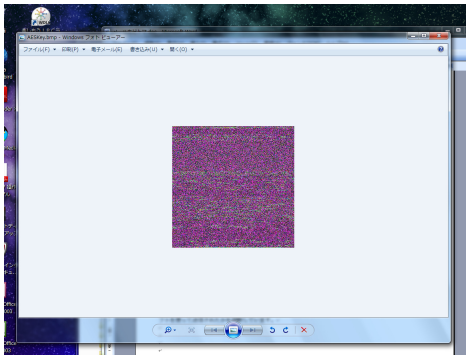
　復号化ソフト、復号化鍵が送信者の暗号化に対応してきちんと設定されていなくてはなりません。

　試用期間でも、ご自分のフリーメールアドレス宛に送信して、その結果もご確認ください。
添付ファイル(test.doc)を付けて、送信した場合は同じ名前のファイルが送られてきますが、そのファイルを保存して、ワードで開こうとすると、下の図のようになり、



開いてもうまく表示できません。

このファイルの拡張子を、bmp にかえて、test.bmp を開くと

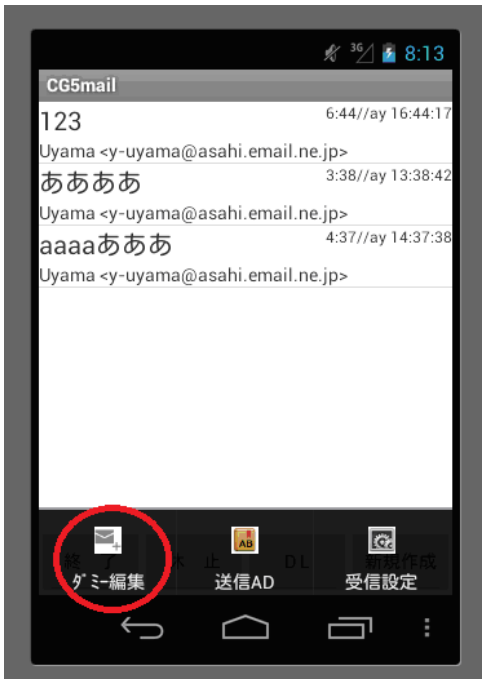


となって、データ形式がビットマップ形式になっていることが分かります。

拡張子を doc に戻してから、保存すれば本来のワード文書にもどります。

2.6　ダミーテキスト編集

本体のメニューボタンをタップすると、次の図になります。



ﾀﾞﾐｰ編集　をタップすると、下の図のようになります。

ファイル名を変更してはいけません。

内容を変更したら、保存終了をタップして下さい。

これは、暗号化メールで本文の代わりとして利用する内容を編集するものです。挨拶くらいにしておいてください。ここで編集して保存した内容が、正規のユーザーが暗号化機能を利用する場合に本文の身代わりとして送信されます。

G メールやヤフーメールでは、この部分がサーバーにおける検索の対象になりますので当り障りの無いものにしておいてください。

３．にゃん語メールの送信と受信

3.1　あなたの猫にメールを運んでもらうには？

世界初の猫語理論による、日本語から世界標準ニャン語への変換と、それを記録したファイルを猫の写真と共に送信するソフトです。

すでに、猫の画像は入っていますので、ヤフーメールなどに送信すると、

のような添付ファイルと、次のメール本文

This is dummy text.

が届きます。

紫色の部分は、メールが国際標準ニャン語に翻訳されたものです。
メールの本文が短いと、紫色の部分は１列か２列の点線のようになります。

受信される方が、ニャン語を日本語に戻す場合は、ソフトの機能は無料で利用できます。
無料で、ベクターからダウンロードして使えます。

もちろん、
世界で一番賢くて、世界で一番かわいい猫は、あなたの飼っている猫です。
その猫に、メールを運んでもらうには次の作業が必要です。

猫の写真を、横幅が 256 ピクセルくらいで、縦幅が 166 ピクセルくらいの大きさで、
１ピクセルの情報が 24 ビットのデータで決定されるビットマップファイルに変換します。

難しそうですが、やってみれば簡単です。次の手順で作業を進めてください。

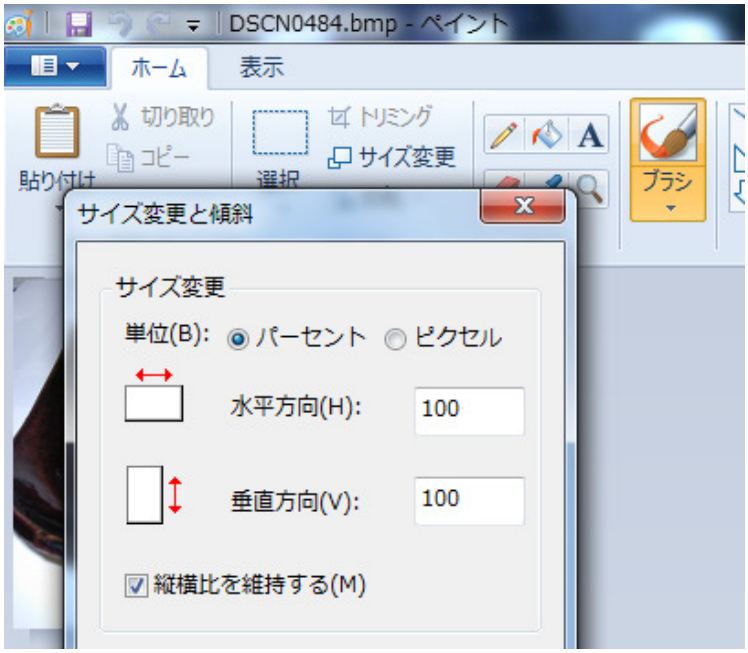
３．　写真をパソコンに取り込む。
デジカメで写真を撮ってください。
ＵＳＢケーブルでパソコンとつないで、写真をデスクトップに置いてください。
写真を右クリックして下さい。

ここで、プログラムから開く(H)を左クリックして下さい。

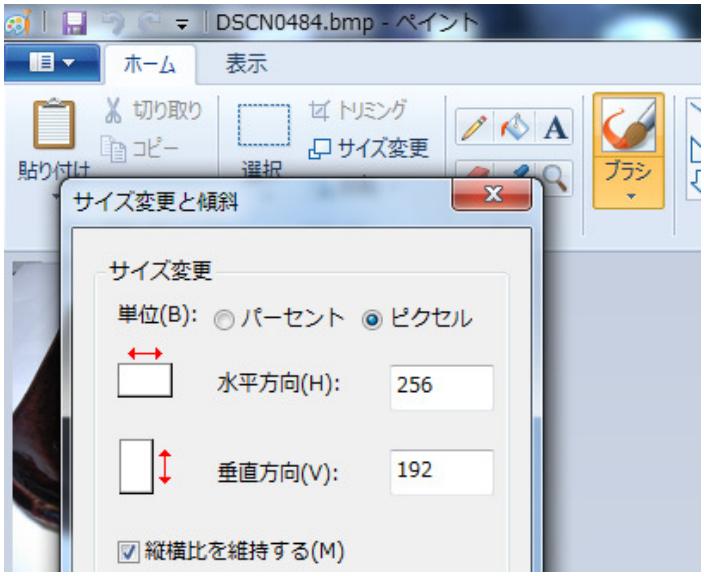
さらに、ペイントの所を左クリックしてください。

4．　ペイントで修正し、保存する。
ペイントのツールを使って、必要な吹き出しを作ってください。
（A のところや、□の所を適当に使う。）

吹き出しの作成後、サイズ変更をクリックします。



上の図は、Windows7 のものです。この場合は、右のピクセルの部分をクリックして、水平方向のところを、256 としてください。

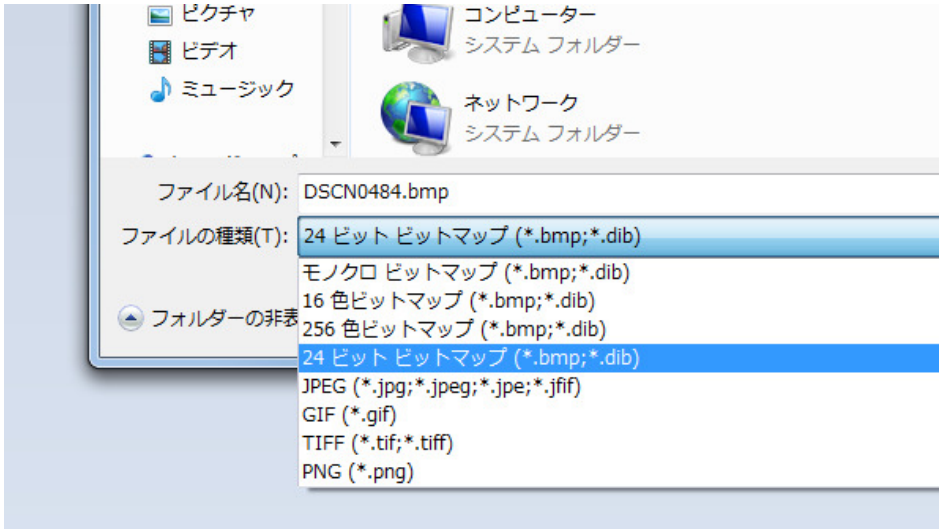


他のバージョンでは、変形のサイズ変更を選択し、サイズ変更で、水平方向、垂直方向の所の値を 50 とか 30 にして、縮小します。横幅の見た目が 5～6 センチ程度になるように調整してください。大きすぎなければ適当でかまいません。

次の作業は最も大切です。正確に行ってください。

適当に縮小したら、ファイルに名前を付けて保存します。

ファイルの種類を、
24 ビット　ビットマップ（*.bmp;*.db）
にしてください。
ファイル名は、必ず
nyanya2.bmp
にしなくてはなりません。（犬が好きな人もこの名前でお願いします。ごめんなさい。）



nyanya2.bmp
のデータサイズは、100ＫＢから 300ＫＢ程度にしてください。
（画像を右クリックしてプロパティーを見て確認してください、）

SD カードの中には、すでに、nyanya2.bmp が入っていますので、あなたの猫の画像 nyanya2.bmp で上書きしてください。このファイル名しか使えません。

3.2　アドレス帳の設定と送受信

アドレス帳の、項目を次のように設定します。(正規ユーザのキーが必要です。)

暗号 1　　nekoEC.exe
暗号鍵 1　　bmpkeyec.bin
復号 1　　nekoDC.exe
復号鍵 1　　bmpkeydc.bin

暗号化ソフトの場所に、nekoEC.exe 暗号化鍵のところは、bmpkeyec.bin
復号化ソフトの場所に、nekoDC.exe 暗号化鍵のところは、bmpkeydc.bin

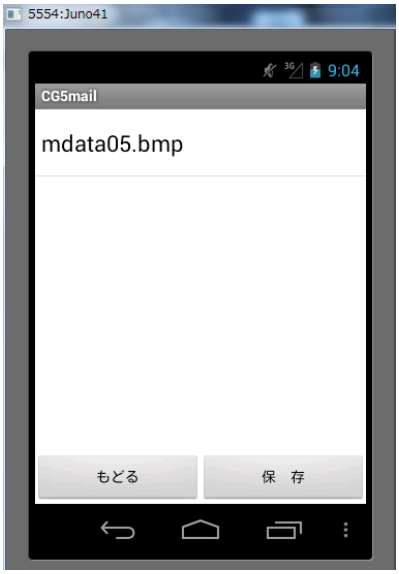
とします。あなたがベクターから正規ユーザーのキーファイルを購入していればこのような設定ができます。

あなた自身の普通のメールアドレスとあなたのフリーメールアドレスも登録して、どちらも同様の内容で設定して置いてください。

ここで使用する暗号化鍵は、Bitoma 暗号で使うものと共通です。新しく鍵を作るときは、BmpCrypt.exe をご利用ください。
作成した鍵を受信者と交換するには、RSA 暗号と楕円曲線暗号が使えます。

賢くてかわいい、あなたの猫がメールを猫語で伝えてくれます。楽しいメールにして下さい。

他の添付ファイルも内容はビットマップファイルですが、ファイル名は元のままです。



本来の添付ファイルに関しては、添付をタップすると、添付ファイルの一覧が出てくるので保存したいものをタップしてから、保存をタップすれば、SD カードの“attachdc”フォルダに保存されます。
送信者のアドレスに対応した復号化ソフトを使って自動的に復号化が行われます。

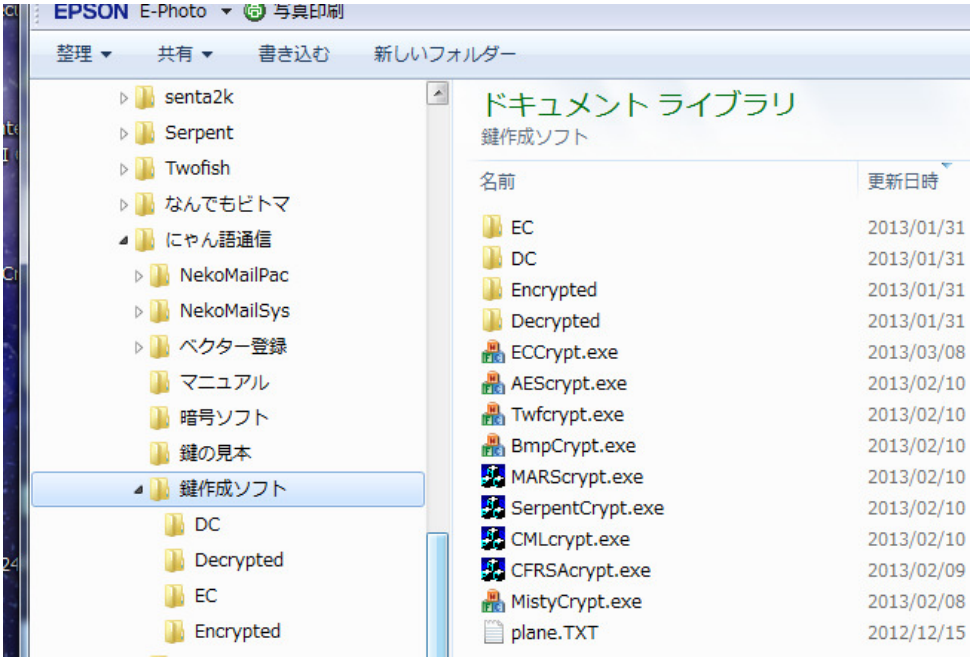
復号化したファイルは他の適切なフォルダに移動してください。そうしないと、さらに同じ作業を繰り返したときに、上書きされてファイルが失われることになります。

3.3　スーパーにゃん語機能（多重暗号化）

ニャン語での送信では、日本語が国際標準ニャン語に変換されますので、世界中の猫は、これを読むことが出来ます。もし、あなたの猫が機密のメールを運ぶときには、次のようにしてスーパーにゃん語機能を利用してください。

鍵作成ソフト.zip を開くと、
鍵作成ソフトのフォルダの中に、暗号鍵を作成するソフトが現れます。
　ここでは、AESCrypt.exe と CMLcrypt.exe を使いましょう。

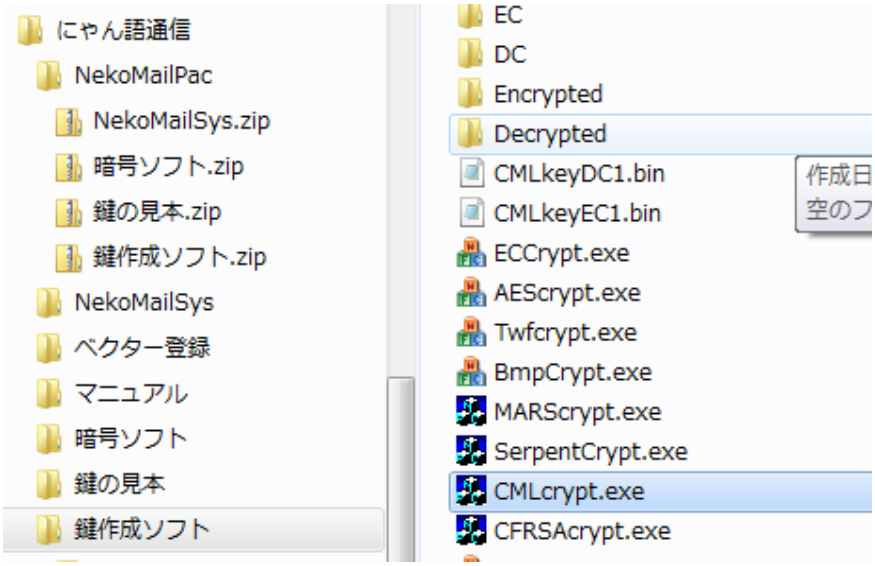
CMLcrypt.exe は日本で開発されたカメリア暗号の鍵を作るソフトです。



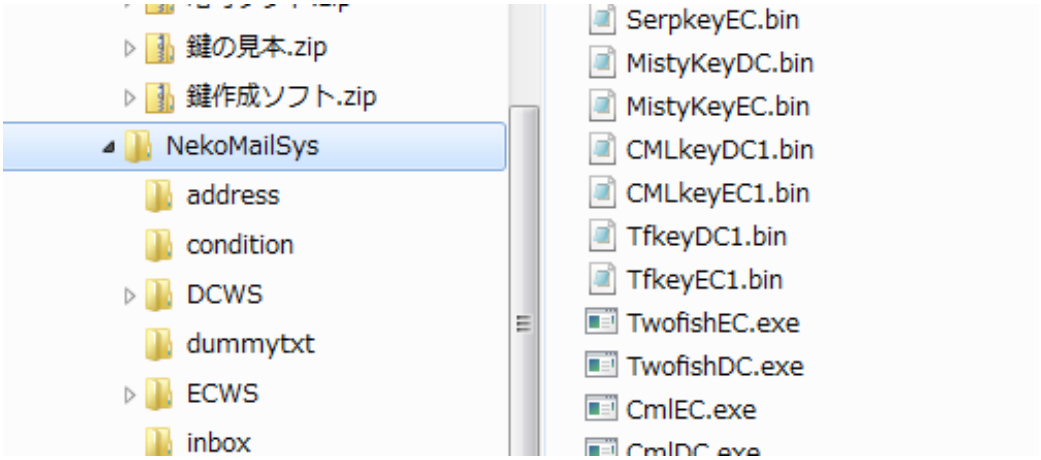
CMLcrypt.exe をダブルクリックすると、

鍵の長さは、256bit、の所をクリックして、次に暗号化鍵名、復号化鍵名を決めます。分かりやすい名前であまり長すぎないようにしてください。
鍵を生成、をクリックすると鍵が作成されます。
保存終了、をクリックすると、

暗号化鍵のファイル CMLkeyEC1.bin と復号化鍵のファイル CMLkeyDC1.bin ができます。



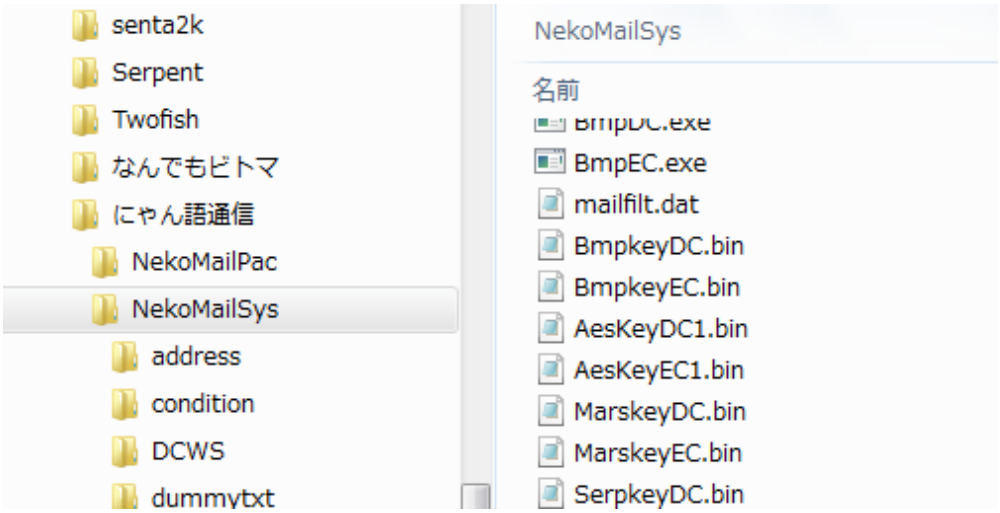
本来は、これを NekoMailSys フォルダのなかに移動するか、ＵＳＢメモリーに保存して使うのですが、
その場合は、通信相手との鍵交換が必要となります。鍵交換は直接あって交換するか、公開鍵暗号を利用して交換することになります。
今回は、すでに入っているものとそのまま使うことにしますので、せっかく作った鍵ですが削除してください。



つぎに、AESCrypt.exe をダブルクリックすると、次の画面が現れます。
ブロックサイズの種類や鍵の長さの種類が普通のＡＥＳよりも多くなっています。これはコンテストに参加したときのままのソースコードを使っているからです。Rijndael （ラインダール）のソースコードは、
The Design of Rijndael: AES - The Advanced Encryption Standard
(Information Security and Cryptography)
に載っていますが、数箇所の誤りがあり修正しました。この修正に関しては著者からその修正が必要であることの確認をとってあります。

可能ならば、ブロックサイズをカメリアの 256bit と変えて、224 か 192bit にして下さい。
この場合は、解読のために扱うブロックのサイズが最小公倍数の 1792bit になります。

でも、すでに存在する、



AesKeyEC1.bin と AeaKetDC1.bin を使うことにしましょう。

アドレス帳の設定は、次のようになります。

暗号１　　CmlEC.exe
暗号鍵１　　CMLkeyEC1.bin
暗号２　　AesEC.exe
暗号鍵２　　AesKeyEC1.exe
暗号３　　NekoEC.exe
暗号鍵３　　BmpEC.bin

復号１	CmlDC.exe
復号鍵１	CMLkeyDC1.bin
復号２	AesDC.exe
復号鍵２	AeskeyDC1.bin
復号３	NekoDC.exe
復号鍵３	BmpkeyDC.bin

アルファベットは全て小文字にしてもかまいません。

このように設定してから、送信すればカメリア暗号とＡＥＳ暗号で２段階に暗号化されたデータがさらに、にゃん語に変換されて相手に届くことになります。

これを、スーパーにゃん語機能とよびます。

４　暗号ソフトの利用

4.1　UserKey.dat

現在、SD カードにある”userkey.dat”というファイルは正式のものではありません。
ベクターに送金後に入手できる同名のファイルで、上書きすれば機能制限が解除されます。
購入したライセンスキーは、同時に 1 台のマシンにおいてのみ使用を許可します。複数台のマシンにおいて本ソフトウェアのライセンスキーを登録する場合は、マシンの台数分のライセンスキーを購入してください。

試用期間中の動きは次のようになります。

1．登録できる暗号化ソフトは Bmp56EC.exe だけです。さらに、暗号化鍵は “K1234567.bin” だけです。
　復号化は 5 段階まで自由に設定でき、復号化鍵は自分で作成したものが利用できます。

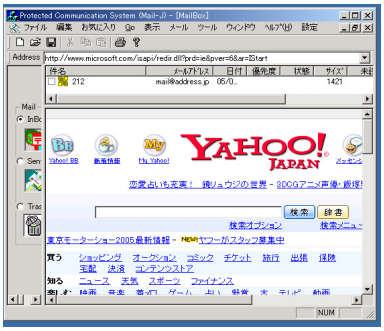
2．このとき、本文と添付ファイルは、データ内容がビットマップ形式として暗号化された添付ファイルとして送信されます。また、本文の代わりにダミーテキストが送られます。

ベクターから購入した正規の”userkey.dat”がある場合は、次のようになります。

1．暗号化、復号化を 5 段階まで自由に設定できます、暗号化鍵は自分で作成したものが利用できます。
　暗号化ソフトがアドレス帳の受信者となる人の欄に登録されている場合
　本文の代わりにダミーテキストが送信されます。
　本文と添付ファイルを暗号化されて送信されます。

2．暗号化ソフトが登録されていない場合
　本文はそのままで暗号化されないで送信されます。添付ファイルも暗号化されません。

4.2　(Web)フリーメールの暗号化



Hotmail　や　Yahoo メール　などの、無料のメールサービスが提供されています。この無料アドレスを使用する場合について考えます。
無料の理由は、ユーザーのメールの内容を解析して、商業活動に役立てるためです。
さらに、サーバーが攻撃されてログイン ID とパスワードが大量に公開されてしまって、他の人に乗っ取られたり、メールの内容を見られたりしています。
たとえ、無料のメールサービスでも暗号化しておくほうが安全です。この“スマホでニャン語”では、アドレス帳を適切に設定して多重暗号化をすることができます。

現在は、クラウドシステムのように、大量のデータが自分の手を離れた形で保存されている状態があります。このようなデータは、しっかりと暗号化されている必要があります。このときの暗号化方式や暗号強度は自由に設定できなくてはなりません。

クラウドデータの暗号化には、“メールもビトマ”や”Web 暗号通信 GY”　をご利用ください。

暗号化で、G メール、ヤフーメールなども安全に使えます。

4.3　利用できる暗号アルゴリズム

利用できる暗号ソフトは、Neko, AES、Camellia、Misty、Twofish、Serpent、Mars、Bitoma、Bmp56です。さらに、鍵作成ソフトの RSA, ECC が有るので、公開鍵暗号を使って、共通鍵の交換をすることもできます。
自分宛のメールで、大きな添付ファイルを送ってみて処理速度、安定性を確認のうえで本格的な使用を開始してください。

データの形式がビットマップ形式になるのは、
NekoEC.exe　　（復号化には　NekoDC.exe　を使います。）
Bmp56EC.exe　（復号化には、Bmp56DC.exe　を使います。）
BmpEC.exe　　（復号化には、BmpDC.exe　を使います。）
です。
これらを、多段階の暗号化の最後の段階で利用すれば図形となったデータが相手に届くことになります。
NekoEC.exe（復号化には　NekoDC.exe　を使います。）による、スマホでニャン語では、日本語が国際標準ニャン語になるのはもちろんですが、ニャン語にするまえに、AES 暗号で暗号化して、さらに Camellia 暗号で暗号化してから、最後に、ニャン語に直すことが出来ます。ニャン語になったデータは、あなたの可愛い猫の写真と一緒になって相手に届きます。前もって暗号化した場合は、 AES、Camellia の鍵を受信者に送っておく必要があります。このためには、公開鍵暗号である RSA 暗号と楕円曲線暗号を利用できます。
国際標準ニャン語ですので、普通の猫は読めます。猫に読んでもらうときに、猫がちゃんと読めたならニャンと鳴き、読めないときはワンと鳴きます。

BmpEC.exe（復号化には、BmpDC.exe　を使います。）では、メールデータが四角い抽象画になって相手に届きます。
NekoEC.exe　　（復号化には　NekoDC.exe　を使います。）
BmpEC.exe　　（復号化には、BmpDC.exe　を使います。）
では、共通の暗号化鍵、復号化鍵を使います。この鍵は、BmpCrypt.exe　で作成します。
Bmp56EC.exe（復号化には、Bmp56DC.exe　を使います。）はデータを抽象画に変えますが鍵は変更できません。
Bitoma, Neko は、処理速度に問題はありませんが、データサイズが 2 倍になります。

高速な処理が可能な対称鍵暗号で、世界的にも評価の高い暗号ソフトとしては、
AesEC.exe　　（復号化には、AesDC.exe　を使います。）　――　AES 暗号
TwofishEC.exe　（復号化には、TwofishDC.exe　を使います。）　――　Twofisah 暗号
SerpentEC.exe　（復号化には、SerpentDC.exe　を使います。）　――　Serpent 暗号
MarsEC.exe　　（復号化には、MarsDC.exe　を使います。）　――　Mars 暗号
CmlEC.exe　　（復号化には、CmlDC.exe　を使います。）　――　Camellia 暗号
MistyEC.exe　（復号化には、MistyDC.exe　を使います。）　――　Misty 暗号
が入っています。

このうちで、AES、Camellia、Misty は有名ですが、他のソフトも優秀です。
AES は、アメリカの新暗号規格（Advanced Encryption Standard）として規格化されたものです。
Twofish, Serpent, MARS　などは AES の良きライバルです。
Camellia は AES と同等の安全性があり、さらにサイズが小さく、高速な暗号化、復号化が可能です。欧州のNESSIEプロジェクトや日本のCRYPTRECが作成した「電子政府推奨暗号リスト」に採用されています。

MISTY は三菱電機が開発した秘密鍵暗号アルゴリズムにより、128bits の暗号化鍵を持つ 64bits ブロック暗号。大量の平文と暗号文の組み合わせを使って暗号を解読する差分解読法や線形解読法を応用した、独自の暗号強度評価指標に基づいて設計され、DES などをしのぐ安全性と実用性を実現している。W-CDMA の標準仕様に採用されて、日本初の世界標準暗号となりました。

各アルゴリズムとも、平文ファイルを暗号化する暗号化ソフト、暗号化されたファイルを復号化する復号化ソフト、暗号化鍵や復号化鍵を作る鍵作成ソフトの 3 つからなっています。暗号ソフトと復号化鍵はすでに、SN5mailSys フォルダに入っています。
各暗号ソフトの詳しい説明は、ホームページ（http://uyama22.pa.land.to/）で確認してください。

これらの暗号ソフトを、5 段階まで適用して 5 重に暗号化できます。様々な暗号技術を多重に適用して通信の秘密を守ります。最新の暗号技術の発展に合わせて使用する暗号化ソフトを今後も提供します。

このソフトによって、アドレス帳に暗号化ソフト名、暗号化鍵のファイル名、復号化ソフト名、復号化鍵のファイル名を登録するだけで、様々な暗号技術を簡単に利用できるようになります。
この方式は、さまざまな暗号化方式のソフトが利用できるので、情報を強力に暗号化して送信できるようになります。それぞれの目的にあった形で十分な暗号強度を持ったものを利用できるようになります。

これらの暗号で使う対称鍵を互いに交換しなくてはなりません。
“メールもビトマ”や”Web 暗号通信 GY”では、鍵交換で利用する公開鍵暗号のソフト、

CFRSAEC.exe　（復号化には、CFRSADC.exe　を使用します。）　――　ARS 暗号

が含まれています。
RSA 公開鍵方式、楕円曲線暗号での暗号化や復号化は処理時間が長くなるので、大きなデータを送信するときの、送信途中での暗号化には向きません。
鍵交換のために、楕円曲線暗号(ECC)のソフトも追加しました。

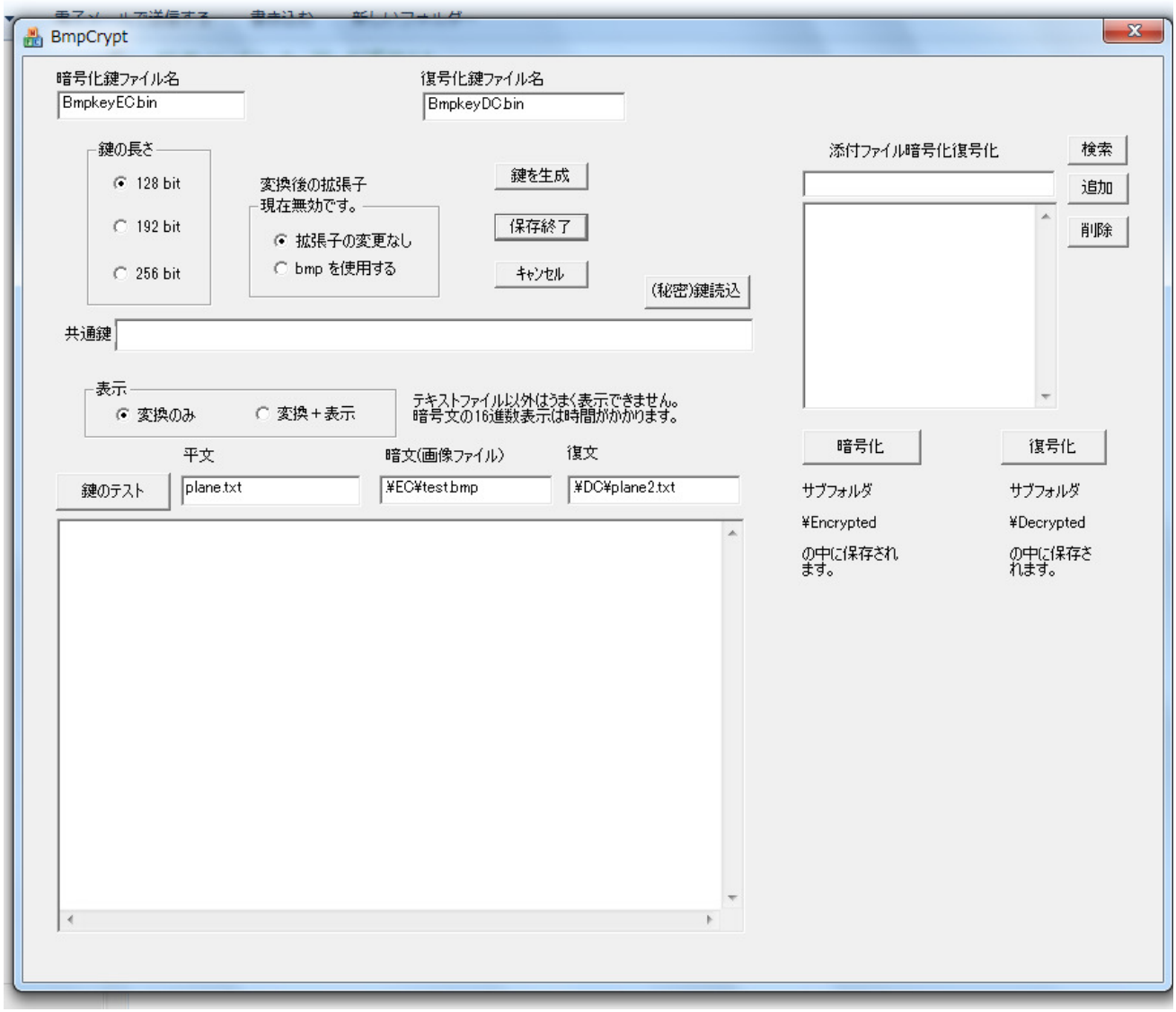
共通鍵（秘密鍵）方式のものでも処理速度には差があります。利用可能なものの中では、Serpent がやや時間がかかるようです。ご自分のコンピュータで十分テストしてください。
暗号メールに楽しさを加えようと考えて作った NekoEC.exe, BmpEC.exe ですが、画像として暗号化したときのデータサイズが大きくなってしまいます。
暗号化したデータの送受信のテストを十分に行ってください。

５　鍵作成ソフト

5.1　鍵作成ソフトの使い方

　サンプルの暗号鍵は、すでに NekoMailSys に入っています。
　鍵を新たに作成する場合は、“鍵作成ソフト.zip”を解凍します。そして鍵作成ソフトのフォルダの中に入っている鍵作成ソフトを起動します。

たとえば、BmpCrypt.exe を起動すると、下の図のようになります。
このソフトは、NekoEC.exe, BmpEC.exe、NekoDC.exe, BmpDC.exe で使う鍵を作成します。



操作手順：
１．暗号化鍵ファイル名、復号化鍵ファイル名を入力する。
　　鍵のファイルは基本的には、鍵作成ソフトと同じフォルダに作成されます。
　　以前作ったものと名前が同じだと前のものが上書きされて消えてしまいます。

５．　　鍵の長さを決定する。
　　ボタンをクリックしてください。

６．　暗号化した後のファイルの拡張子を決定する。
この場合は、暗号化した後ではファイルはビットマップファイルという画像ファイルになります。
拡張子が bmp にしてあれば画像として扱われ暗号化後のファイルを画像として見ることができます。

７．　鍵を生成
鍵を生成　のボタンをクリックしてください。鍵が作成されます。もう一度クリックすると別の鍵が作成されます。

８．　保存終了
鍵作成ボタンをクリックしてから、保存終了をクリックすれば同じフォルダに鍵が保存されます。

９．　鍵のテスト
鍵のテストボタンをクリックすると、作成した鍵による暗号化と復号化の様子が一番下の窓に表示されます。テキストファイルしか表示できませんので、もとのデータがワードの文書のような場合はうまく表示できません。暗号化した結果は変換後のデータを 16 進数で表示します。

１０．途中経過の表示
表示　の部分の選択で、暗号化、復号化のと中継かを表示するか否かを選べます。表示には長い時間と大きなメモリーが必要です。途中経過を表示しなくても結果は直接確認できます。

ここで、鍵作成とその鍵を使った暗号化と復号化のテストができます。鍵作成ボタンをクリックしてから、保存終了をクリックすれば同じフォルダに鍵が保存されます。他の鍵作成ソフトも同様です。
鍵の長さは可能な範囲で自由に設定できます。鍵を生成するときは鍵の名前に十分注意してください。同じ名前で生成された鍵はすでに使っているものを上書きしますので、復号化が出来なくなる可能性があります。鍵ファイルの最後の数字を変えるか、もっと分かりやすい名前にするか工夫してください。
本格的な運用では、鍵は新たに作成したものをお使いください。作成した鍵を SD カードにコピーしてください。

使用する暗号と鍵を SD カードにコピーしたら、アドレス帳に登録します。あなたが、MistyEC.exe と MistykeyEC.bin を使って暗号化したデータを、B さんに送るなら、B さんに MistykeyEC.bin と同時に作成されたところの、MistykeyDC.bin を事前に B さんに手渡してください。
そして B さんのアドレス帳のあなたの項目で、
復号化のところを、MistyDC.exe、MistykeyDC.bin と設定してもらってください。

直接会って鍵交換するのが難しい場合は、公開鍵暗号 RSA がありますので、それを利用してください。使い方や設定方法は、鍵の交換の項目で詳しく記載します。

B さんは、あなたから受け取った MistykeyDC.bin を BmpMailSys の中に入れます。名前がぶつかるなら、ファイル名を BmpkeyDC2.bin などと変更し、復号化鍵の登録内容も BmpkeyDC2.bin と変えます。

暗号通信をする相手の方が、貴方に送るデータを暗号化するように設定してもらってください。もちろん暗号化ソフト、

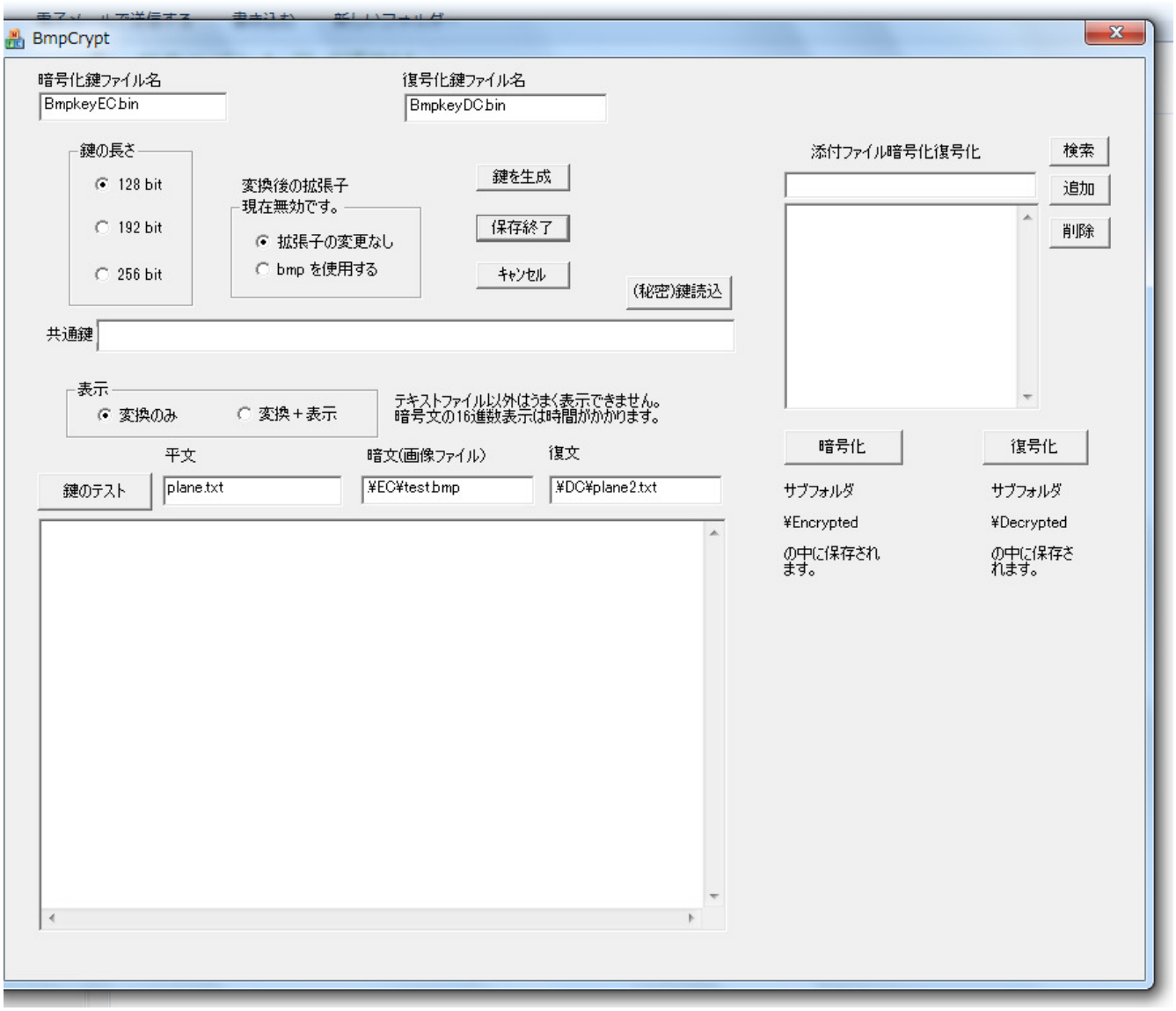
処理速度、変換前と変換後のデータサイズの変化について、十分注意して確認してください。
送信する相手のコンピュータの処理速度、相手のプロバイダーで受信できる添付ファイルの大きさの上限についても配慮してください。

鍵作成ソフトのフォルダには、
AESKey.exe, BmpKey.exe, CMLkey.exe, MarsKey.exe, MistyKey.exe, SerpentKey.exe, TwofishKey.exe, CFRSAKey.exe が入っています。それぞれが、対応する暗号化ソフト、復号化ソフトのための鍵を作成します。ひとつひとつ確認しておきます。

AEScrypt.exe, は AesEC.exe, AesDC.exe で使う暗号化鍵と復号化鍵を作ります。

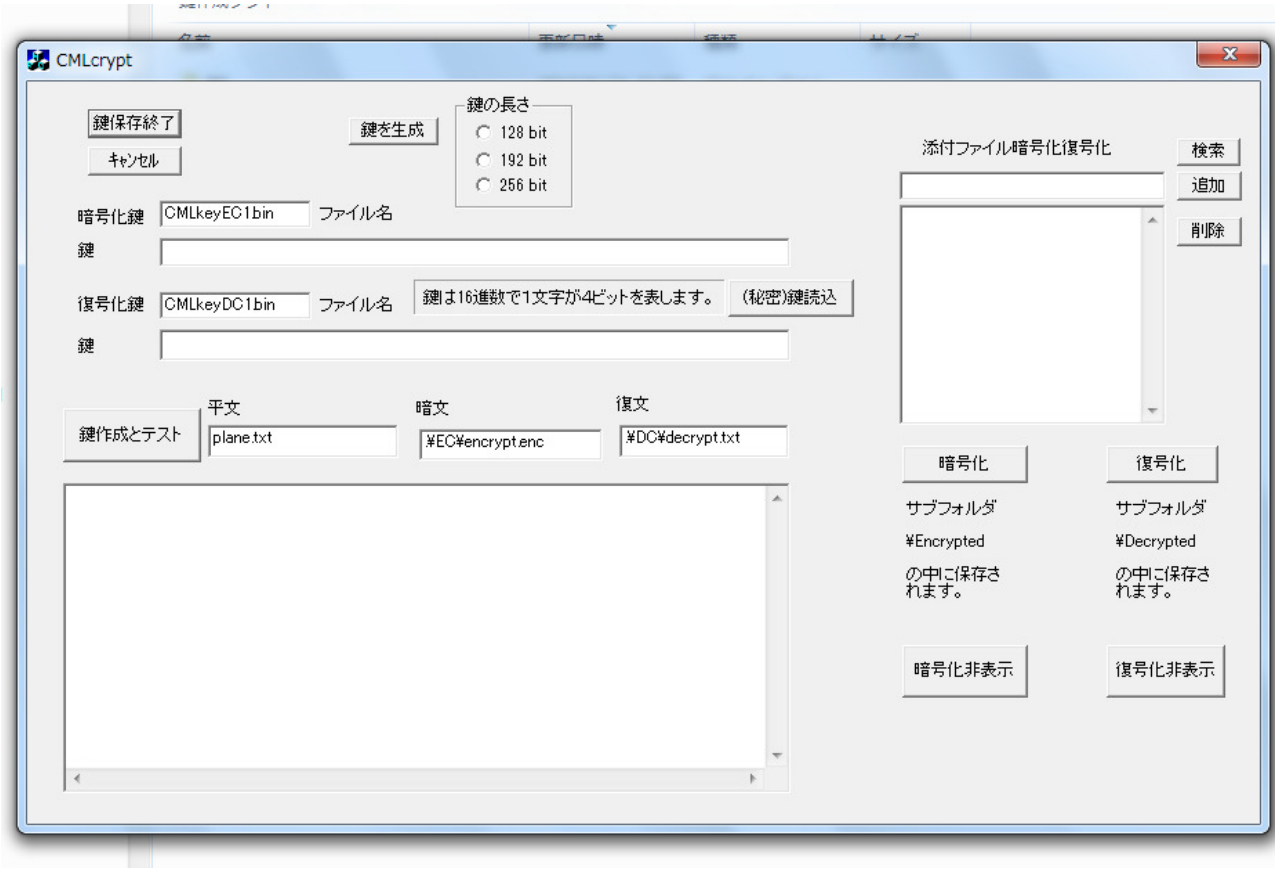
これは、アメリカの新暗号規格（Advanced Encryption Standard）AES として規格化されたものよりも、鍵のサイズ、ブロックサイズの種類が多くなっています。応募したときの古い形のままにしました。
多重暗号化したときに、ブロックサイズが互いに異なるほうが解読しにくいと考えます。

BmpCrypt.exe,　は　BmpEC.exe, BmpDC.exe で使う暗号化鍵と復号化鍵を作ります。
NekoEC.exe,NekoDC.exe　でもこの鍵を共通で使います。



　このソフトでは、変換後のデータサイズが 2 倍近くなってしまいます。画像としての扱いはよいのですが、メールサーバでのデータサイズの上限にはご注意ください。

CMLcrypt.exe, は　CmlEC.exe, CmlDC.exe で使う暗号化鍵と復号化鍵を作ります。

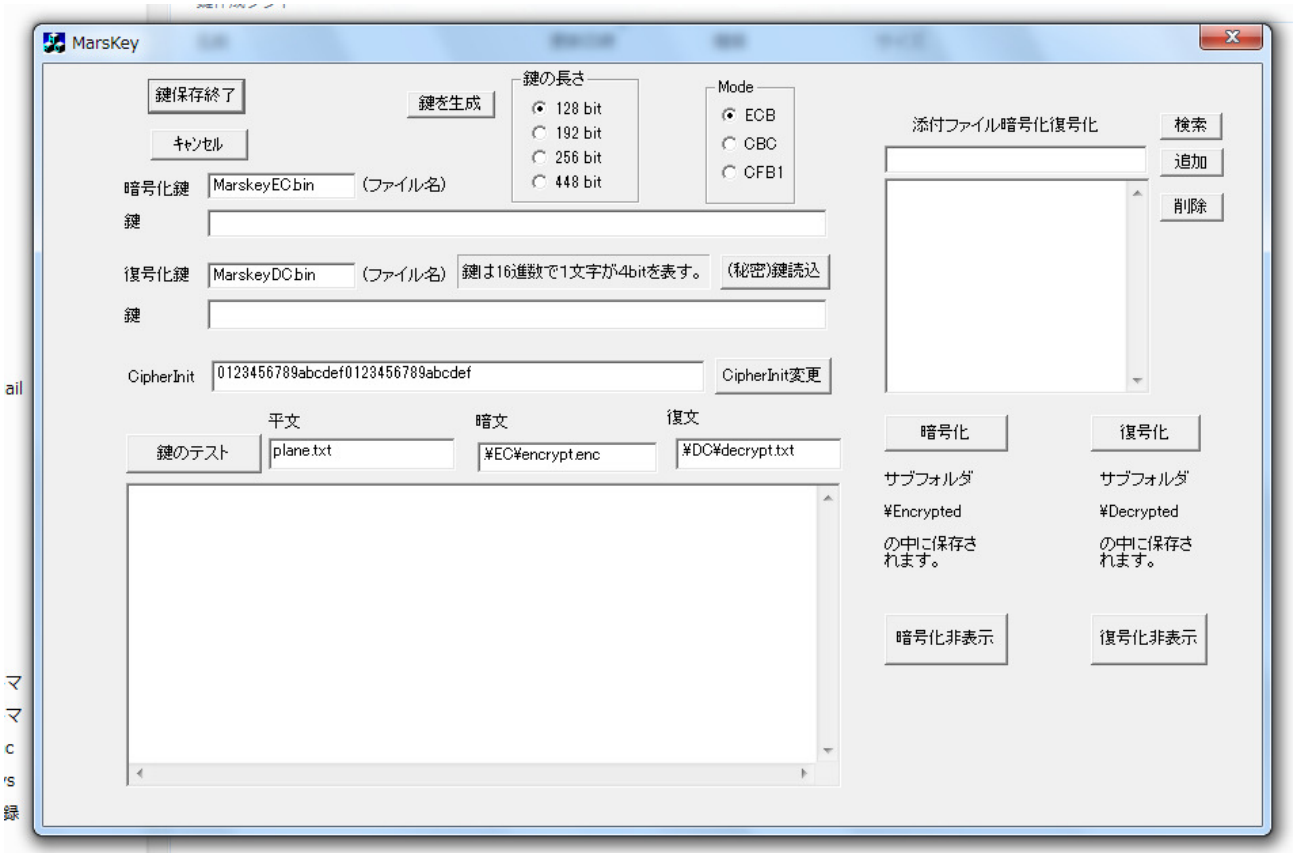


鍵の長さを選んでから鍵を生成します。鍵の表示場所が 2 箇所ありますが、共通鍵ですから同じ値になります。

鍵のテストでは、平文にエクセルファイルや、ワード文書を選ぶと表示はうまくできませんが、暗号化は行われていますのでご安心ください。

カメリアは日本で作られた優秀な暗号ソフトです。

MarsCrypt.exe, は　MarsEC.exe, MarsDC.exe で使う暗号化鍵と復号化鍵を作ります。



これは、IBM が作成した暗号ソフトです。AES 暗号の候補でもありました。

他のものより設定が複雑ですが、あまり気にしないでクリックして下さい。
設定するのは、ファイル名、鍵の長さ、モード、初期値です。
初期値は、CipherInit 変更　をクリックするだけです。何回かクリックしてみてください。
モードは
暗号文に変換するときの方法を決めます。これも適当に設定してください。
鍵の長さは、長くすると計算時間が少し長くなります。気にするほどではありません。

そして、テストしてから、鍵保存終了　で終わりです。

MistyCrypt.exe, は MistyEC.exe, MistyDC.exe で使う暗号化鍵と復号化鍵を作ります。

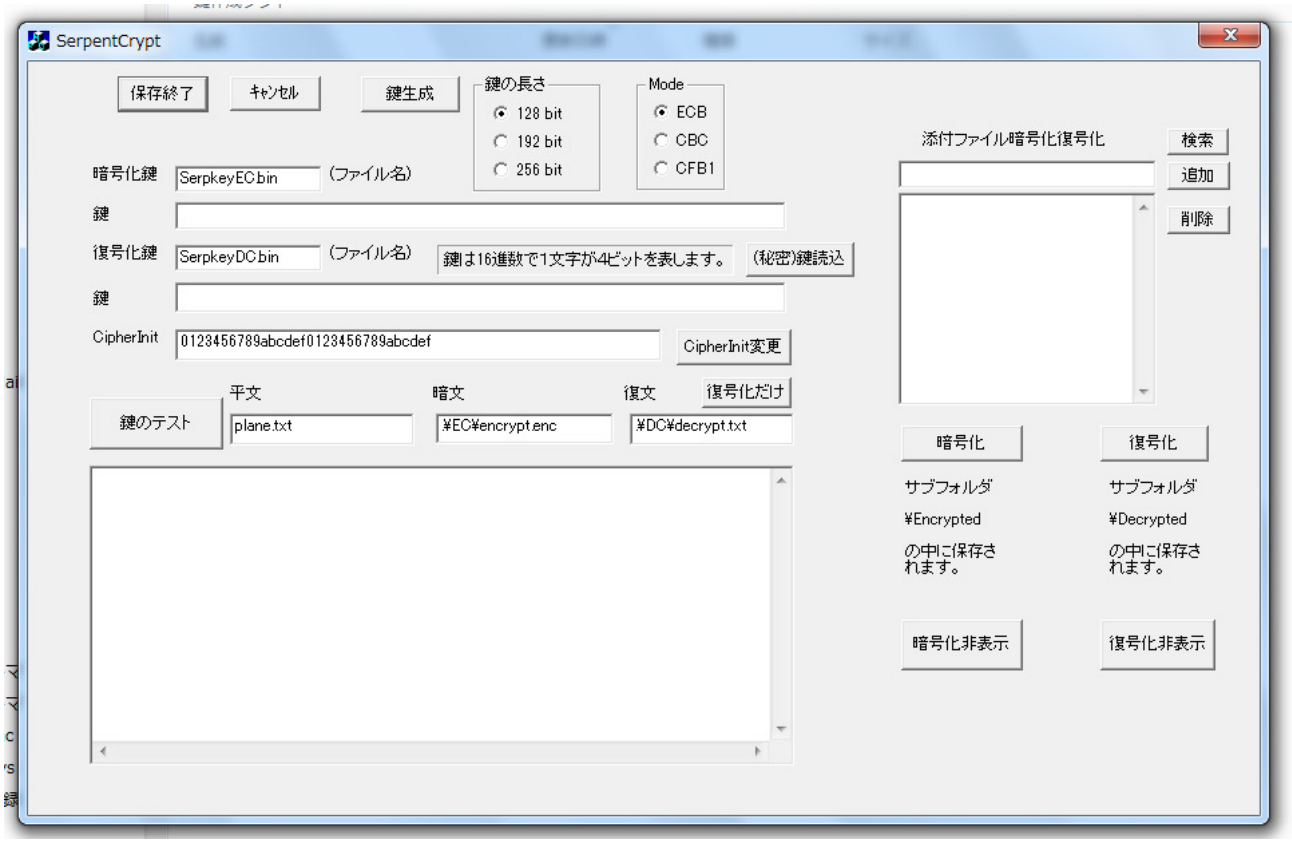
日本製の、軽量で高速な暗号ソフトです。

鍵作成は、鍵作成ボタンをクリックします。クリックするたびに新しい鍵が作成されます。

Test をクリックすると、暗号化の様子だけが表示されます。

そして、保存終了　で鍵のファイルが同一のフォルダに保存されます。

SerpentCrypt.exe, は SerpentEC.exe, SerpentDC.exe で使う暗号化鍵と復号化鍵を作ります。



　他のものより設定が複雑ですが、あまり気にしないでクリックして下さい。
設定するのは、ファイル名、鍵の長さ、モード、初期値です。
初期値は、CipherInit 変更　をクリックするだけです。何回かクリックしてみてください。
モードは
暗号文に変換するときの方法を決めます。これも適当に設定してください。
鍵の長さは、長くすると計算時間が少し長くなります。気にするほどではありません。

そして、テストしてから、鍵保存終了　で終わりです。

TwfCrypt.exe, は TwofishEC.exe, TwofishDC.exe で使う暗号化鍵と復号化鍵を作ります。

　設定するのは、ファイル名、鍵の長さ、モードです。
モードは、暗号文に変換するときの方法を決めます。これも適当に設定してください。
鍵の長さは、長くすると計算時間が少し長くなります。気にするほどではありません。

そして、テストしてから、鍵保存終了　で終わりです。

ただし、Bmp56EC.exe, Bmp56DC.exe のための暗号鍵は、作成できません。
また、RSA 暗号、楕円曲線暗号に関連するものは次の項目で説明します。

5.2　RSA 暗号の使い方

公開鍵暗号 RSA 方式のソフトは、“メールもビトマ”、"Web 暗号通信 GY” における共通鍵（対称鍵）の交換のために作成しました。貿易管理令に違反しないようにソースコードを HP で公開します。
鍵は、512 ビット、1024 ビット、1536 ビット、2048 ビット、2560 ビットの長さの鍵を扱えるようにしました。（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、3.5 時間です。メモリーの量や CPU の性能で異なります。）
公開鍵暗号は処理速度が遅いので、メールの送信途中での暗号化に利用すると、時間がかかりすぎてサーバーとの接続が切れてしまう恐れがあります。小さなデータの交換に利用するか、事前に暗号化したものを添付ファイルとして送信するようにする必要があります。

この鍵作成ソフトは公開鍵、秘密鍵を別々に登録し、別々に機能させることもできますので、
相手から受け取った公開鍵で、必要なファイルを暗号化してから、相手に送信すればよいのです。

共通鍵方式（対称鍵方式、秘密鍵方式）と呼ばれる方式では、この共通鍵を秘密にしておかなくてはなりません。自分が作成した鍵をどのようにして相手に届けるかが問題となります。
直接会って受け渡しができればそれでかまいませんが、会えない場合には公開鍵暗号を利用します。

電子署名と PKI

さらに、公開鍵暗号方式を使用して電子署名というものが実現できます。この仕組みを、PKI といいます。これは公開鍵暗号の有効な使用方法だと言えますが、問題点もあります。

RSA 暗号では、公開鍵で暗号化したものを秘密鍵で復号化することが基本ですが、逆に秘密鍵で暗号化したものを、公開鍵で復号化できます。

秘密鍵は、鍵を作成した人だけが所有し、秘密にしておく性質のものです。
セットになっている公開鍵で復号化出来るのは、セットになっている秘密鍵で暗号化されたものだけです。もし、秘密鍵が盗難にあっていなければ、不正にコピーなどされていなければ、公開鍵で復号化できるデータは、秘密鍵の所有者によって暗号化されたと言えます。

RSA 暗号では、「片方の鍵を使って暗号化したものはそれと対になっているもう一方の鍵を使用しなければ復号化できない」のです。これはすなわち、公開鍵で暗号化したものは秘密鍵でしか復号化できないということとともに、秘密鍵で暗号化したものは公開鍵でしか復号化できないということでもあります。電子署名ではこれを利用します。
「公開鍵はだれにでも公開しているものなんだから、秘密鍵で暗号化することって意味がないんじゃないの？」と思われる方もいるかもすれませんが、ところが、これが大いに意味があるのです。
電子署名の原理は、A さんが B さんにある文書を送ろうとしている。この文書（平文）とともに、文書を自分の秘密鍵で暗号化したものを一緒に送るのです。この 2 つを受け取った B さんは、まず暗号化された文書を A さんの公開鍵で復号化する。それと平文を比較する。これが一致したとき、どのようなことが言えるだろうか。それは、「その文書は A さん以外のだれかによって改ざんされていない」ということが言えるのである。なぜならば、公開鍵を用いて復号化できる＝それは対応する秘密鍵、すなわち A さんのみが持つ秘密鍵で暗号化された＝暗号化したのは A さんに間違いない、という考え方が成り立つからです。（図 1）

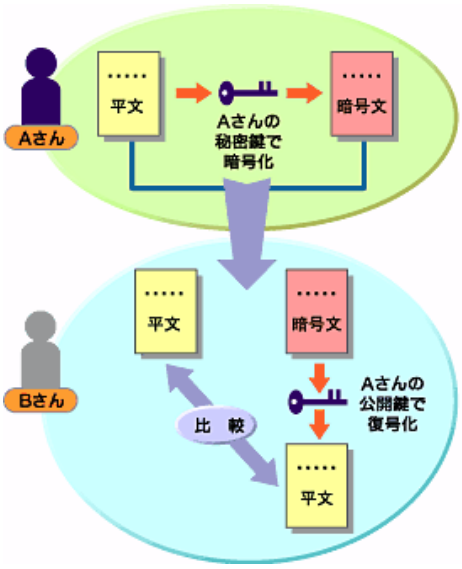


図 1　電子署名の考え方

しかし、この方法には大きな欠点があります。
それは、安全性を求めて鍵の長さを大きくすると暗号化や復号化に時間がかかるのです。電子メールで大きなデータを扱うときは、送信の途中で暗号化したり、受信の途中で復号化したりしようとすれば、タイムアウトでサーバーとの接続が切れてしまう恐れがあります。
そこで、ハッシュ関数を使ってもとの文章から得られた小さなデータ（ハッシュ値）を秘密鍵で暗号あする方法を取ります。

ハッシュ関数とは、以下のような特徴を持つ関数です。
元データの長さに関係なく、ハッシュアルゴリズムの出力値（これをハッシュ値という）は必ず決められた長さ（128 ビットや 160 ビット）になる。
元データが少しでも異なれば、ハッシュ値は大きく異なる。
ハッシュ値から元データを推測することはほぼ不可能である。

このような理由から、平文のハッシュ値を平文の代わりに秘密鍵で暗号化するという形が一般的です。（図２）

A さんは、平文から、ハッシュ関数を使ってハッシュ値を計算します。ハッシュ関数には、MD5, SHA-1, SHA-2 などいろいろありますが、SHA-1, SHA-2 が使えます。さらに、SHA-2　には、4 種類の関数があります。

この電子署名によって、「なりすまし」「改ざん」のリスクを回避することができ、結果として「否認」のリスクも回避することができることになります。

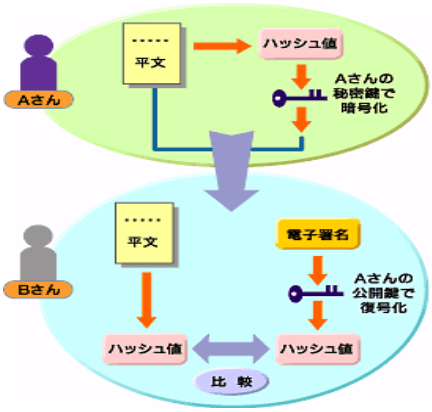


図２　ハッシュ関数での電子署名

日本でも電子署名法（正式には「電子署名及び認証業務に関する法律」）が国会で可決され、施行されます。
この電子署名法は、電子データの文書に電子署名がされた場合、押印がされたものと同等の効力を持たせること、そして特定の基準を満たした認証局については「特定認証業務」というお墨付きを与えようというものです。

もちろん、認証局を使っていないので法律的な効力はありません。しかし、改ざんを防ぐことに関しては、十分な強さを持っていると考えます。

具体的な手順を見てゆきます。

電子署名の作成

実際に電子署名を付加する手順を確認します。
(1) 相手に送信したい情報（平文）のハッシュを作成する。(SHA-2 を利用)
(2) 作成したハッシュの内容を自分の(RSA 暗号の)秘密鍵で暗号化する（これが電子署名となる）
(3) 平文と電子署名のペアを相手に送る

電子署名の検証

受け取った側の検証手順は次のようになります。
(1) 相手の公開鍵を入手する
(2) その公開鍵で送付された電子署名を復号化する
(3) 送付された平文から、相手と同じアルゴリズムを用いてハッシュを作成する

（4）（2）の結果と（3）で作成したハッシュを比較する

2 つの値を比較した結果、両者が一致すれば送り手が署名してから受け手が署名を検証するまでの間にその文書が改ざんされていないことが検証されたことになります。

問題点：
公開鍵と秘密鍵の持ち主は誰か？

公開鍵と電子証明書
公開鍵はだれが入手してもよく、どんな方法で相手に渡してもかまわないのです。では、公開鍵を受け取った人は、どのような方法でその持ち主を確かめるのでしょうか？
公開鍵の持ち主（＝その公開鍵に対応した秘密鍵の持ち主）を証明するものとして「電子証明書」というものが存在し、その証明書を発行する機関を「認証局」という。A さんの公開鍵を受け取ったら（実際には証明書の中に公開鍵が含まれた形になっている）、証明書の内容に不備がないか、そしてその証明書を発行した認証局が信頼できる認証局かどうかで確認するということになるのですが、認証局による身元調査の確実性はどの程度なのでしょうか？

身元調査の仕方にはいろいろあります。個人なら戸籍謄本、職場での素行調査、資産調査、生育暦に沿っての経歴調査、指紋や DNA での確認、兄弟や親との DNA 比較などです。
犯罪ですが、戸籍を買うこともできますので、本人確認はかなり難しいことになります。どこまでやるかで費用もだいぶ違ってきます。日本の戸籍を持っていた外国のスパイの例もあります。買い取った戸籍に記載された人物として普通に仕事や生活をしていたら、本来の戸籍の持ち主の指紋でもない限り、嘘を見破ることはできません。生まれたときに全員の指紋と DNA を登録させれば判別できるようになります。
したがって、証明書の効力についても、しっかり考える必要があります。

個人宛の証明書の発行の実際：
無料で、個人の証明書を発行してくれる機関もあります。お金がかかるので、その個人の存在や名前などの正しさに関する調査はしません。偽名でとった、ヤフーアドレスがあるなら、その偽名のままでヤフーアドレス宛に、証明書が送られてきます。　証明しているのは、ヤフーのアドレスが存在していることだけです。本当は誰が使っているかは分かりません。証明書の内容が信頼できる根拠は見つかりません。

”スマホでニャン語”では、知り合いや信頼できる相手との通信を想定していますので、本人確認の電子証明書は扱いません。

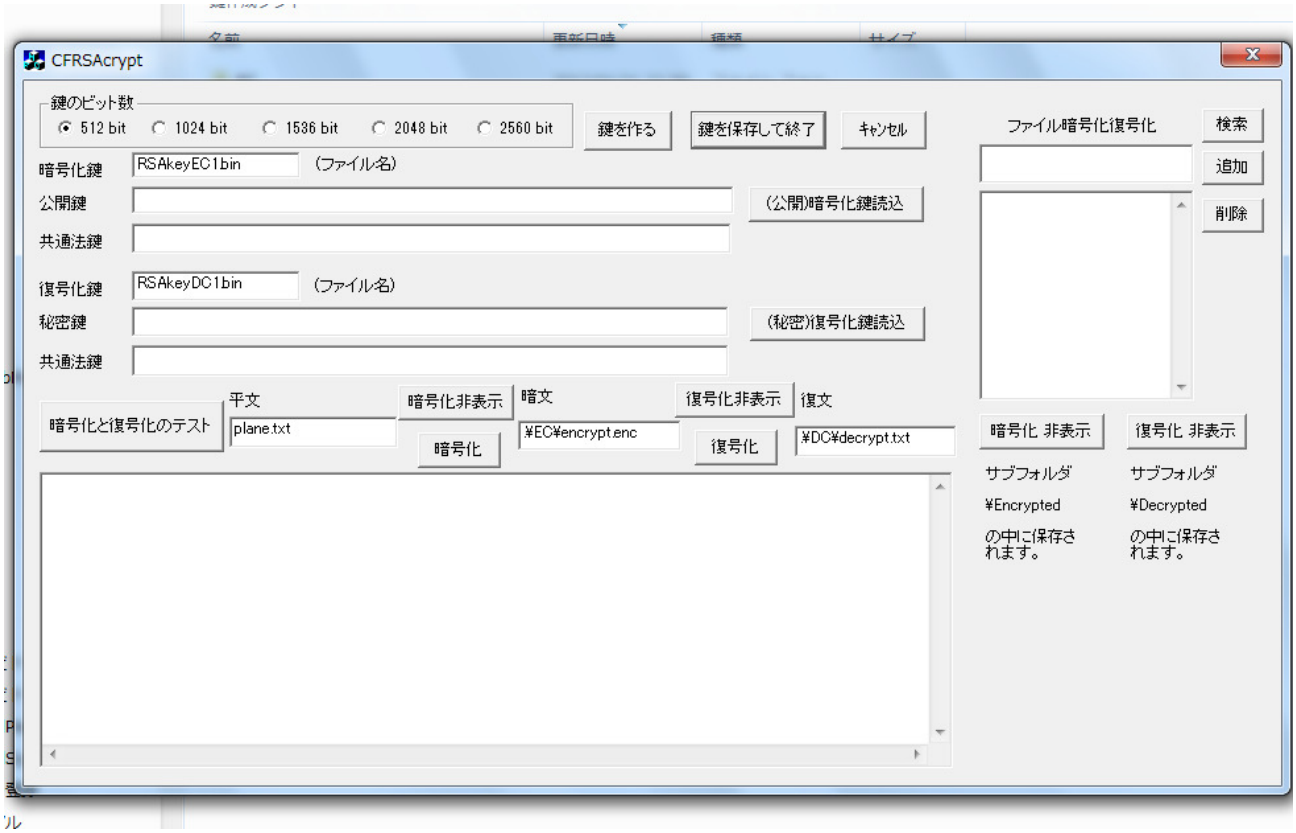
また、最近話題になった、
http://www.gizmodo.jp/2015/02/pc_superfish.html
レノボ製の 2014 年 9 月～12 月製造（lenovo 発表）のパソコンに工場出荷の段階で「セキュアな取引きまで傍受できる」とんでもないアドウェアがプリインストールされていたことが、同社フォーラムに寄せられた苦情多数で明らかになりました。
ソフトの名前は「Superfish」。グーグルの検索結果やサイトを開くとユーザーの許可なしにサードパーティー製の広告を挿入するアドウェアで、少なくとも Chrome や IE では動作が確認されています。
広告挿入もひどいけど、問題はそれだけじゃありません。こやつ、自己署名証明書を自己発行して、偽の SSL 証明書を生成し、SSL 通信の中身まで覗けるようにする不届き者なのです。俗に言う「オレオレ証明書」。

などもあるので、証明書を使う方は、よく注意して下さい。

RSA 鍵作成ソフトを使っての対象鍵の交換

最初は、鍵作成ソフトの機能から説明します。

これは、"CFRSAEC.exe","CFRSADC.exe"で使う暗号化、復号化の鍵を作成します。



操作について

1．鍵のビット数
あなたがお使いのコンピュータばかりではなく相手の使用しているコンピュータの計算能力を考える必要があります。長い鍵ではメモリーの量が問題になります。鍵を作るための時間ほどではありませんが、暗号化、復号化にも時間がかかります。
　ですが、相手に合わせて何種類も作成すると区別するのが大変になります。その場合は鍵交換用のシステムを利用してください。
2．鍵を作る　をクリックしてしばらくお待ちください。
3．暗号化と復号化のテスト　これをクリックすると暗号化、復号化が連続して行われます。
表示できるのはテキストファイルです。暗号化したものは 16 進数で表示されます。
4．暗号化　暗号化の過程を表示しながら暗号化します。
5．暗号化非表示　暗号化の過程を表示しないで暗号化を実行します。
6．復号化　復号化の過程を表示しながら復号化します。
7．復号化非表示　復号化の過程を表示しないで復号化します。
8．（公開）暗号化鍵読込　暗号化に使う公開鍵を読み込みます。
これが、読み込んであれば、暗号化、暗号化非表示　ができます。
9．（秘密）復号化鍵読込　復号化に使う秘密鍵を読み込みます。
これが、読み込んであれば、復号化、復号化非表示　ができます。

この鍵作成ソフトだけで処理する場合は、次の様になります。

あなた（アリス）が相手（ボブ）に、対称鍵暗号（秘密鍵暗号）で使う暗号化の鍵を送りたいときは次の手順になります。

１．相手に送る対称鍵暗号（秘密鍵暗号）を作成します。この鍵作成ソフトと同一のフォルダに置いてください。

２．ボブに、RSA で使う鍵を作成してもらい、公開鍵をメールの添付ファイルとして送ってもらいます。
　この公開鍵は秘密にする必要はありません。

３．受け取ったボブの公開鍵のファイルを、同一フォルダの置いてください。

４．（公開）暗号化鍵読込　をクリックして、受け取った公開鍵を登録します。

５．平文　の所のファイル名を対称鍵暗号（秘密鍵暗号）ファイルの名前にしてください。たとえば、"eckey.bin"とします。

６．暗文　の所にファイル名は必ず異なる名前にしてください、たとえば、"eckey2.bin"などです。

７．これ"eckey2.bin"を、相手に普通のメールソフトを使って添付ファイルとして送信します。そのとき、相手に、本来のファイル名を伝えること、復号化には使っている公開鍵のファイルに対応した秘密鍵を使って実行するように依頼してください。

８．相手（ボブ）に、メール用のシステムでの、アドレス帳におけるあなたの項目において、復号化した鍵を登録してくれるように依頼します。

注意：
　鍵のセットを作成したらどの鍵がセットになっているかを間違えないようにしてください。
作成した暗号化鍵を相手に送ります。秘密鍵を他の人に知られてはいけません。
相手から、公開鍵を受け取ったらそれを使って共通鍵を暗号化します。暗号化した共通鍵を相手におくります。公開鍵が誰から送られてきた公開鍵かが分からないと大変です。
　自分の公開鍵で暗号化されて送られてきた共通鍵は、公開鍵とセットの秘密鍵で復号化します。相手に合わせて公開鍵と秘密鍵のセットを作る場合はセットの管理にご注意ください。
“メールもビトマ”、"Web 暗号通信 GY”を使って、鍵交換用のフォルダを作り、鍵交換専用のシステムでの管理を薦めます。

まとめ：
　１．暗号通信の送受信者がそれぞれ公開鍵暗号 RSA での公開鍵を作成し、相手にそれぞれ送ります。
　２．それぞれが、対称鍵による暗号化アルゴリズムを決定しその暗号化鍵のファイルを作成します。
　３．１で受け取った公開鍵で、暗号化鍵ファイルを暗号化して相手に送ります。
　４．３で受けとたファイルを復号化して、暗号化ソフトとセットにしてアドレス帳に登録します。

“メールもビトマ”、または"Web 暗号通信 GY”を使って、鍵交換用のフォルダを作り、鍵交換専用のシステムとして利用する場合は次のようになります。

１．鍵交換用　というフォルダを作り、その中に"Web 暗号通信 GY”を展開します。

２．お互いに、"CFRSAKey.exe"　を使って、それぞれが公開鍵と秘密鍵を作成します。

３．アリスが作成した公開鍵を"AOpenkey.bin"、秘密鍵を"ASeckey.bin"。
ボブが作成した公開鍵を"BOpenkey.bin"、秘密鍵を"BSeckey.bin"。とします。

４．アリスは、ボブから公開鍵を受け取ります。これは秘密にする必要がないので普通のメールに添付してかまいません。ボブもアリスからの公開鍵を受け取ります。

５．アリスは､”鍵交換用”フォルダにある､”暗号通信”のアドレス帳のボブの項目の暗号化ソフトの部分に、"CFRSAEC.exe”を登録します。暗号化鍵の部分には、ボブから受け取った”BOpenkey.bin"を登録します。これで、ボブから受け取った公開鍵で暗号化したデータをボブに送信できます。
復号化ソフトの部分には､"CFRSADC.exe"を登録します。この復号化で利用する鍵は､"ASeckey.bin"です。

６．ボブは､”鍵交換用”フォルダにある､”メールもビトマ”のアドレス帳のアリスの項目の暗号化ソフトの部分に、"CFRSAEC.exe”を登録します。暗号化鍵の部分には、アリスから受け取った”AOpenkey.bin"を登録します。これで、アリスから受け取った公開鍵で暗号化したデータをアリスに送信できます。
復号化ソフトの部分には､"CFRSADC.exe"を登録します。この復号化で利用する鍵は､"BSeckey.bin"です。

７．この設定によって、メールの文章、添付ファイルともに、RSA 暗号で暗号化されます。ただし、変換に時間がかかるので、データは最小にしてください。
　添付するのは鍵のファイルのみ。文面は、使用する暗号方式と順序、対応する鍵の名前のみにしてください。

８．鍵交換用のシステムで受け取った場合は、そのまま復号化できます。

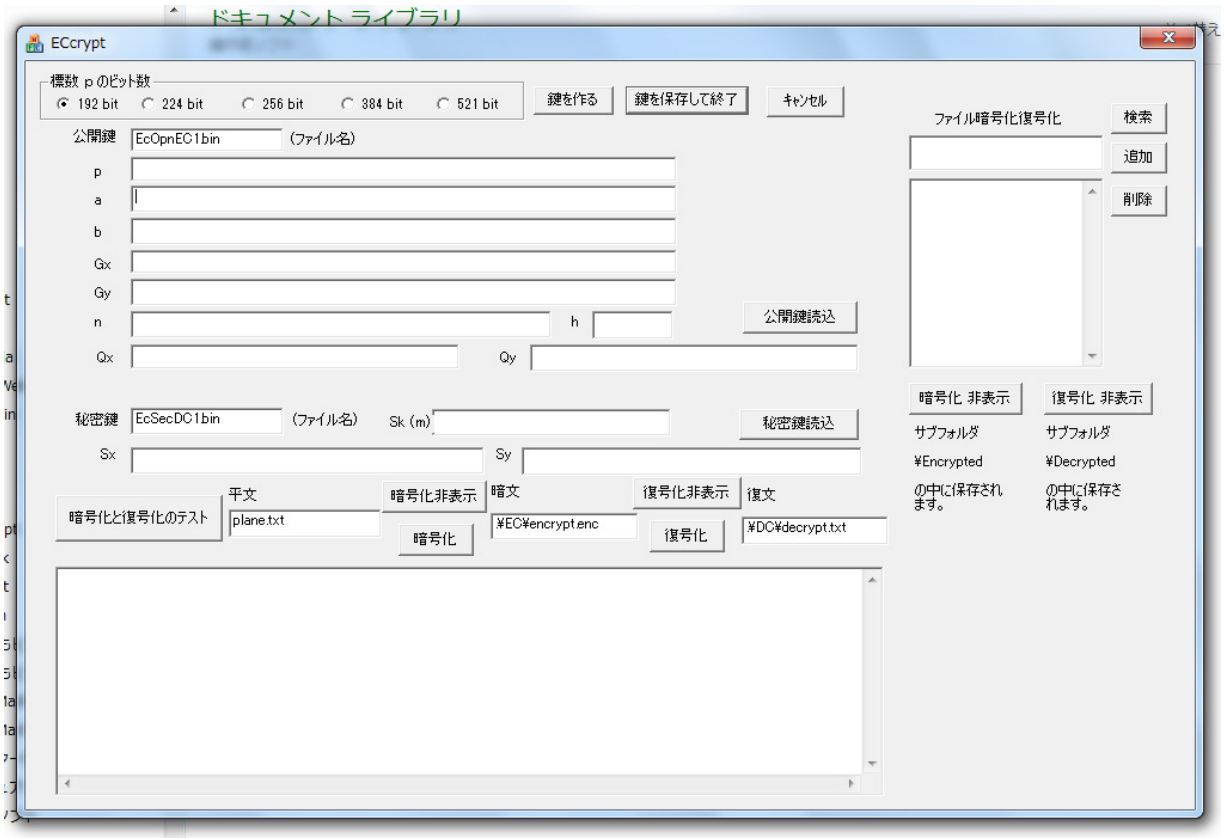
９．ほかのメールソフトで受け取った場合は、添付ファイルを適当なフォルダに移動し、鍵交換用システムでのツールの復号化で復元できます。

１０．受け取った対称鍵（秘密鍵）をメール用のほうに移動してから、そちらで設定してから利用してください。

いくつかの公開鍵と秘密鍵のセットを利用する場合は鍵交換用のほうに登録しておくほうが便利です。

5.3　楕円曲線暗号を使った対称鍵の交換

ECCrypt.exe を起動すると次のようになります。



通信の仕方は次のようになります。

アリスの作業
1．素数 p のビット数を決定する。192,244,256,384,521 ビットから選ぶ。
2．鍵を作る　ボタンをクリックする。
3．公開鍵、秘密鍵の名前、Ao***, As***　を決める。
4．鍵を保存して終了する。
注意：
　現在は、素数のビット数を選ぶと、楕円曲線のパラメータ　T = (p, a, b, G, n, h)　が 1 組決まります。
　秘密の値　m　は乱数として決定されます。m　の値は、113 ビットから 392 ビットの間に設定しました。
　この値　m　は秘密にしておきます。
5．相手（ボブ）に、(T , mG) を送る。（これが公開鍵）

ボブの作業
1．アリスから送られた公開鍵を読み込む。これで素数 p のビット数が決まる。
2．鍵を作る　ボタンをクリックする。
3．公開鍵、秘密鍵の名前、Bo***, Bs***　を決める。
4．鍵を保存して終了する。
5．アリスの公開鍵を読み込む。自分(ボブ)の秘密鍵を読み込む。

６．ECcrypt.exe　と同じフォルダに対称鍵をおく。
７．暗号化する対称鍵の名前を、平文のところに設定する。
８．暗文、復文の名前も設定する。
９．暗号化のボタンをクリックする。
１０．暗号化された対称鍵をアリスに送る。

アリスの作業
１．ボブから送られてきた暗号化された鍵を暗文のところにセットする。
２．自分（アリス）の秘密鍵を読み込む。
３．復号化のボタンをクリックする。
４．復文の作成し、メールもビトマで利用する。

以上です。

ECcrypt のソースコードについては、著作権を主張します。
このソフトは、楕円曲線暗号の公開鍵と秘密鍵を作成し、暗号化、復号化の様子を確認するためのソフトです。暗号化したものは、16 進数の列として表示します。

楕円曲線暗号での暗号化の仕組みは次のようになります。

アリスの作業
１．楕円曲線のパラメータ　T = (p, a, b, G, n, h)　を選ぶ。
２．秘密の値　m　を選ぶ。（これは秘密にしておく）
３．相手（ボブ）に、(T , mG) を送る。（これが公開鍵）

(T , mG) を使って行われる、ボブの作業での、プログラムの動作
４．ファイル全体を分割する。
５．分割した各部分を数値 X1　とみなす。
６．整数値　X1+α　に対して、P = (X1+α , Y) が楕円曲線の上に載るようにする。
７．秘密の値　k　を決める。
８．kG を作り、ファイルの先頭に置く。
９．アリスから受け取った、(T , mG) を利用して、P+kmG を計算してファイルに書き込む。
１０．　ファイルの終わりまで繰り返し終了したら、それをアリスに送る。

アリスの作業でのプログラムの動き
１１．ファイルの先頭から、kG を取り出す。
１２．自分の持っている値　m を使って、mkG を計算する。
１３．ファイルの残りの各ブロックに対して、(P+kmG)－mkG ＝P　を計算する。
１４．P　の x 座標（X1+α）を取りだして、X1 = (X1+α)－α　を計算して並べる。

これらの計算で、必要となるものは
１．多倍長整数の計算
２．ヤコビ記号の計算
３．平方根の計算
４．楕円曲線上の点の k 倍の計算
です。
RSA 暗号を作るときに作成したものを少し変改し、さらに新しい関数を少し追加しました。

これは、楕円曲線暗号を利用した公開鍵暗号のソフトで、“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。パラメーラーに関しては、

Standards for Efficient Cryptography
SEC 2: Recommended Elliptic Curve Domain Parameters
Certicom Research
Contact: Daniel R. L. Brown (dbrown@certicom.com)
January 27, 2010

にある値を利用しました。

GF p での p の値は、192 ビットから、521 ビットの間です。 k および m の値は、113 ビットから 392 ビットの間に設定しました。
ファイル全体を暗号化出来ますが、とても時間がかかります。RSA 暗号が速く見えるほどです。したがって、対称鍵の暗号化にしか利用できません。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 で公開します。

多倍長整数の計算は、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ます。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。
ヤコビ記号の計算と平方根の計算、素数生成、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、

Journal of Applied Sciences 5 (4): 604-633, 2005
ISSN 1812-5654

Theory and Implementation of Elliptic Curve Cryptography

Kefa Rabah
Department of Physics, Eastern Mediterranean University, Gazimagusa, North Cyprus, via Mersin 10, Turkey

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。

このソースコードについては、著作権を主張します。技術内容を公知の技術にするために、HP でソースファイルを公開します。

６．操作方法の補足

6.1　メイン画面

　起動すると、次の画面になります。あなたの受信用のメールサーバーが設定されていれば、
一番上に設定されているメールアドレスとそのメールサーバーから、設定した数だけのメールを受信した状態で起動します。

　上のほうにメニューが並びますので左から順に説明します。
4.1.1　終了　　アプリを終了します。
4.1.2　休止　　アプリは休止状態で、ほかのアプリの後ろに回ります。
4.1.3　DL　　メールをダウンロードします。
4.1.4　新規作成　　新しいメールを作成して、送信します。

　本体のメニューボタンをタップすると、次の画面になります。

　ここで、ﾀﾞﾐｰテキストの編集、アドレス帳の編集、あなたのメールサーバーの設定を行います。

4.2 アドレス帳

アドレス帳が開いたときに、現れるメニューを左から説明します。

4.2.1　もどる　　編集を中止して、前の画面に戻ります。
4.2.2　メール　　対象となっているアドレスに向けたメールを作成します。
4.2.3　新規　新しいアドレスを作成し登録します。
4.2.4　編集　登録内容を編集します。

　削除方法
削除したい項目をタップしてから、編集をタップ。編集画面で削除をタップします。

５．多重暗号化：

暗号化技術の発展は同時に解読技術の発展でもあります。これに対応するために多重暗号化を採用します。多重暗号化によって解読困難とする事が出来ます。このメーラーは送信する内容を異なる暗号ソフト、暗号化鍵を用いて５回まで多重暗号化できるようになっています。もちろん同じアルゴリズムと異なる鍵の組み合わせでの多重暗号化も可能です。

5 回までの多重暗号化ですが、ビットマップにする暗号化を採用すると、データサイズが大きくなります。たとえば、５段階の暗号化で、２Ｍバイトのデータが５Ｍバイトのサイズになっていました。

米国での標準暗号(AES)や、ヨーロッパで採用された Camellia なども利用できますので、個人的な情報を守るには十分であると考えています。できるだけ最新の暗号化方式を組み合わせて利用することをお勧めします。

多重暗号化では、
暗号化ソフトは送信するデータに対して、１，２，３，４，５の順で使われますが、
復号化では受信したデータに対して、５，４，３，２，１の順に使われます。
したがって、対応するソフトが同じ番号のところに設定されます。
これについては、（注意２）をご覧ください。

最後が、BmpEC.exe で暗号化された場合は、データの形式はビットマップ形式になっています。ファイル名はもとのままです。したがって、ABC.doc が元のデータで、多重暗号化の最後が BmpEC.exet として送られてきたデータを他のメールソフトで受信して保存してから、拡張子を bmp に変更すれば図形としてみることができます。

このメールソフトで受信してそれを保存すると、保存の過程で復号化されて、本来のワードのデータになります。

送受信：

このメーラーを利用する上で、大切なことは送信者と受信者が暗号化に関して協調していることです。送信側で暗号化の設定をしているときは、受信側でも復号化の設定をして下さい。また、
送信側で暗号化の設定をしていないときは、受信側でも復号化の設定をしないで下さい。

協調した形での設定がしてないと、暗号化されたものが復号化されなかったり、平文が復号化の操作を受けて読めなくなったりします。十分注意してください。

ここでは、強調した形での設定がしてある場合について説明します。

（１）　送信者側で暗号化の設定をし、受信者側で復号化の設定をしている場合

送信時にメール本文は暗号化された特別な添付ファイルとして送信されます。さらに、メール本文の代わりとして、dummy.txt の内容が平文として送信されます。本来の添付ファイルも暗号化されてから、添付ファイルとして同時に送信されます。

このメーラーで受信したときは、暗号化された本文は自動的に復号化されて表示されます。dummy.txt を表示することもできます。暗号化されて送信された本文や、添付ファイルは、添付ファイルの一覧として表示されます。保存するときに自動的に復号化されます。

本文を暗号化したものは、mdata05.bin という名前の添付ファイルです。

他のメーラーで受け取った時には、dummy.txt　の内容が表示されます。メール本文は暗号化されたままの mdata05.bin という添付ファイルとして受信されます。本来の添付ファイルは暗号化されたままの添付ファイルとして受信されます。

（2）両者ともに、暗号化の設定をしていない場合
メール本文が暗号化されないままで送信されます。本来の添付ファイルも暗号化されないままで送信されます。このメーラーで受信したときは本文が表示されます。本来の添付ファイルは、普通の添付ファイルとして受信されます。

注意１：
通信時に使用する暗号化ソフトや復号化ソフトの特定はメールアドレスによって行いますので、このアドレス帳に同じメールアドレスを２つ以上登録してはいけません。同じ人が二つ以上のメールアドレスを持っている形の登録は可能で全く問題ありません。もちろん自分自身を登録して、自分宛に暗号メールを送信して確認することも可能です。

お互いに、暗号化鍵、復号化鍵を作成し必要なものを相手に送り、それを使って、暗号化ソフト、復号化ソフト、暗号化鍵、復号化鍵の設定を正確に行って下さい。
◎送信側と受信側で暗号化の設定がバラバラの場合には、受信したものが表示できません。
◎多重暗号化するときは、暗号化と復号化で順序が違っていると復号化できませんので、ご注意ください。１番と１番、２番と２番、のように、暗号化ソフトと復号化ソフトを対応させてください。
◎鍵の作成では鍵ファイルの名前に注意してください。別の鍵を作成するつもりで同じ名前のファイルを作って上書きしてしまうと、上書きされた鍵を使っていた暗号通信が出来なくなります。通信相手の名前とアルゴリズムなどを分かりやすく入れたものにして下さい。

注意２：
送信済みのメールの内容を見ないならば、自分が A さん、相手が B さんとしたとき、

A さんのアドレス帳では、

名前	電子メールアドレス
B さん	bsan@xyz.co.jp

	暗号化ソフト	暗号化鍵
1	cmlEC.exe	cmlkeyEC.bin
2	BmpEC.exe	bmpkeyEC.bin
3		
4		
5		

	復号化ソフト	復号化鍵
1	MistyDC.exe	mistykeydc.bin
2	marsdc.exe	marskeydc.bin
3		
4		
5		

となっていて、

B さんのアドレス帳では、

名前	電子メールアドレス
A さん	asan@pqr.com

	暗号化ソフト	暗号化鍵
1	MistyEC.exe	mistykeyec.bin

2　marsEC.exe　　marskeyec.bin
3
4
5

　　復号化ソフト　　復号化鍵
1　 cmlDC.exe　　cmlkeyDC.bin
2　 BmpDC.exe　　bmpkeyDC.bin
3
4
5

　これによって、A さんから、B さんあてに出されるメールは、
暗号化ソフトの 1 によって、CmlEC.exe で暗号化されます。さらに、BmpEC.exe で 2 回目の暗号化がなされます。その後送信されます。
　これを受け取った B さんのほうでは、A さんから来るデータは上のように暗号化されているので、
A さんの項目の復号化部分が、番号の大きなものから適用されて、最初に BmpDC.exe で復号化されます。さらに、CmpDC.exe で復号化されます。これで、元に戻るので、この復元されたデータがメールの内容として表示されます。
　添付ファイルの場合も同様に暗号化に対応する復号化が行われて、B さんのパソコンに保存されることになります。

ですから、A さんが B さん宛てに送信したものを後で見る必要が無ければこれで十分です。

　A さんの送信済みトレイには、暗号化されて送信されたものが保存されています。
　自分（A）が B さんに送ったメールは、自分の送信済みトレイに保存されるのですが、この内容は、データが最初は cmlec.exe で暗号化されて、次に bmpec.exe で暗号化されたものが保存されています。

その内容を見るには、bmpdc.exe で変換したものを、さらに cmldc.exe で変換しなくてはなりません。
自分のアドレス帳には、自分が送ったものを復号化するための復号化ソフトがありません。
　もちろん、B さんは、A さんから来たデータを復号化するためのソフトを登録していますので、受信したデータを復元できます。これが、順序対方式での設定です。

どうしても、後で自分が B さん宛てに送信したデータの内容を見る必要がある場合には、次のように設定します。

A さんのアドレス帳では、
　　名前　　電子メールアドレス
　　B さん　　bsan@xyz.co.jp

　　暗号化ソフト　　暗号化鍵
1　 cmlEC.exe　　cmlkeyEC.bin
2　 BmpEC.exe　　bmpkeyEC.bin
3
4
5

　　復号化ソフト　　復号化鍵
1　 cmlDC.exe　　cmlkeyDC.bin

2	BmpDC.exe	bmpkeyDC.bin
3		
4		
5		

として、さらに

B さんのアドレス帳では、

名前	電子メールアドレス
A さん	asan@pqr.com

	暗号化ソフト	暗号化鍵
1	cmlEC.exe	cmlkeyEC.bin
2	BmpEC.exe	bmpkeyEC.bin
3		
4		
5		

	復号化ソフト	復号化鍵
1	cmlDC.exe	cmlkeyDC.bin
2	BmpDC.exe	bmpkeyDC.bin
3		
4		
5		

と設定し、順序対ごとに暗号化方式を設定するのではなく、集合{A,B}に対して暗号化方式を設定することになります。

こうすれば、A さんから送られてきたデータを B さんが復号化して見ることもできるし、A さんが B さんに送ったデータを、後で確認することもできます。

送信済みトレイに保存されたデータに対して使われる復号化ソフトは、送信する相手の項目の、復号化の部分に登録されている内容が使われます。
A さんが、B さん宛てに送った物が送信済みトレイにある場合は、そのデータを復号化するときには、A さんのアドレス帳における、B さんの項目の中での復号化ソフト、復号化鍵が使用されます。

おわり。　　宇山靖政