
# Crypto Anywhere - OpenPGP Edition

# User Manual

# Table of Contents

# 1 Introduction

## 1.1 What is Crypto Anywhere ?

### Secure email in an incredibly small package!


**Don't be a Glass Citizen!**
**Protect your privacy with Crypto Anywhere.**
**Advantages at a glance...**

- Strong encryption
- Small, fast and portable
- Supports public key encryption and password based encryption
- Message recipients do not need Crypto Anywhere to read self decrypting messages
- New : OpenPGP support, compatible with PGP ™ 8.0
- New : Themes support for application skins
- New : Direct deposit of messages keeps your ISP from reading your mail
- New : Automatically creates a travel floppy or USB drive for use in internet cafés
- New : Microsoft Outlook Express ™ Integration
- New : Microsoft Outlook Office 2000/2002 ™ Integration

| | |
|---|---|
| ***The Sydney Morning Herald :*** *Australia, May 10th, 2003* | *Two words: "portability" and "privacy"* |
| ***News24.com :*** *South Africa, May 2nd, 2003* | *If you need to send confidential e-mail, try Crypto Anywhere for size.* |
| ***Telegraph :*** *United Kingdom, July 10th, 2003* | Top tip...Crypto Anywhere is a simple-to-use email program with powerful built-in encryption. |
| ***CHIP Magazine Online:*** *Greece* | A practical, portable encryption solution |

*Crypto Anywhere is secure email on the move!* Crypto Anywhere is small enough to fit on a single floppy or USB key chain drive and is very easy to use. Don't have a computer yourself but want to protect your web based e-mail at your local internet cafe? Crypto Anywhere is for you! If you suspect your employer is reading your private email, put an end to that. If you run Crypto Anywhere from a floppy disk or USB drive, you can encrypt your email without even installing software on your workstation. With Crypto Anywhere you can send and receive secure mail to and from anyone with an email account - the recipients do not have to be "crypto savvy" or even have Crypto Anywhere themselves.

Crypto Anywhere implements trusted, industry standard, strong encryption algorithms based on RSA public key encryption, the Twofish block cipher and the ISAAC random number generator. Crypto Anywhere e-mail is compatible with SecExMail based encryption. Version 2.0 and later of Crypto Anywhere support OpenPGP encryption and provide compatibility with PGP Corporation's PGP ™ product.

# 2 Usage

## 2.1 Encrypting Mail 1,2,3

To encrypt mail, open Crypto Anywhere, select *My Messages* on the left, then click the *Compose Message* icon. This will display the compose message view as shown below.


**Step 1:** Specify the recipient(s)

Enter recipient email address.

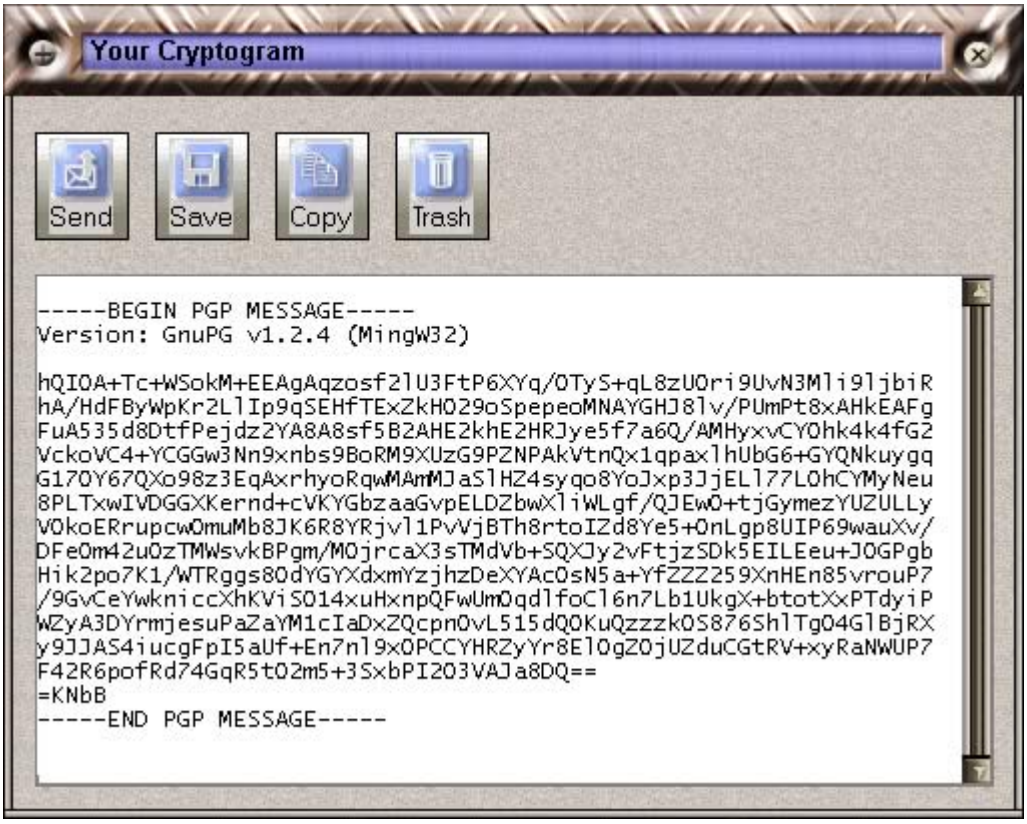
**Step 2:** Enter the subject and your message

If you are a registered user of Crypto Anywhere you may attach documents and files to your

message.

**Step 3:** Encrypt the message

Select "*Encipher*" from the menu or click the encipher button. This will display the encrypted message or cryptogram, ready for sending. Click "*Send*". Depending on the availability of encryption keys, Crypto Anywhere will generate a SecExMail encrypted message, an OpenPGP encrypted message, or a password protected message.




## 2.2 Decrypting Mail 1,2,3

If you have received a Crypto Anywhere message, follow the simple steps outlined below.

**Step 1:** Copy the encrypted message to the Windows clipboard

In your favorite e-mail client or web browser, select the entire encrypted e-mail with your mouse and copy it to the windows clipboard. To do this click above or to the left of the line

*--Begin SecEx 1.1--*

and hold the left mouse button down while scrolling to the end of the page. The entire message should now be highlighted. Now select *Edit*, *Copy* from the menu or use the keyboard shortcut Ctrl-C. This will copy the encrypted message to the Windows clipboard.

If you have received an OpenPGP encrypted message, click above or to the left of the line

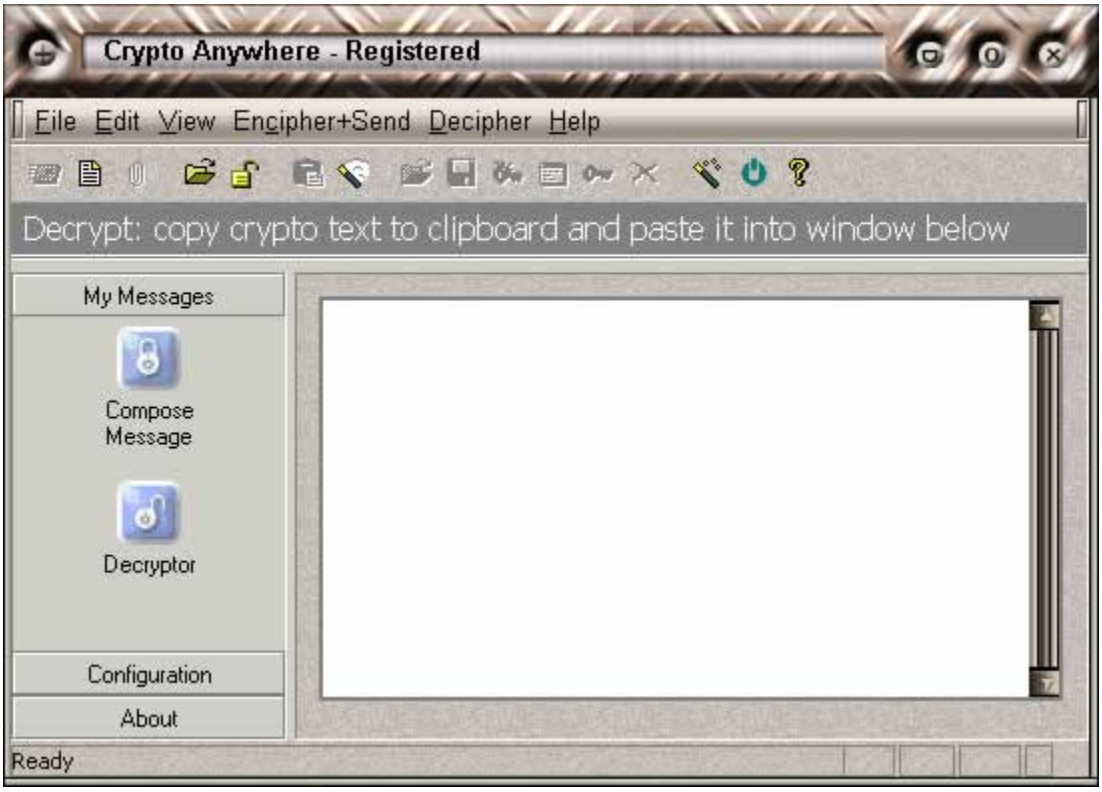
-----BEGIN PGP MESSAGE-----

and hold the left mouse button down while scrolling to the end of the page. The entire message should now be highlighted. Now select *Edit*, *Copy* from the menu or use the keyboard shortcut Ctrl-C. This will copy the encrypted message to the Windows clipboard.

If you have received a self decrypting message, simply follow the instructions in the accompanying email.

**Step 2:** Paste the encrypted message into Crypto Anywhere

Open Crypto Anywhere. Select *My Messages* on the left, then click the *Decryptor* icon. Now click the *Paste* button on the toolbar.

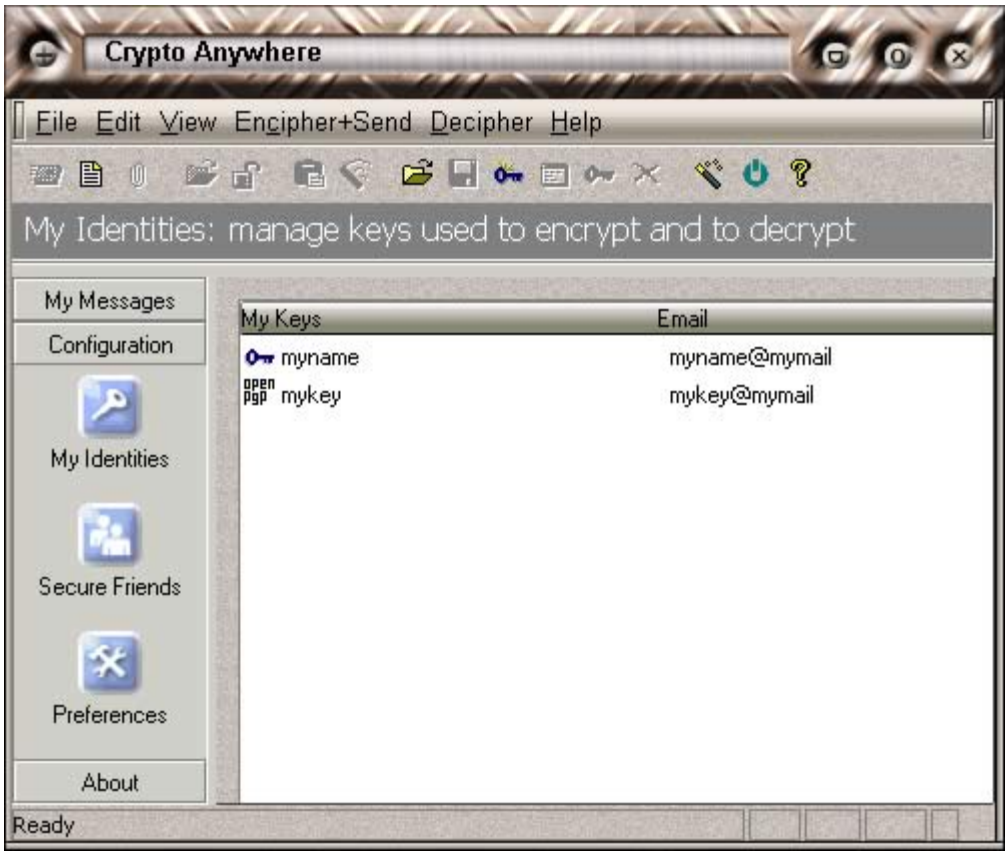



**Step 3:** Decrypt the message

Select "*Decipher*" from the Crypto Anywhere menu or click the decipher button on the toolbar. This will decrypt the message and display the plain text in the message window.

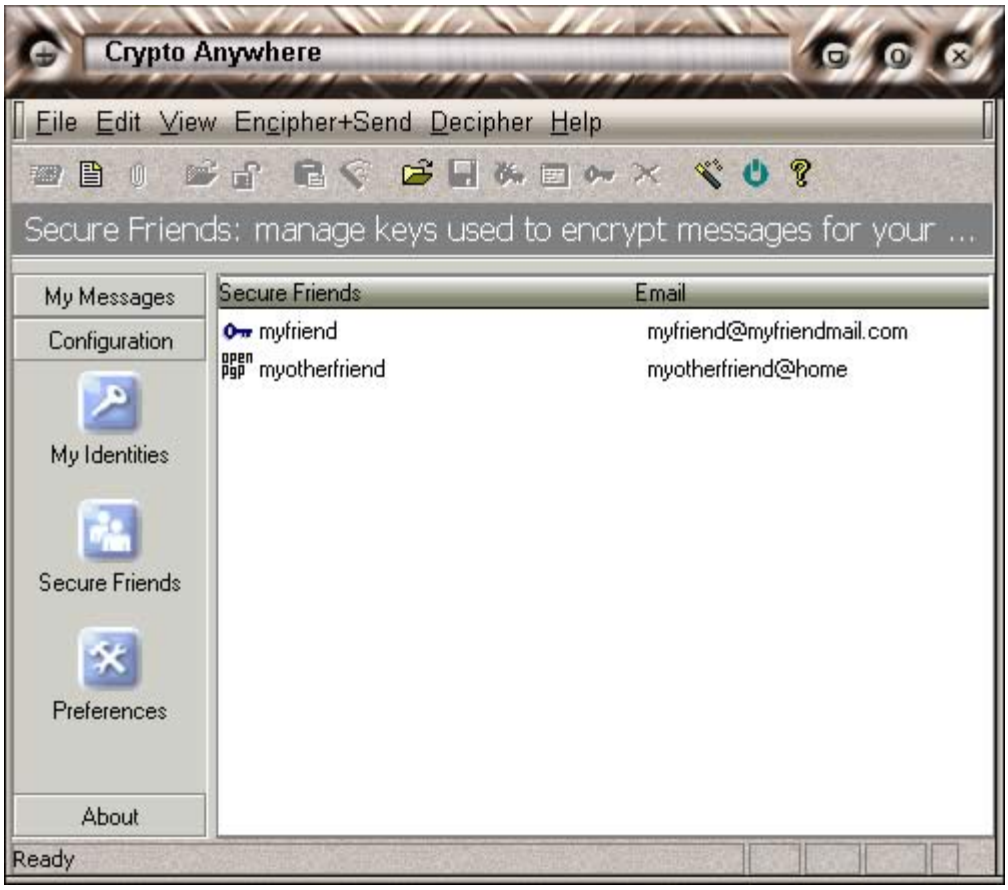

## 2.3 My Identities

The ***My Identities*** screen shows your own SecExMail and OpenPGP keys. From here you can create new keys, change the passphrase on existing keys, back up and restore keys to and from disk.




## 2.4 Secure Friends

The ***Secure Friends*** screen shows people on your secure contact list. On this screen you can add and remove friends from your secure contact list and display key properties including fingerprints. E-mail sent via Crypto Anywhere to people on the secure friends list will be encrypted automatically and without the need for further interaction by you, the user. Crypto Anywhere will automatically select SecExMail mode or OpenPGP mode encryption based on the key type listed for the message recipient. If no key is listed, Crypto Anywhere will default to SecExMail password protected encryption.



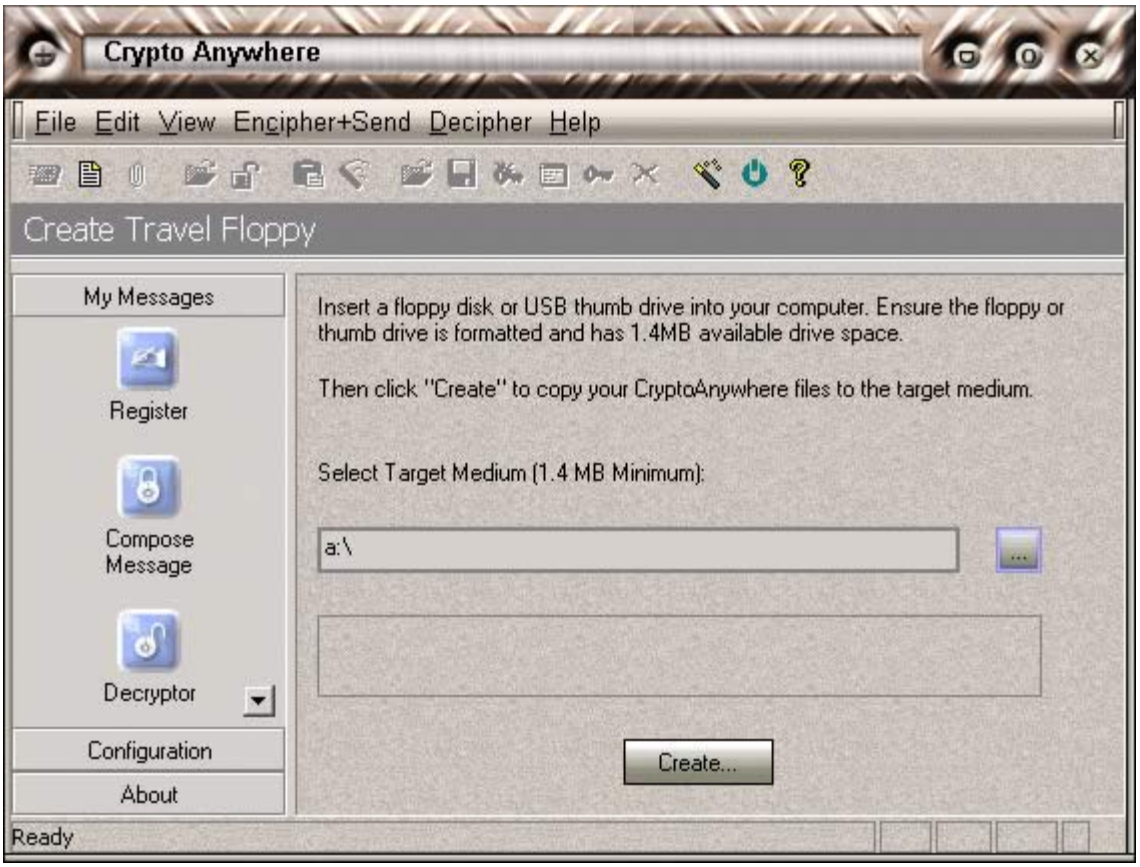

## 2.5 Direct Drop

Direct Drop delivers emails across the internet directly to the recipient's mail box. This feature enhances your privacy because it bypasses your internet service provider's mail server. If you suspect that your internet service provider logs your email messages or you plan to use Crypto Anywhere from internet cafés, Direct Drop is recommended.

Note that some spam filters will discard direct drop e-mails from dial-up links. If your messages are being refused, switch to your usual mail server to send messages.


## 2.6 Create Travel Floppy

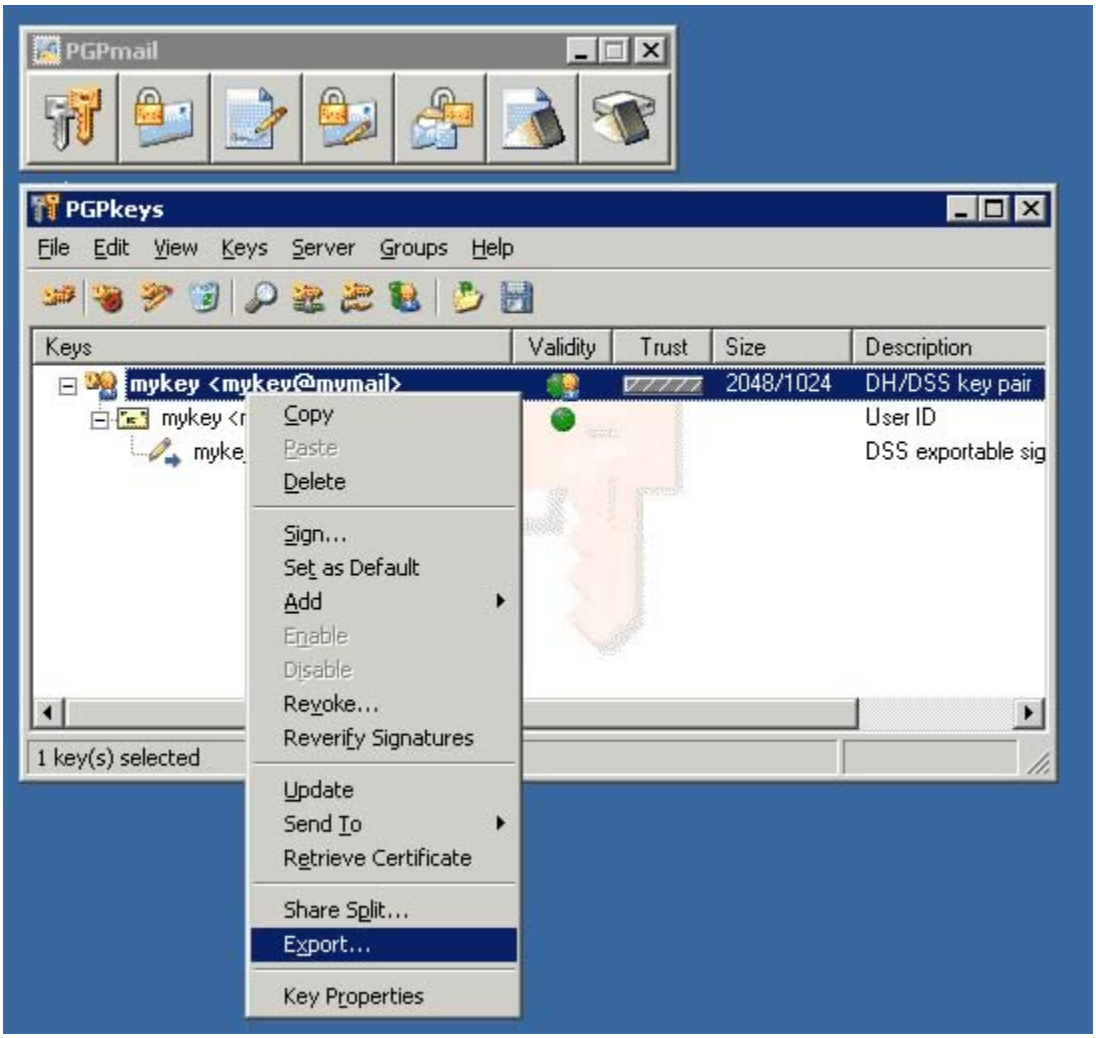
If you have installed Crypto Anywhere on your hard drive and wish to use on a friend's computer or in an internet cafe, you may wish to create a portable installation on a floppy disk, USB drive or similar removable medium. To do this, simply create a travel floppy via the "Create Travel Floppy" screen shown below. Only the files required for portable execution of Crypto Anywhere including your keys and personal configuration files will be copied to the floppy.



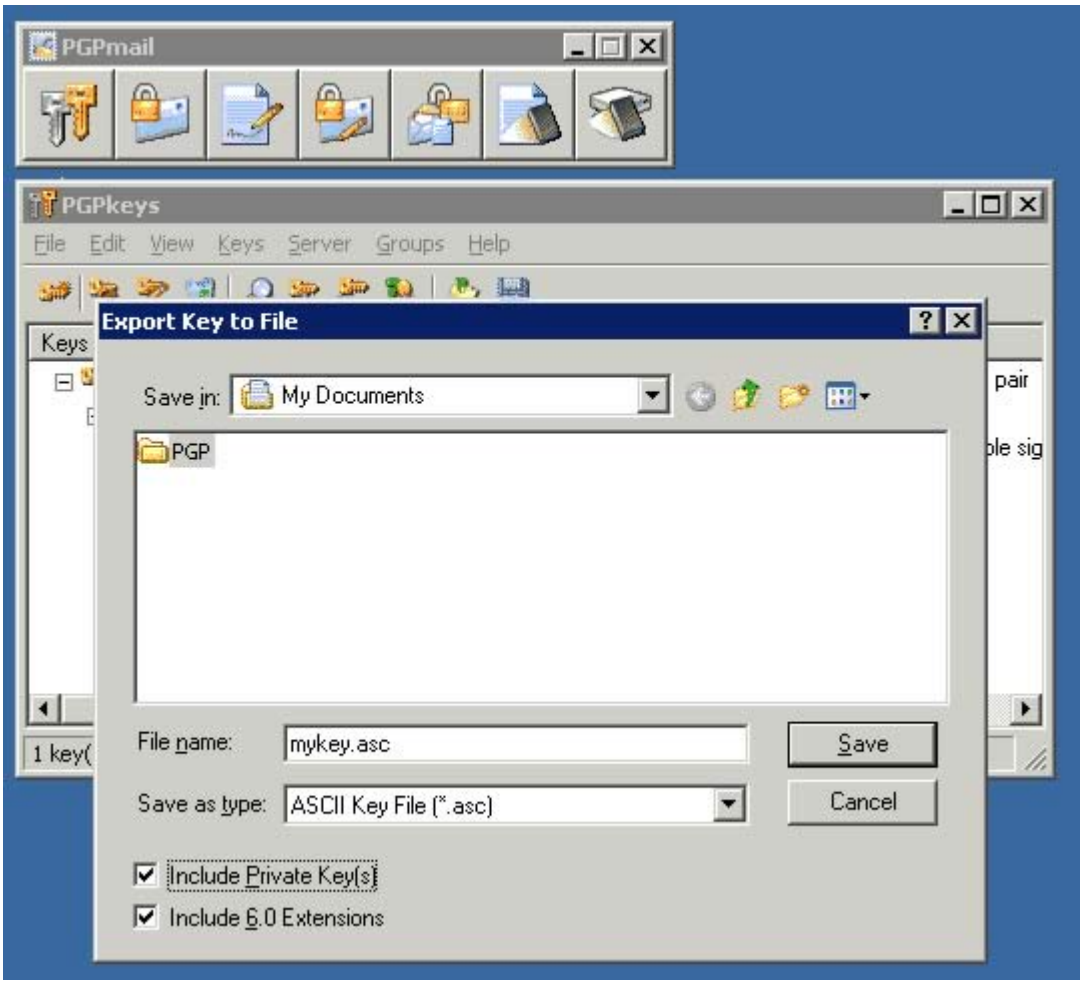

## 2.7 Import PGP (tm) Keys

Version 2.0 and later of Crypto Anywhere support OpenPGP encryption and provide compatibility with PGP Corporation's PGP ™ product. If upgrading from PGP ™ to Crypto Anywhere, you may wish to import your old PGP ™ 8.0 keys and those of your friends. This provides an ideal migration path to the stronger SecExMail cipher also supported by Crypto Anywhere while maintaining backwards compatibility with legacy software. To import your PGP ™ keys, follow the illustrated guide below.

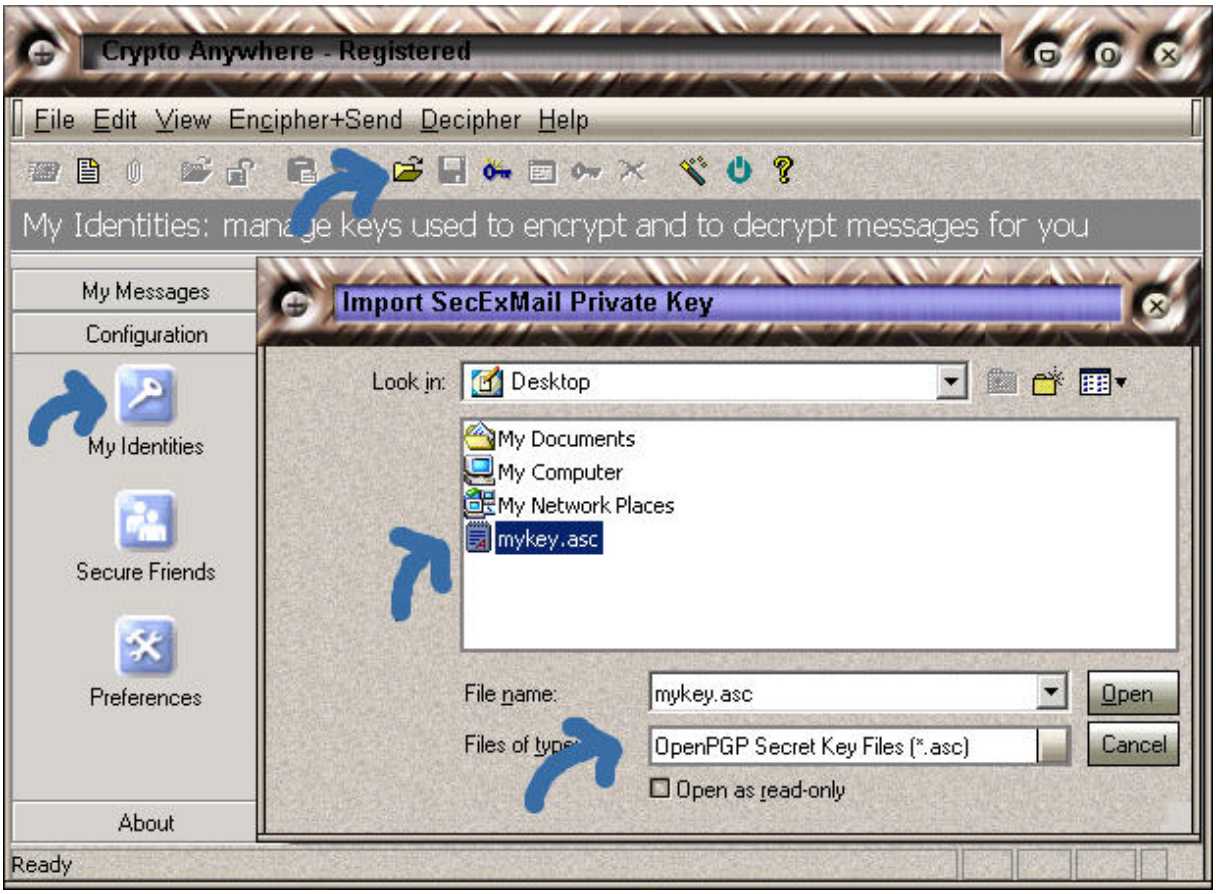
- Open your PGP ™ key chain, select your key and then select the export option.




- Save your key to disk as an ASCII key file and check the "Include Private Key(s)" option as shown below




- In Crypto Anywhere, navigate to the "***My Identities***" screen under "Configuration" on the left tool menu. Then click the open folder icon on the toolbar to activate the "***Import SecExMail Private Key***" dialog. Under "***Files of type***", select "***OpenPGP Secret Key Files***" and navigate to the key file you exported from PGP ™. Now click open.




- Your PGP ™ key will appear in the My Identities screen. In the future you will need only your PGP ™ passphrase to decrypt messages sent to you from your PGP ™ friends.


## 2.8 For your eyes only screen

When sending encrypted e-mail, you will need to specify the recipient(s) of your message. As you receive Crypto Anywhere messages from other people, Crypto Anywhere collects encryption keys from the senders - your secure friends. When sending mail to your secure friends, messages are encrypted so that only your secure friends will be able to read them. You yourself won't be able to decrypt a message encrypted to a secure friend - unless of course you selected your own key for encryption also. You may select one or more keys. Using secure friend keys is the recommended mode of encryption.


In many cases, the intended recipient of a message has not provided you with an encryption key. This will be especially the case when communicating with someone for the first time. In this case simply click "*unlisted email address*". This will select "*Self decrypting e-mail*" as encryption method.


Self decrypting e-mail messages carry an attachment which bundles your encrypted message, the Crypto Anywhere software needed to decrypt the message and any required encryption keys into a self extracting archive. The encryption key required to decode the message is itself stored using 3DES encryption and protected by the passphrase you supply. Therefore you will need to supply the recipient of the message with this passphrase. The ability to receive email attachments will vary from recipient to recipient. Some email clients or email servers block self extracting attachments or block attachments with specific file names or extensions. For this reason you may send self decrypting e-mails in three formats under "*Send As*". The following options are supported :

- default - zip archive
- exe - self extracting executable

- zip - zip archive
- 123 - self extracting executable with ".123" file extension

Request encrypted reply

Check this option if you want to include keys needed to send you encrypted e-mail ( your public keys ).

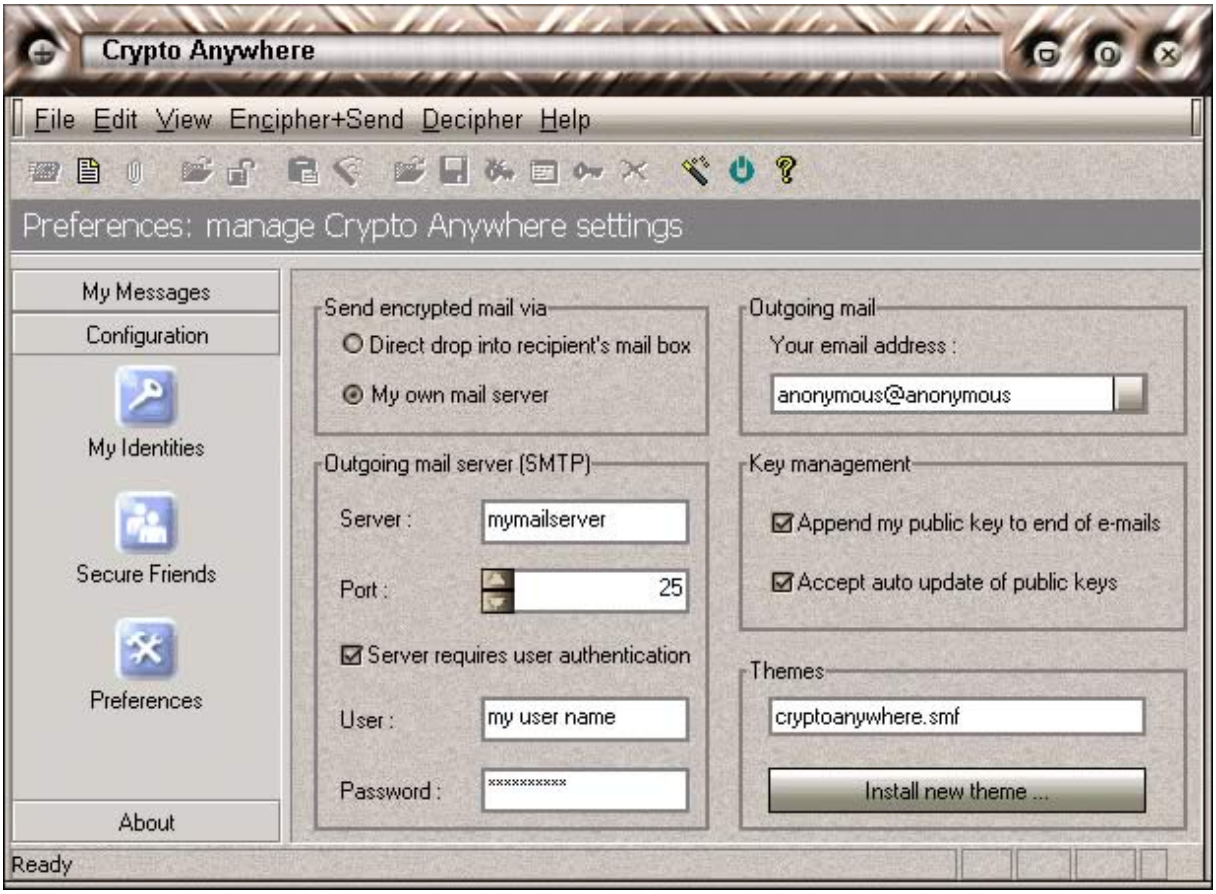
Share secure friends list

Check this option if you want to share your secure friends list with the recipients ( secure friends public keys ).

In most cases you will only have to send a self decrypting email to a particular recipient once. After decrypting and reading your message, the recipient will be given the option to configure Crypto Anywhere immediately and send you encrypted mail in reply.

## 2.9 Preferences

The preferences window allows you to customize the behavior of Crypto Anywhere. See documentation below.



- **Send encrypted mail via**

  Direct drop into recipient's mail box :
  Direct Drop delivers emails across the internet directly to the recipient's mail box. See Direct Drop for details.
  Crypto Anywhere has a built in SMTP module to send e-mail. This allows Crypto Anywhere to send e-mail independently of mail settings of the computer or computers on which it is run. This option is especially useful if you plan to use Crypto Anywhere in internet cafe's. Some service providers do not allow access to their SMTP send mail servers when connecting from other service provider's networks and might require SMTP logon to permit you to send mail. See "*Server requires user authentication*".

  My own mail server :
  This option is recommended if you usually use Crypto Anywhere from the same computer. Simply enter the details of the mail server you ordinarily use for outgoing mail.

- **Outgoing mail server (SMTP) :**

  Server :
  This option is only required in SMTP mode. Please provide the DNS name or IP address of your outgoing mail server.

  Port :
  This option is only required in SMTP mode. Please provide the port number of your outgoing mail server SMTP service. It is safe to leave the default value.

  Server requires user authentication :
  This option is only required in SMTP mode. Some service providers require user logon to permit sending of e-mail. Usually this is the same information as is required for the checking of e-mail. User logon, also called SMTP AUTH, is only available with extended SMTP, or ESMTP.

  User :
  This option is only required in extended SMTP mode with SMTP AUTH. Please enter your user name for your e-mail account.

  Password :
  This option is only required in extended SMTP mode with SMTP AUTH. Please enter your password for your e-mail account.

- **Outgoing mail :**

  Your e-mail address :
  This option specifies your return e-mail address or "*reply-to*" address. By default, the "*reply-to*" e-mail address corresponds to the e-mail address of your default Crypto Anywhere / SecExMail key.

- **Key management :**

  Append my public key to end of e-mails :
  If you check this option, Crypto Anywhere will append your default public key to the end of outgoing messages as a "*tag line*". This enables other users to send encrypted mail to you. You will be added to the secure friends list of other Crypto Anywhere users automatically

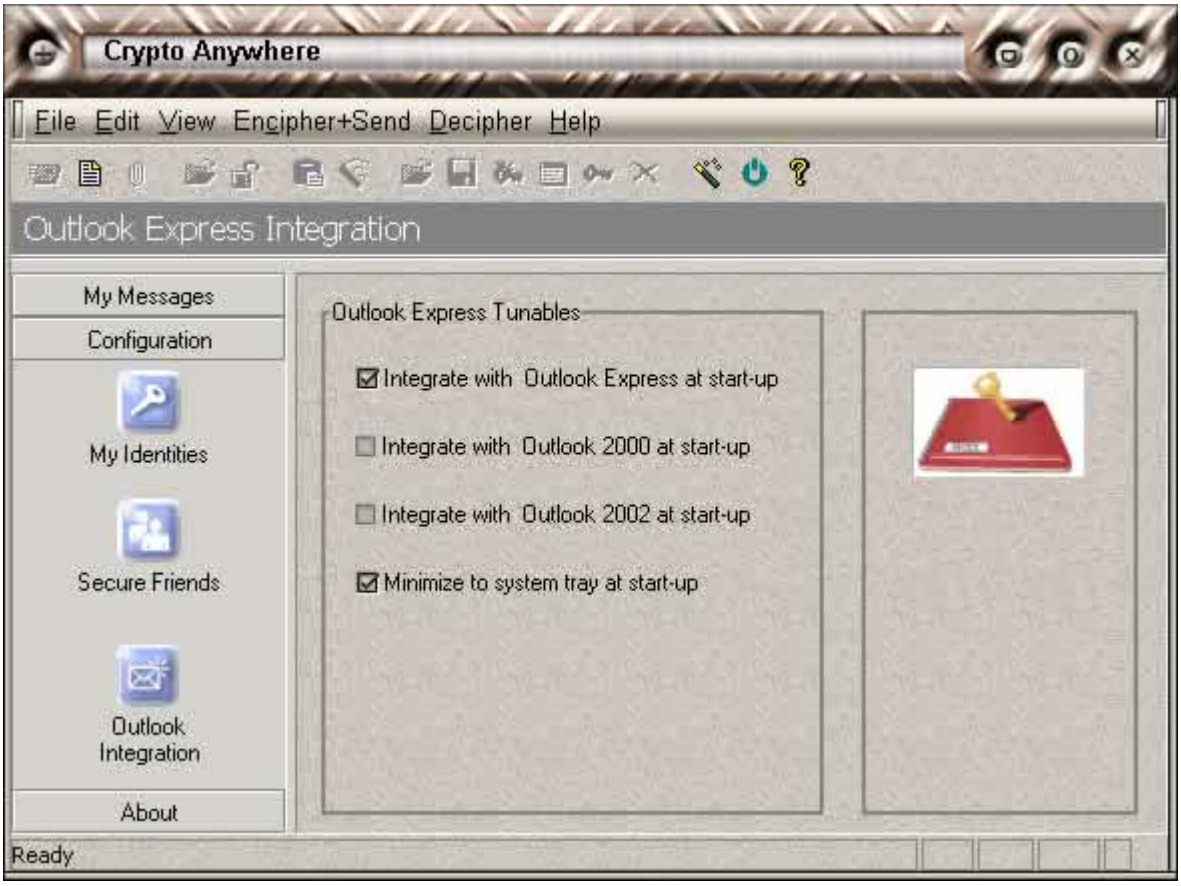
  Accept auto update of public keys :
  If you check this option, Crypto Anywhere will accept new public keys from other people and add them to your secure friends list when ever a key is not found on your secure friends list already. You will be prompted prior to each update.

- **Themes :**

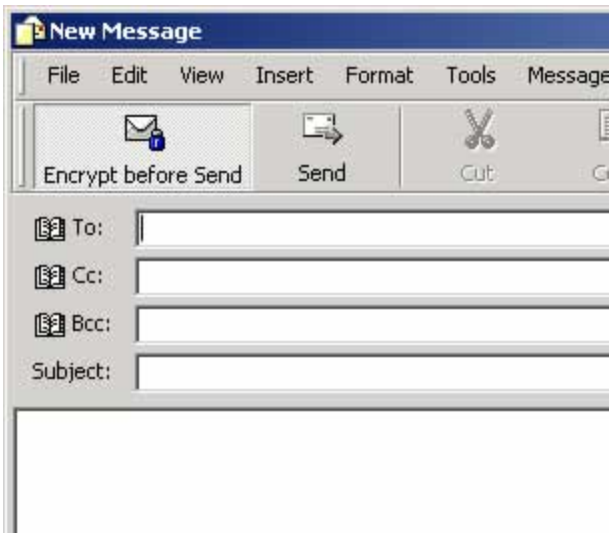
  Crypto Anywhere now supports application skins. Please check www.bytefusion.com for availability.

## 2.10 Microsoft Outlook Express Plug-In

Crypto Anywhere integrates with Microsoft Outlook Express ™ to produce seamless encryption and decryption from within popular email software: You can easily send OpenPGP, SecExMail, as well as password protected messages directly from within your favorite email client. To enable Microsoft Outlook Express ™ support, navigate to the ***Outlook Integration*** screen in the ***Configuration*** section and check the setting "*Integrate with Outlook Express at start-up*". If this option is enabled, Crypto Anywhere will load the Microsoft Outlook Express ™ plug-in at the next start-up. In order for Outlook Express ™ to recognize the plug-in, Crypto Anywhere must be started before Outlook Express ™. If you require continual Crypto Anywhere support from within Outlook Express ™, check the "Minimize to system tray at startup" option. This option pre-loads Crypto Anywhere when you log into Windows, ensuring that Outlook Express ™ always receives encryption support via Crypto Anywhere.




In order to encrypt outgoing messages from within Outlook Express ™, click the "***Encrypt before Send***" button in ***New Message*** window as shown below. When you press ***Send***, Outlook Express ™ will submit the message to Crypto Anywhere for encryption prior to sending the message.




To decrypt mail from within Outlook Express ™, simply click the "Decrypt Message" button in your inbox message window as shown below. You will be able to view the decrypted message in the dedicated Crypto Anywhere message viewer and reply directly to the sender of the message using the encryption method of your choice.


Compatibility

Crypto Anywhere support for Outlook Express ™ has been tested with the following configurations:

- Outlook Express 6.0 and Microsoft Windows 2003 ™
- Outlook Express 6.0 and Microsoft Windows XP ™
- Outlook Express 6.0 and Microsoft Windows 2000 Professional ™
- Outlook Express 6.0 and Microsoft Windows 98 ™
- Outlook Express 5.0 and Microsoft Windows 95 ™
- Outlook Express 5.0 and Microsoft Windows 98 ™

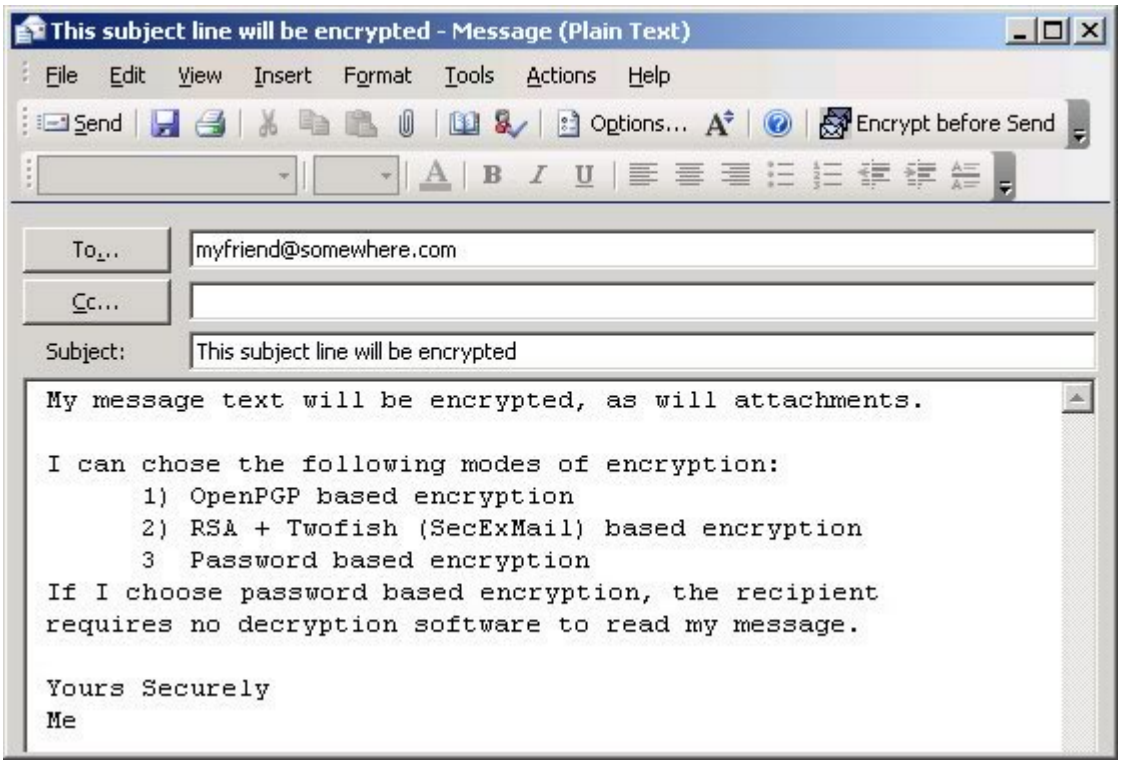
## 2.11 Microsoft Outlook Office Plug-In

Crypto Anywhere integrates with Microsoft Outlook Office ™ to produce seamless encryption and decryption from within popular email software: You can easily send OpenPGP, SecExMail, as well as password protected messages directly from within your favorite email client. Crypto Anywhere support for Outlook Office ™ is available for the following versions of Outlook:

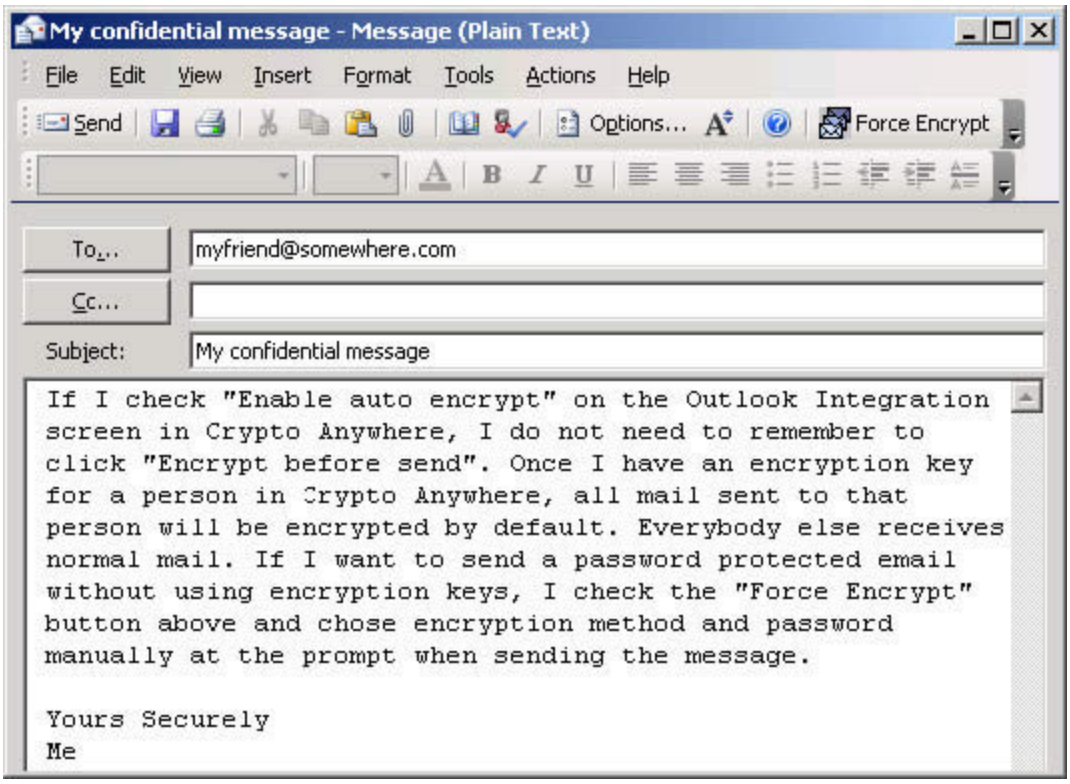
1. Microsoft Outlook Office 2000 ™
2. Microsoft Outlook Office 2002 ™
3. Microsoft Outlook Office 2003 ™

The Crypto Anywhere plug-in for Microsoft Outlook Office ™ is also compatible with Microsoft Exchange ™.

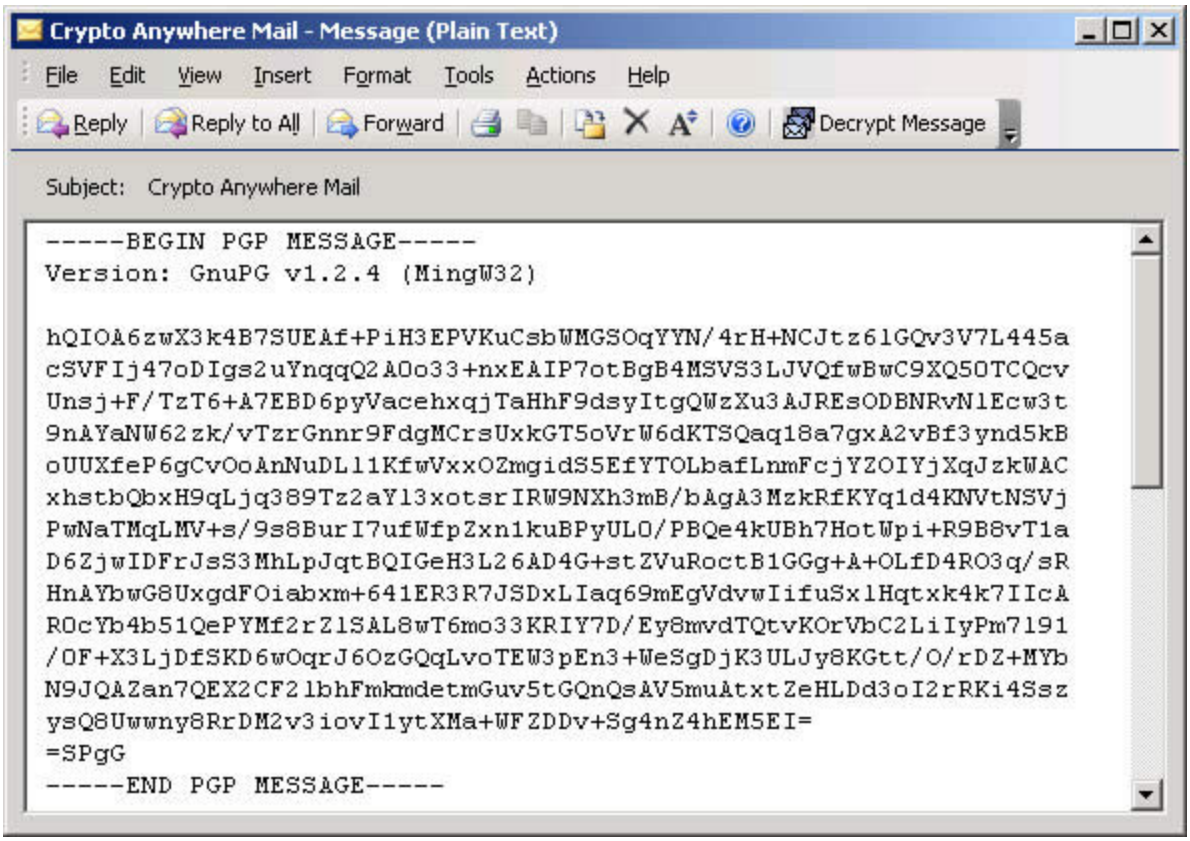
When the Outlook Office plug-in is loaded, you will see a new toggle button "***Encrypt before Send***" on the toolbar when composing a new message. Clicking the "***Encrypt before Send***" button, prompts Crypto Anywhere to be invoked when sending the message. At that time, you will be able to chose the encryption method as well as encryption keys and or password for your message.




The Crypto Anywhere plug-in for Microsoft Outlook Office ™ can automatically select plain text or encryption mode email based on the availability of encryption keys. To enable this feature, click "***Enable auto encrypt***" on the Outlook Integration screen in Crypto Anywhere.

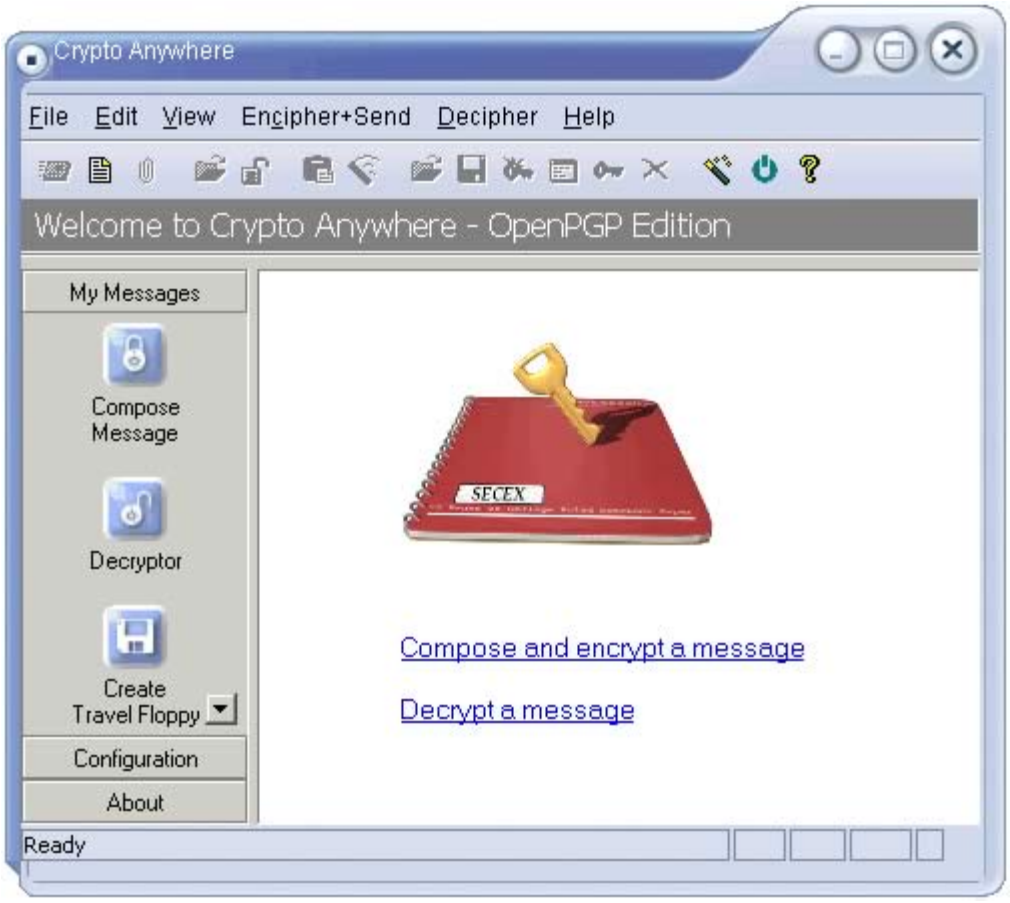


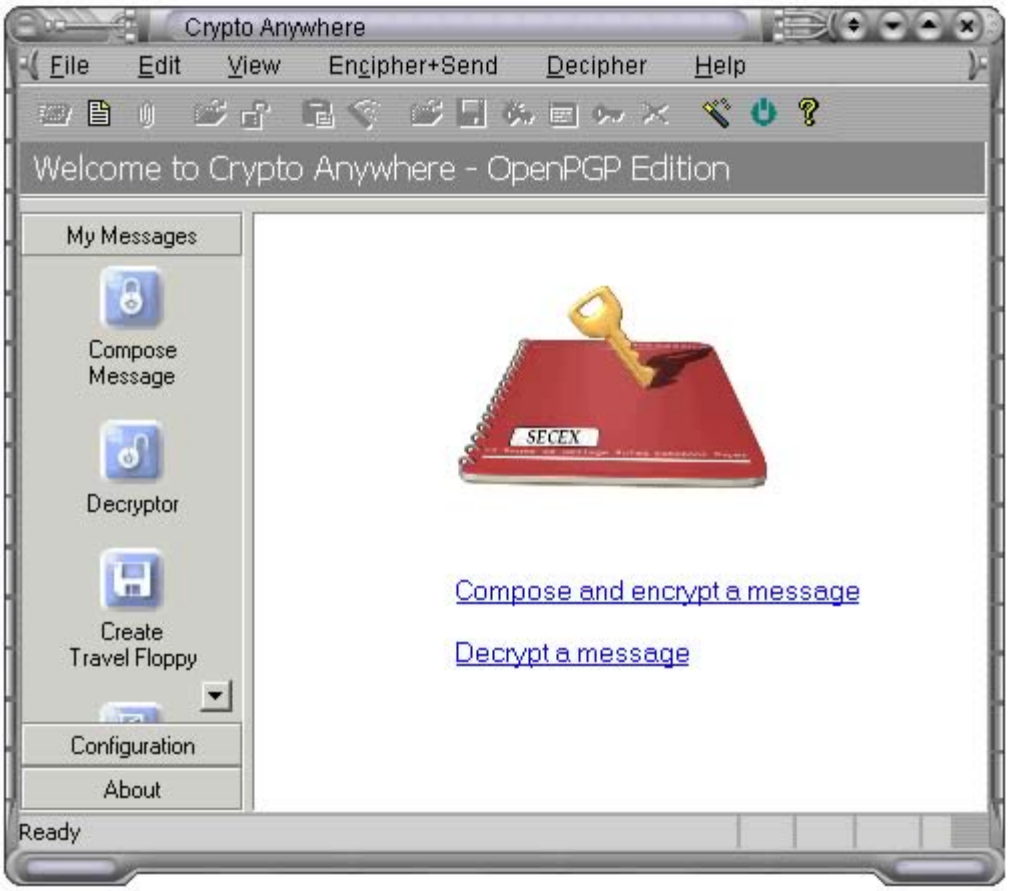

When opening an encrypted message, you will see a new button "***Decrypt Message***". Click this button to decrypt the message text and any attachments.

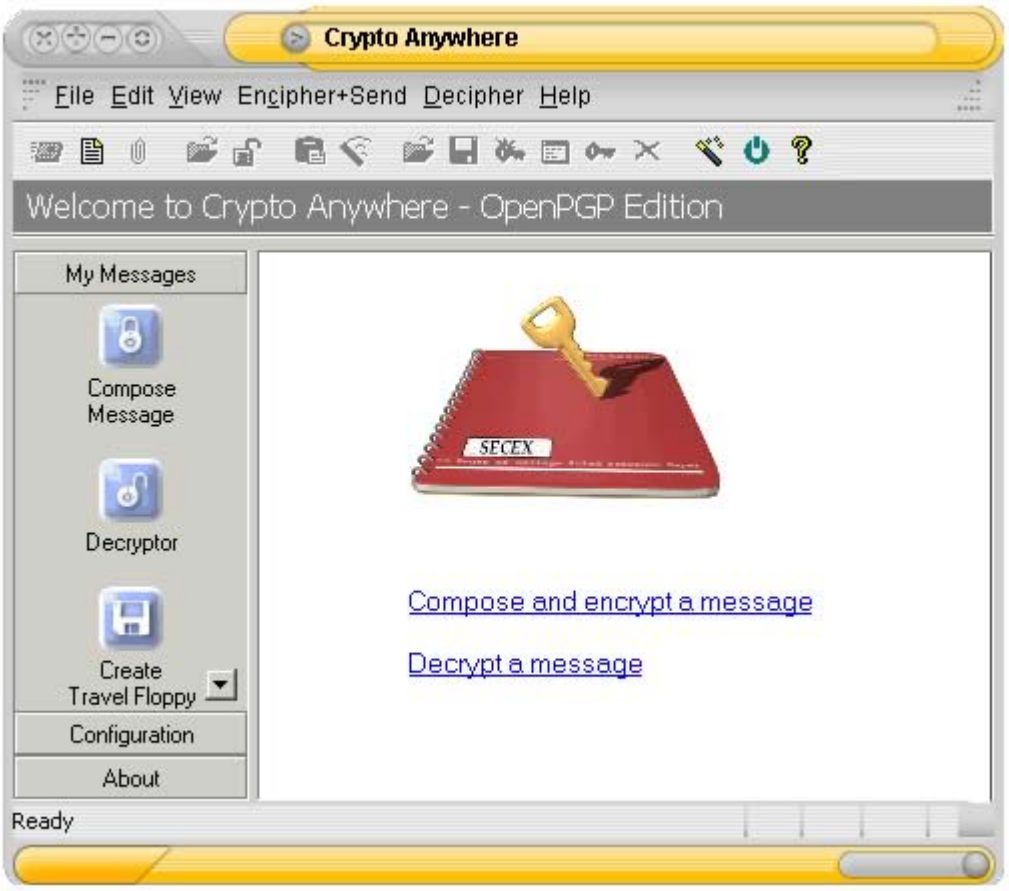



## 2.12 Application Themes

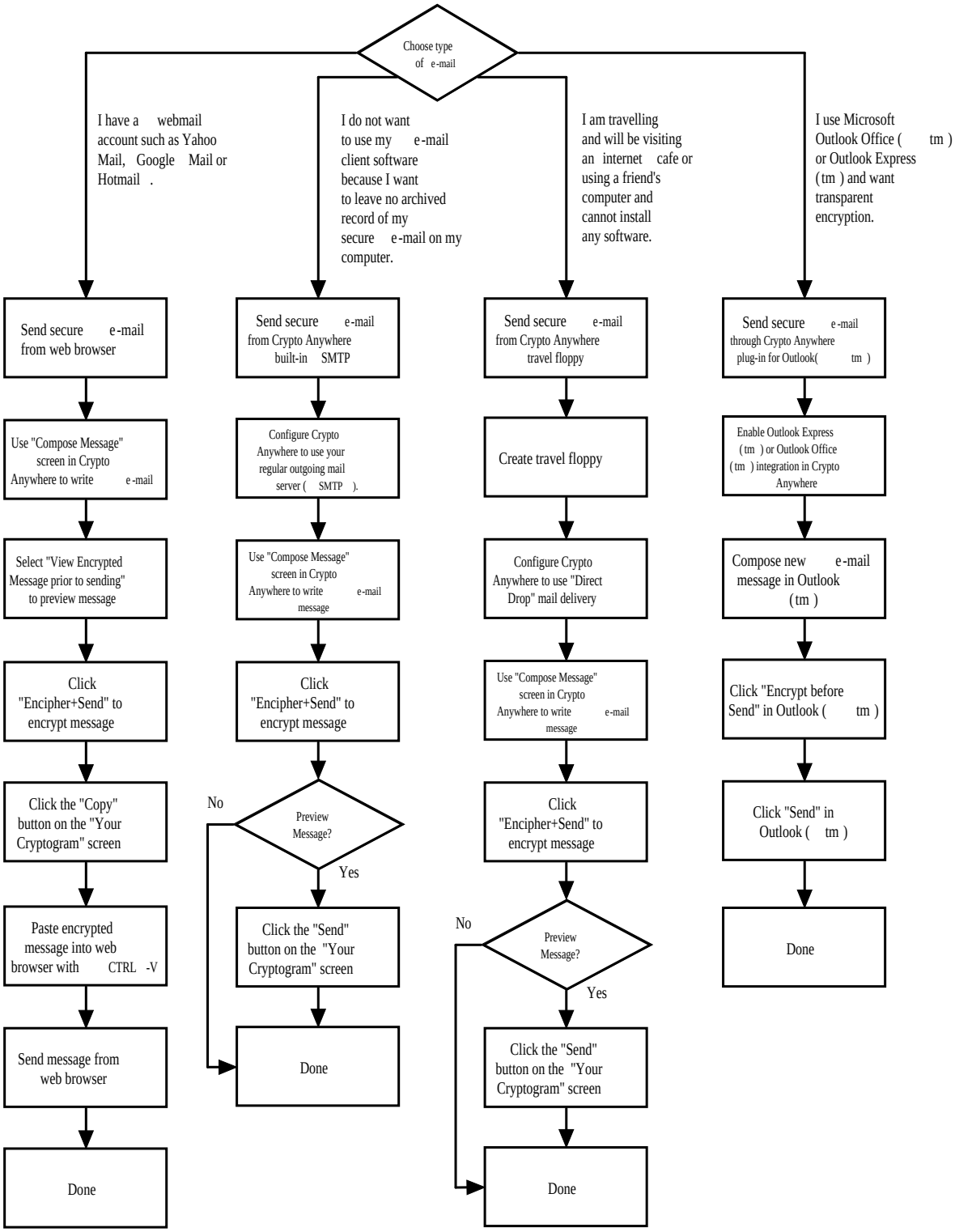
Security need not look conservative. Version 2.0 and later of Crypto Anywhere support user definable application skins. Check www.bytefusion.com for availability of Crypto Anywhere themes. Application skins require Windows NT / 2000 / XP / 2003 (TM) and are not available on Windows 95 (TM) and Windows 98 (TM).



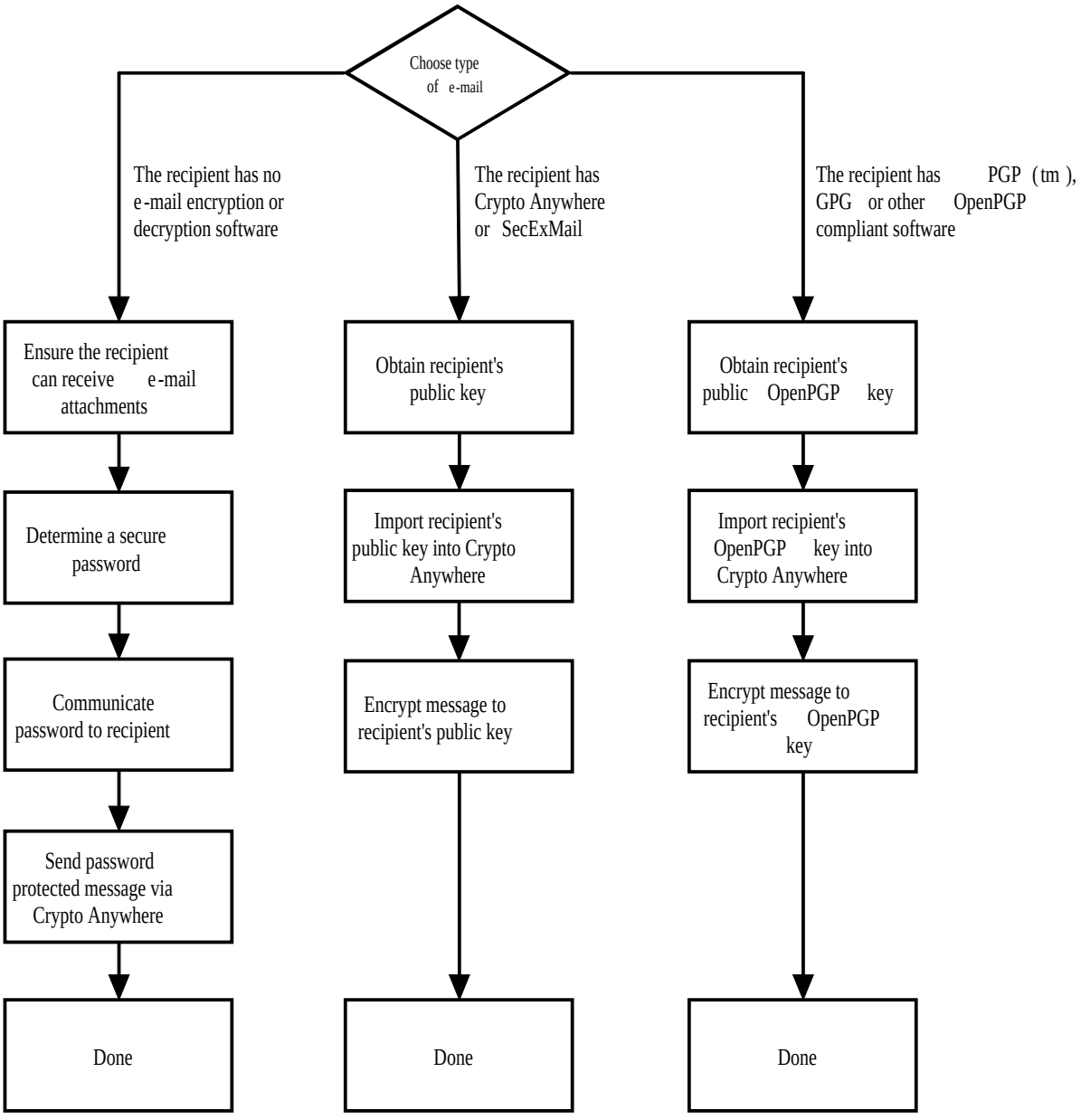




## 2.13 Mail Delivery Modes



## 2.14 Modes of Encryption




# 3 Technical

## 3.1 RSA Public Key Encryption

**"c = me mod n"** is the algorithm that turns the world of e-commerce. Introduced in 1978 by Rivest, Shamir and Adleman after whom the cipher is named, RSA is the worlds foremost public key encryption system. Contrary to the design of classic encryption algorithms where the same key is used to lock and

## 3.2 ISAAC Random Number Generator

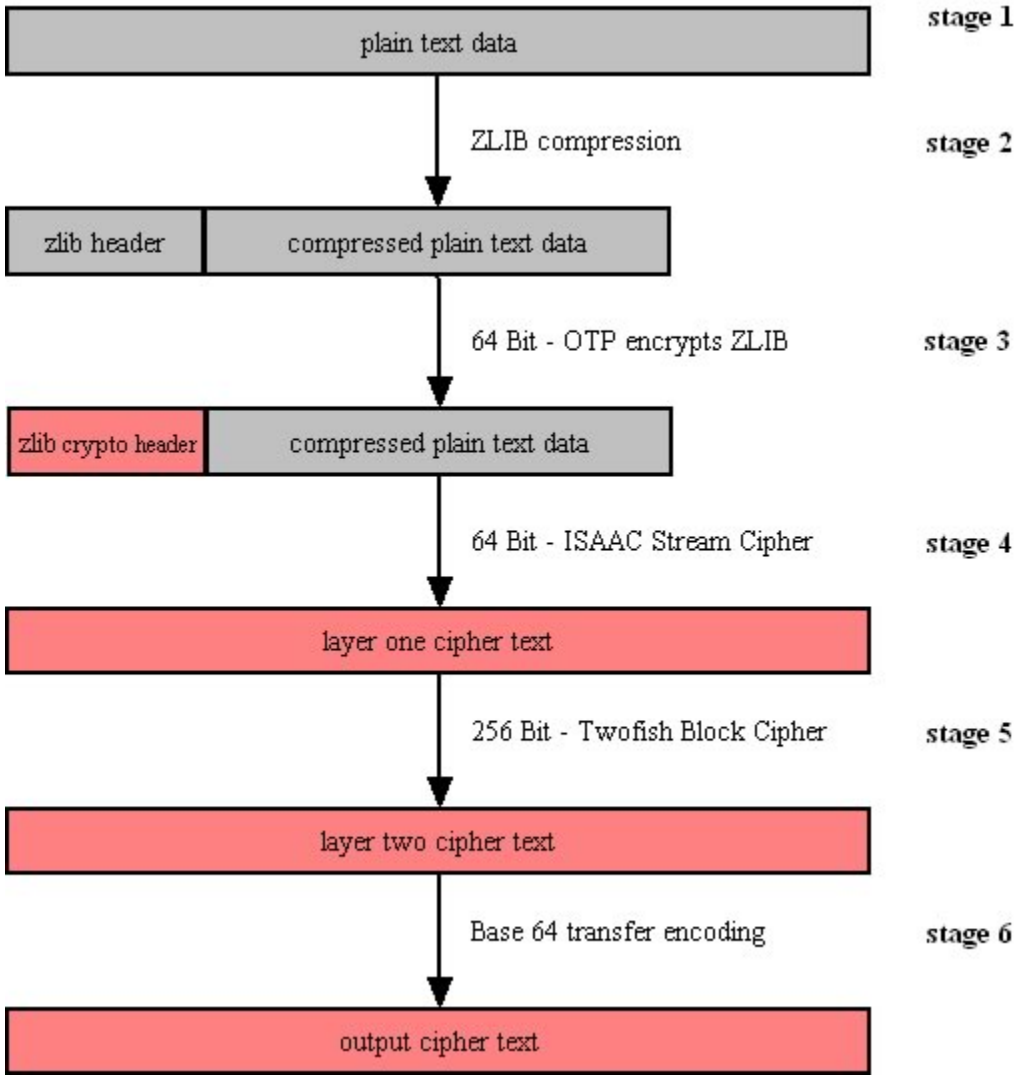
ISAAC (Indirection, Shift, Accumulate, Add, and Count) is a cryptographically secure pseudo random number generator. With an average cycle length of 2 to the 8295th power its output is uniformly distributed and unpredictable. ISAAC has been developed by Bob Jenkins and placed into the public domain in 1996. See Acknowledgements for legal information on ISAAC.

ISAAC is at the heart of SecExMail's entropy collection system and comprises the stream cipher subsystem of the SecExMail cipher.

## 3.3 The SecExMail / Crypto Anywhere Cipher

The SecExMail cipher is a composite cipher specifically designed to operate on real-time email streams. It uses cryptographic primitives which are available to the general public and have been subject to extensive peer review. The SecExMail cipher incorporates RSA public key encryption. Message encryption is performed via the Twofish block cipher and the ISAAC stream cipher. The SecExMail cipher is warranted to be free from spy-ware, key escrow or key recovery features of any kind. The email encryption process is described in detail below. See diagram.

**SecExMail Composite Cipher**




- **Stage 1**

  Email data is received in variable length data blocks. SecExMail parses SMTP header info, mail and data bodies.

- **Stage 2**

  Because email messages frequently contain known plain text, such as salutation and or tag lines, which gives rise to known plain text attacks on the encrypted message and in order to minimize overall message expansion, the plain text is first compressed using the ZLIB compression algorithm. The net effect of deflating large amounts of data, containing both tidbits of known plain text such as greeting or tag lines as well as unknown message text into a compressed data stream is that any known plain text is effectively obscured.

- **Stage 3**

  The ZLIB stream has a fixed header format which in itself might be exploited as known plain text by a savvy cryptanalyst. For this reason, the first 64 bits of the steam are enciphered by way of a

One Time Pad, using standard XOR masking. This approach acknowledges that email messages will contain portions of known plain text and proactively manages this problem.

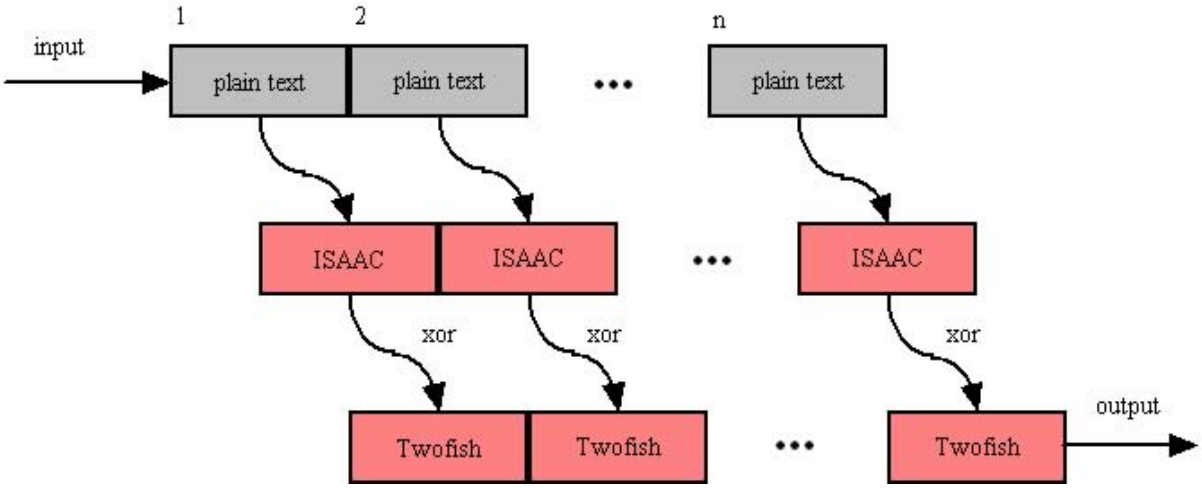
- **Stage 4**

  At this point the compressed data is encoded using the 64 bit ISAAC stream cipher creating the layer one cipher text.

- **Stage 5**

  The next step in the encryption process is to encrypt the layer one cipher text using the 256 bit Twofish block cipher. Twofish is used in chained block mode, but instead of XOR'ing the previous block's cipher text into the plain text of the current block, the output from the ISAAC layer is "chained in". This chaining process is illustrated below.

**ISAAC Twofish Block Chaining**



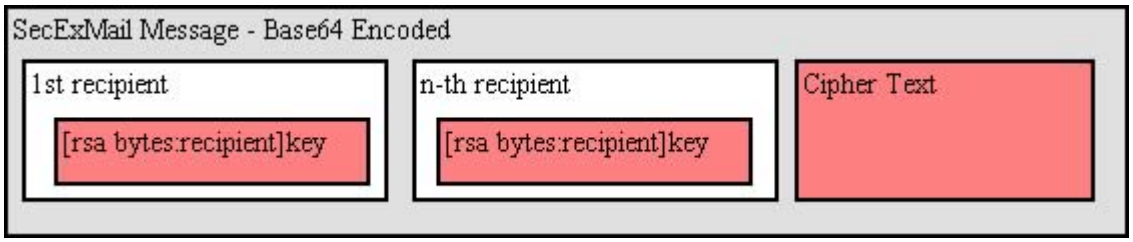

- **Stage 6**

The final step is to assemble the output in base64 transfer encoded format for transmission via mail transfer agents (MTA).

## 3.4 SecExMail / Crypto Anywhere Message Format

SecExMail messages are transferred in base64 encoded format. Messages may be encrypted to multiple recipients. The internal message layout is defined as follows :

**[<rsa bytes>:<recipient>]key[<rsa bytes>:<recipient>]key...cipher text**




- **RSA Bytes**

This is the size of the recipient's RSA key in bytes. Therefore a 2048 bit RSA key would be listed as having a size of 256 bytes. RSA This parameter is defined for RSA key sizes of 2048, 4096, and 8192 bits.

- **Recipient**

This is the email address of the recipient to whom the message is encoded.

- **Key**

This is the SecExMail session key material, encrypted with the RSA public key of the recipient. The SecExMail session key is used to encrypt the message body of the email message and is comprised
of a 64 bit One Time Pad key, a 64 bit ISAAC stream cipher key, and a 256 bit Twofish key.

- **Cipher Text**

This is the message body encrypted with the SecExMail Cipher.

A typical SecExMail enciphered message is depicted below :

```
--Begin SecEx 1.1--
WzI1NjpjaHJpc0BvZmZzaG9yZW1haWxyb29tLmNvbV0dJyyJnwwCm0LI0659zpBY/asERA3FRG9
9
OYRhm5f+rwohYORt8Wp3rmwI2Nguhk38KvH5pg8ZRTXXWiEHYMakQPPXpbnaJepJFZeXTcNMTi/
d
p0Rc5HCTui5okW/00Gv8Sp328Ldh3DlgQcGW7oYt9qxG/cJ/PaVxxxEfDM3I4cnsCyLjfX+I0JY
6
h+emWt4U/N6u+K0tPL4ua2OfGhGoBXo+6KK042bXGpk/Pj6WEOQMcKyR+VrsOx6ZcTgpqS3WCcU
c
2/JDy9zHqlkPLohXcT4G2Hiwp/1JhviaQtoKA2NYYimuY5ZjNUGPMsIaN0h6AKS3/qZsHhK1Ltc
A
WpLnuoFbQleekuJngBCC1RIlIlI4lfFgMkxoUkZrtXg6E217Q6GMMhHMANJ4EU3D2c1BgauDYAQ
G
Rpz0p8efm/WAZoXai6KVElMEiK7tv98s8wu9LpUxN44QYj2eNRVI+72lGPfkBoKvr6eK5/TU4cH
N
Dg9VxCGj4n8KDvfYsPRpBSNzLL+Ta4iz7toQ/MGdPCQa
--End SecEx Mail--
```

## 3.5 SecExMail / Crypto Anywhere Keys

SecExMail employs public key encryption. Messages are encrypted to one or more recipients using their **public keys**. Only the intended recipient can, upon receipt of the message, recover the plain text using his/her **private key**. Public key encryption differs from classical encryption because the recipient of a message does not use the same key for decryption as the sender used for encryption.

In cryptography the fictional characters "Alice" and "Bob" are often used for illustration purposes. Consider the following scenario : Alice lives in New York and Bob lives in Los Angeles. Alice wants Bob to be able to send her confidential mail. She goes to her local hardware store and purchases a dozen or so combination padlocks, sets the unlocking code on each padlock, confuses the dials again, and sends the open padlocks to Bob in Los Angeles.

Bob is now in possession of Alice's padlocks, but not the unlocking codes. When Bob wants to send Alice a confidential letter, he places the letter inside a steel box and locks it with one of Alice's padlocks. Once the padlock is snapped shut, even he himself cannot re-open the box since he is not in possession of the combination which will release the lock. Only Alice will be able to open the box and therefore read the letter once she has received Bob's parcel in the mail.

Public key encryption works much in the same manner. The **public key** may be thought of as an open, electronic padlock. You can send this electronic padlock to all your friends. Your friends may then use that padlock to secure their emails to you in an electronic box. This electronic box is the encrypted email. Upon receipt of the encrypted email, you dial the secret combination which is your **private key** and retrieve the original message.

SecExMail does all this for you.

## 3.6 SecExMail / Crypto Anywhere Key File Format

The SecExMail keys are stored in conventional text files ending in "#.pubrsa" and "#.privrsa" for public keys and private keys respectively. Files are divided into an administrative segment and a data segment. The administrative segment contains information required by SecExMail for key management.

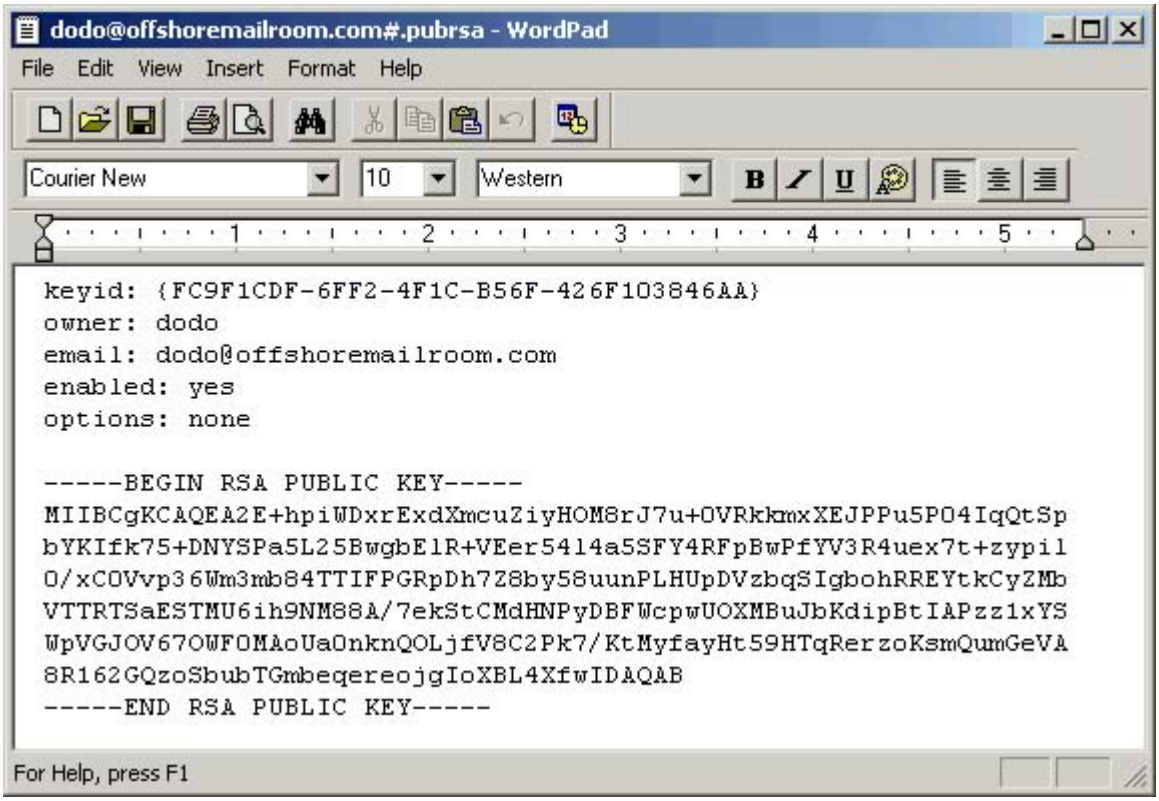
Administrative Segment

| | |
|---|---|
| keyid | Globally unique key identifier; used by SecExMail to associate private and public key components. |
| owner | owner of the SecExMail key |
| email | Email address of key owner |
| enabled | reserved for future use |
| options | vendor options field - reserved for future use |

New lines in the administrative section are denoted by carriage return line feed pairs (ASCII characters 13 + 10).

Data Segment

The data section is comprised of a single RSA key in base 64 encoded format. New lines in the data section are denoted by a single linefeed ( ASCII character 10 ). Private RSA keys are stored in 3DES encoded, chained block cipher format and protected with a passphrase.




## 3.7 One-Time Pads

A one-time pad is a block of random data used to encrypt a block of equal length plain text data. Encryption is usually by way of XOR'ing the one-time pad with the message text. This process may be thought of as a 100% noise source used to mask the message. The one-time pad is secure if it is comprised of random data and is never reused. Because of this, one-time pads have limited application in modern ciphers, but are commonly acknowledged as the holy grail of cryptography.

SecExMail uses one-time pads to encrypt the ZLIB compression header in SecExMail messages.

## 3.8 Requirements

- Windows 95 / 98 / ME / NT / 2000 / XP / 2003
- Access to internet mail server ( SMTP & POP3 )
- Pentium class IBM compatible computer
- Application skins require Windows NT / 2000 / XP / 2003


## 3.9 Known Plain Text Attack

A known plain text attack is the attempt by a cryptanalyst to break a cipher based on knowledge about the plain text of a message prior to its encryption. Simply put, if the cryptanalyst knows the method of encryption, any encryption, part or all of the plain text input to the cipher, and is able to observe the encrypted message text, he / she will likely be able to infer the key used to encrypt the message. This in turn can compromise the security of future messages sent with that key. In greatly simplified terms :

**Plain Text + Key = Cipher Text**
**Cipher Text - Plain Text = Key**

Consider the following scenario : Alice sends Bob an email and attaches her favorite holiday snapshot. The email is encrypted. Assume further that she sends the same holiday snapshot to her mother in plain text. Steve, who wishes to spy on Alice and Bob, was able to intercept her email to Mom and now has a copy of "myholiday.jpg". If the picture consisted of 200 Kilobytes of data (about 200,000 letters) and Alice included only a short personal message to Bob with the picture ( say 50 letters ), then Steve already knows 99% of the message contents prior to encryption and now has greatly improved chances of breaking Alice's key if he comes into possession of the corresponding cipher text.

Crypto Anywhere includes comprehensive protection against known plain text attacks. See SecExMail Cipher for more information.

## 3.10 Registration Advantages

Registered users receive the following benefits :

- Commercial use license
- Product support
- Multiple identities - private keys

- Unlimited secure friends - public keys
- Encrypt attachments
- Themes / application skins
- Create travel floppies
- Variable passphrase length on self decrypting e-mails

Most registered user benefits, with the exception of commercial use, are available during the first 30 days of operation.

# 4 About

## 4.1 About Crypto Anywhere


**Crypto Anywhere - OpenPGP Edition**
**Version 3.0**


## 4.2 About Bytefusion Ltd.


**Bytefusion Ltd.**
**22 Duke Street**
**Douglas, IOM**
**IM1 2AY**
**British Isles**

**Inquiries: sales@bytefusion.com**

## 4.3 Acknowledgements

- **ISAAC Random Number Generator**

  At the time of writing, the ISAAC home page can be found at http://burtleburtle.net/bob/rand/isaacafa.html.
  ISAAC has been placed into the public domain by its author, Bob Jenkins in 1996.

  ---
  My random number generator, ISAAC.
  (c) Bob Jenkins, March 1996, Public Domain
  You may use this code in any way you wish, and it is free. No warrantee.
  ---

- **RSA Public Key Encryption**

  The RSA algorithm was patented until September 2000 when RSA® Security Inc. released the algorithm into the public domain. *"BEDFORD, Mass., September 6, 2000 -- RSA® Security Inc. (NASDAQ: RSAS) today announced it has released the RSA public key encryption algorithm into the public domain, allowing anyone to create products that incorporate their own implementation of the algorithm."* At the time of writing a copy of this statement can be found at http://www.rsasecurity.com/news/pr/000906-1.html

- **Twofish Block Cipher**

  The Twofish block cipher by Counterpane Labs was developed and analyzed by Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall and Niels Ferguson. Twofish was one of the five Advanced Encryption Standard finalists. At the time of writing the Twofish homepage can be found at http://www.counterpane.com/twofish.html. The cipher has been made available to the general public by the following statement on http://www.counterpane.com/about-twofish.html :

  " Twofish is unpatented, and the source code is uncopyrighted and license-free; it is free for all uses. Everyone is welcome to download Twofish and use it in their application. There are no rules about use, although I would appreciate being notified of any commercial applications using the algorithm so that I can list them on this website. "

- **ZLIB Compression Library**

  ZLIB is a lossless data-compression library written by Jean-loup Gailly and Mark Adler. ZLIB is made
  available as free, unpatented software to the general public at http://www.gzip.org/zlib/. The license conditions are set forth at http://www.gzip.org/zlib/zlib_license.html and reproduced below :

```
" Copyright (C) 1995-2002 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied
warranty.  In no event will the authors be held liable for any damages
arising from the use of this software.

Permission is granted to anyone to use this software for any purpose,
including commercial applications, and to alter it and redistribute it
freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not
```

```
   claim that you wrote the original software. If you use this software
   in a product, an acknowledgment in the product documentation would be
   appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not
be
   misrepresented as being the original software.
3. This notice may not be removed or altered from any source
distribution.

Jean-loup Gailly jloup@gzip.org
Mark Adler madler@alumni.caltech.edu "
```

- **RIPEMD-160**

  The RIPE message digest was written by Antoon Bosselaers for Katholieke Universiteit Leuven, Department of Electrical Engineering ESAT/COSIC, Belgium. License conditions ask us to quote the following :

```
" RIPEMD-160 software written by Antoon Bosselaers,
available at http://www.esat.kuleuven.ac.be/~cosicart/ps/AB-9601/ "
```

- **Viking Art - SecExMail Logo**

  Katja Bengtsson of Brisbane, Australia ( katja@offshoremailroom.com )

- **OpenSSL Project**

  SecExMail contains cryptographic software from the OpenSSL project at www.openssl.org which is licensed under a "*BSD-style*" open source licenses. These licenses asks us to state the following :

```
"This product includes software developed by the OpenSSL Project for use
in the OpenSSL Toolkit. (http://www.openssl.org/)"

"This product includes cryptographic software written by  Eric Young
(eay@cryptsoft.com). This product includes software written by Tim Hudson
(tjh@cryptsoft.com)."
```

  SecExMail is an independent, derived work and no endorsement of SecExMail by the OpenSSL project is implied. The full text of the OpenSSL license and the original SSLeay License is reproduced below.

```
OpenSSL License

=====================================================================
Copyright (c) 1998-2001 The OpenSSL Project.  All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in
   the documentation and/or other materials provided with the
   distribution.
```

3. All advertising materials mentioning features or use of this
   software must display the following acknowledgment:
   "This product includes software developed by the OpenSSL Project
   for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
   endorse or promote products derived from this software without
   prior written permission. For written permission, please contact
   openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL"
   nor may "OpenSSL" appear in their names without prior written
   permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following
   acknowledgment:
   "This product includes software developed by the OpenSSL Project
   for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
OF THE POSSIBILITY OF SUCH DAMAGE.
====================================================================

This product includes cryptographic software written by Eric Young
(eay@cryptsoft.com).  This product includes software written by Tim
Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
All rights reserved.

This package is an SSL implementation written
by Eric Young (eay@cryptsoft.com).
The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as
the following conditions are adhered to.  The following conditions
apply to all code found in this distribution, be it the RC4, RSA,
lhash, DES, etc., code; not just the SSL code.  The SSL documentation
included with this distribution is covered by the same copyright terms
except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in
the code are not to be removed.
If this package is used in a product, Eric Young should be given
attribution
as the author of the parts of the library used.
This can be in the form of a textual message at program startup or
in documentation (online or textual) provided with the package.

```
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
   must display the following acknowledgement:
   "This product includes cryptographic software written by
   Eric Young (eay@cryptsoft.com)"
   The word 'cryptographic' can be left out if the routines from the
library
   being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof)
from
   the apps directory (application code) you must include an
acknowledgement:
   "This product includes software written by Tim Hudson
(tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE
ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The licence and distribution terms for any publicly available version or
derivative of this code cannot be changed.  i.e. this code cannot simply
be
copied and put under another distribution licence
[including the GNU Public Licence.]
```

- **SecExMail Encryption**

  Chris Kohlhepp and Mark Robertson, Bytefusion Ltd.

## 4.4 GNU Privacy Guard - License

OpenPGP integration support in Crypto Anywhere is provided via the GNU Privacy Guard, GPG. GPG is included free of charge as standalone software, licensed under separate license terms. The version of the file GPG.EXE included with Crypto Anywhere is an entirely unmodified version of the GNU Privacy Guard (GnuPG 1.2.4) available from www.gnupg.org, compressed with the executable packer UPX for compact distribution. You are free to distribute GPG under the terms of the license shown below.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991



Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not

compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may

consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

## 4.5 DIG - License

Mail server lookup for direct drop mail delivery is provided via the internet name server BIND utility program DIG. The files DIG.EXE and LIBBIND.DLL are included free of charge as standalone software, licensed under separate license terms. You are free to distribute DIG.EXE and LIBBIND.DLL under the terms of the license shown below.



Internet Software Consortium
950 Charter Street
Redwood City, CA 94063
Tel: 1-888-868-1001 (toll free in U.S.)
Tel: 1-650-779-7091
Fax: 1-650-779-7055
Email: <info@isc.org>

# Index