Table of Contents

1 Introduction

1.1 What is SecExClipboard ?

SecExClipboard is designed primarily to be a travel-mate for SecExMail users. It's small size allows it to be stored on a floppy disk and carried anywhere. When reading or writing email from an internet café, while away from your home or office computer, SecExClipboard allows you to maintain your privacy. Like SecExMail, it implements open standard encryption algorithms to protect the privacy of your email on the public internet. SecExClipboard is compatible with SecExMail so any messages you send to a recipient who uses SecExMail will be readable to them.

How SecExClipboard works :

The images below show a message typed into SecExClipboard, before and after encryption with the recipient's public key. Note: The subject will appear as the email subject when the recipient receives the message.

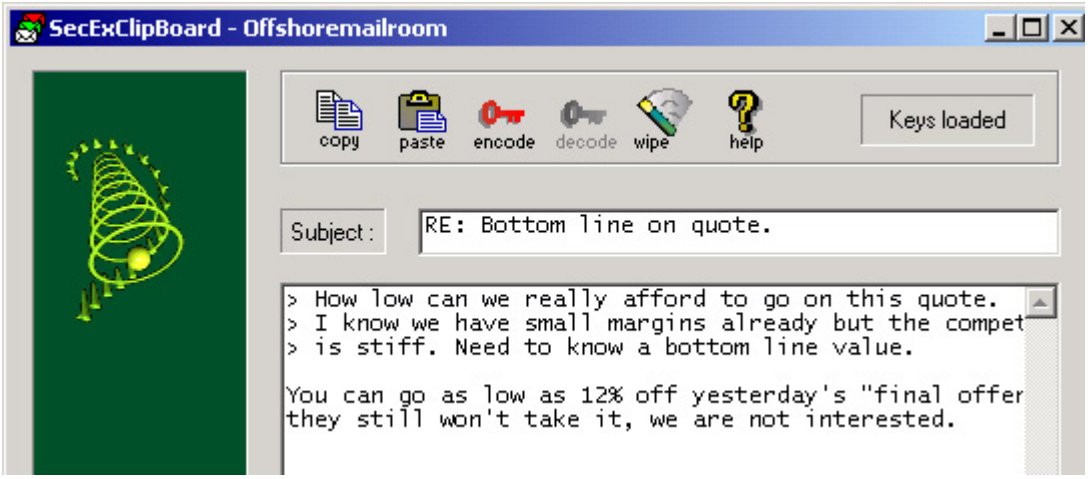
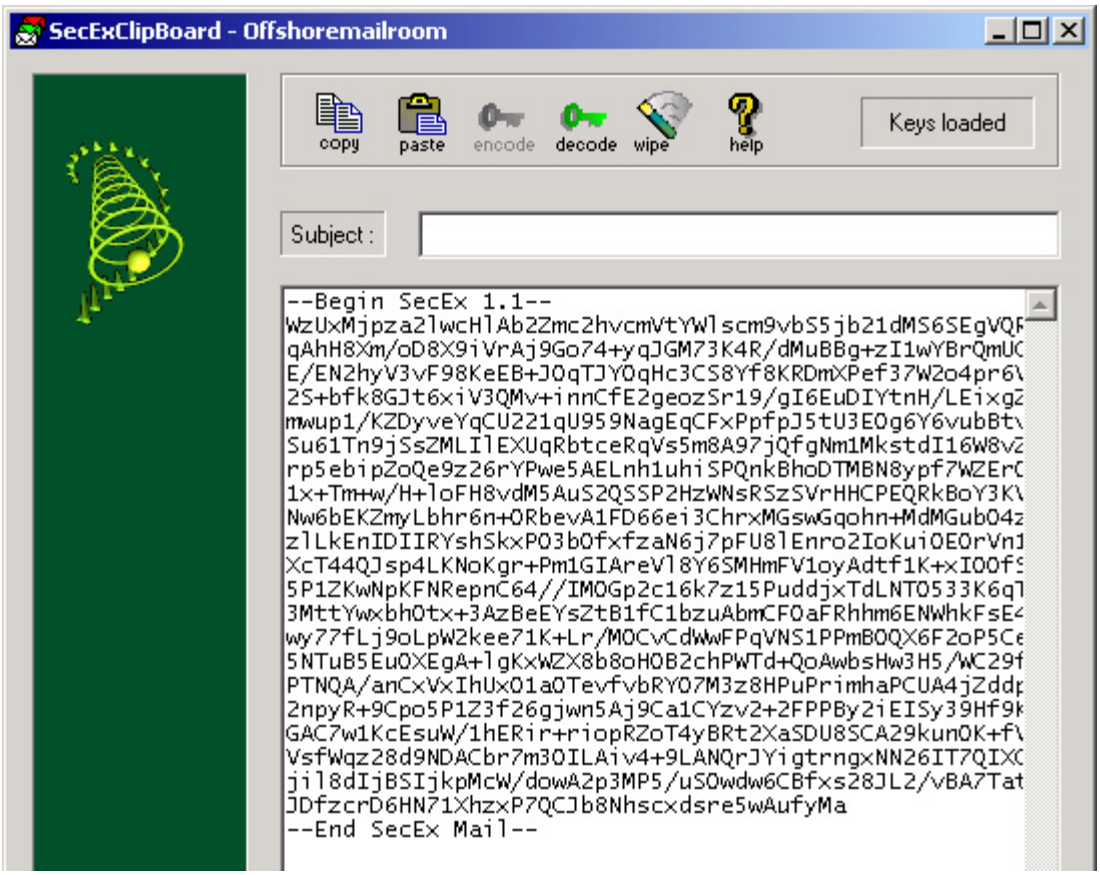


Image above: Clear text message typed directly into SecExClipboard.



Once encoded, the cypher text appears and can be copied to the clipboard and later to a web-based mail system for sending to the recipient.

General Features :

- Easy to configure

  SecExClipboard is one file. When you are going to be on the road, copy SecExClipboard to a floppy disk and export your SecExMail keys to the same floppy disk. That's it.

Technical Features :

- Public Key Encryption

  SecExClipboard uses standard RSA based public key encryption. Supported key sizes are 2048, 4096 and 8192 bits (up to 10240 bits for offshore edition and corporate edition). Two messages are never encrypted with the same session key. Instead the public key associated with the recipient of a message is used to encrypt a random session key which is used to encrypt the message. Generation of strong session keys is based on a sophisticated entropy collection system.

- Message Encryption

  Individual messages are double encrypted via 64 bit ISAAC and 256 bit Twofish encryption .

- Coexistence with other encryption standards

  SecExClipboard encrypts data and therefore does not interfere with existing methods of encryption. As such, it is possible to encrypt with PGP or GPG first, and then send the resulting cipher text through SecExClipboard for further encryption. On the remote end, the recipients SecExMail or SecExClipboard restores the PGP cipher text which can then be decrypted by the user's email client or associated PGP decryption module.

1.2 Making your SecExClipboard Disk

This is the guide for creating a floppy disk to be taken with you on the road.

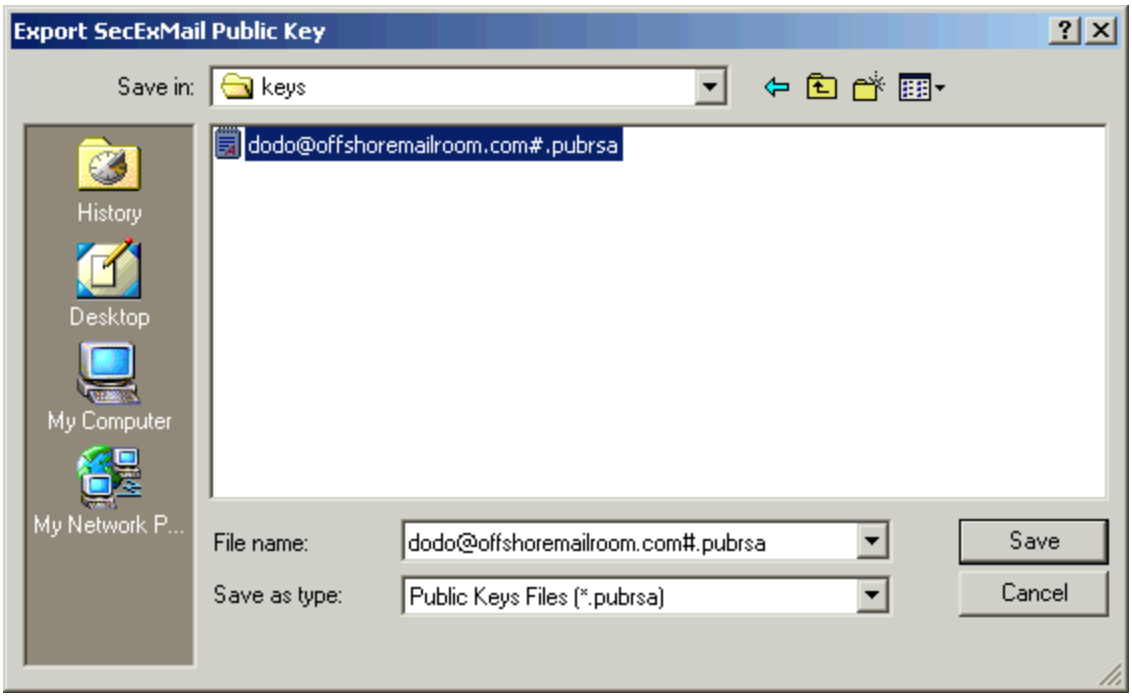
- **Step 1**

Copy SecExClipboard to a floppy disk.

- **Step 2**

Right-click the SecExMail tray icon on the computer where you have your keys stored, choose Open SecExMail. Click on the My Keys tab and then the Export Key Button.

Because your own keys are comprised of a public and a private key component, exporting your own key involves a two stage process. During the first stage the public key component is exported - a typical dialog to export SecEx public keys is shown below.

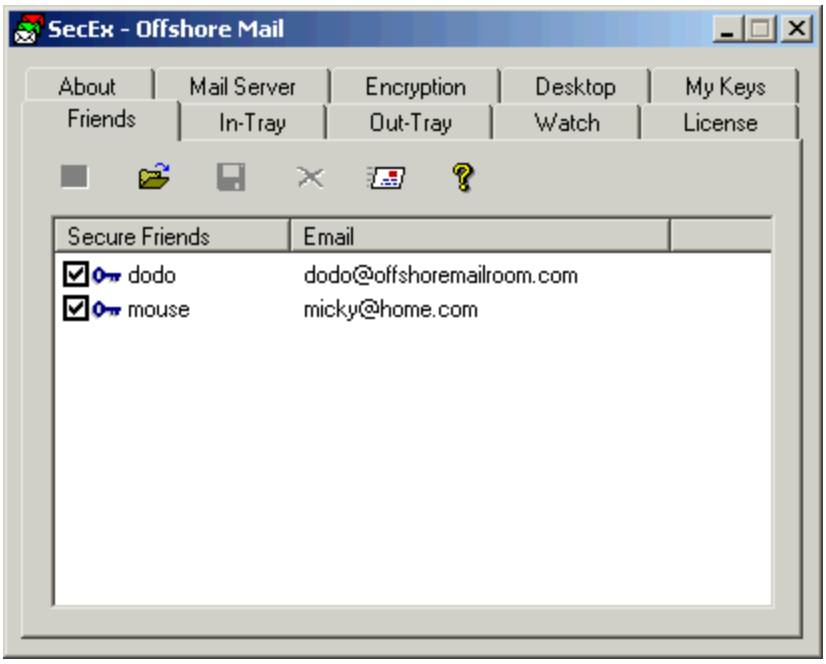


Save your Public Key in the same directory on the floppy disk as the SecExClipboard executable. You will then be prompted to decide if you wish to export the private key component also. See image below.

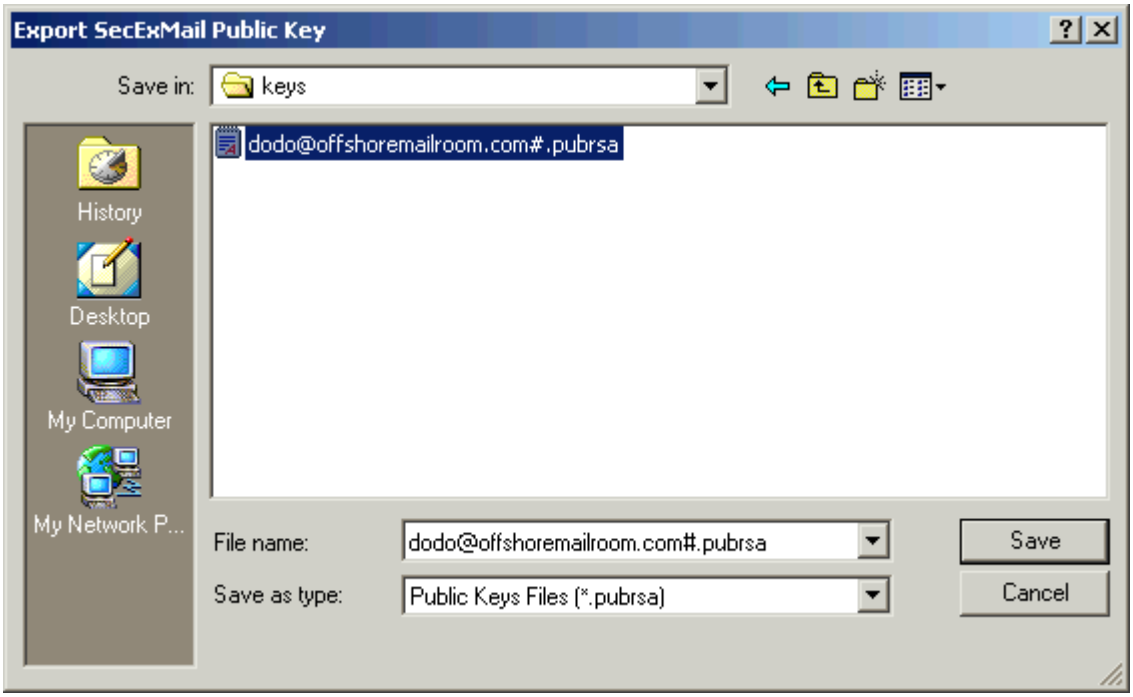
Choose Yes as you will need your Private key to read messages encrypted to you and you may need your public key if you wish to send it to a friend. Private keys are stored in 3DES encoded, chained block cipher format and protected with a passphrase but you should always keep your SecExClipboard disk secure.

- **Step 3**

You will need to export all of your Friend's keys who you wish to communicate with while you are on the road. To do this, click on the Friends tab. A typical Friends tab is shown below.



Choose a key and click the Export icon. A typical Export Key dialog is shown below.



Save the key in the same location as you saved your SecExClipboard executable and Private/Public keys.
Note: You will not be prompted to save a Private key as you should not have the Private key of a Friend.

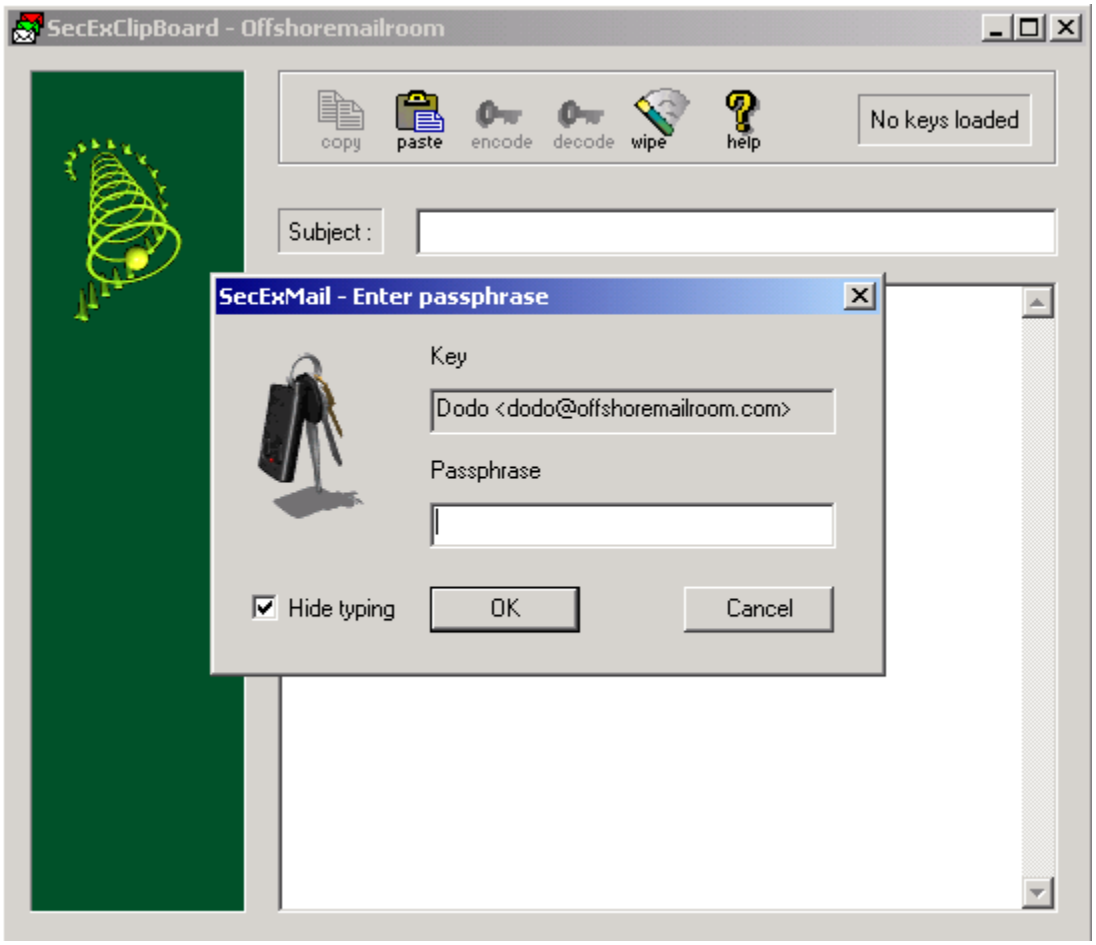
Repeat Step 3 for the keys of all Friends you may need to communicate with.

1.3 Using Your SecExClipboard Disk

It is a good idea to test your SecExClipboard Disk before leaving home. You may even wish to make a copy of the disk should one be damaged or lost.

- **Starting SecExClipboard**

Insert the floppy disk in the drive and browse to the location where you saved SecExClipboard and your keys. Double-click SecExClipboard. SecExClipboard will launch and request the passphrase for your Private Key. A typical window is shown below.



Enter your passphrase and click OK. SecExClipboard is now ready to encrypt and decrypt text.

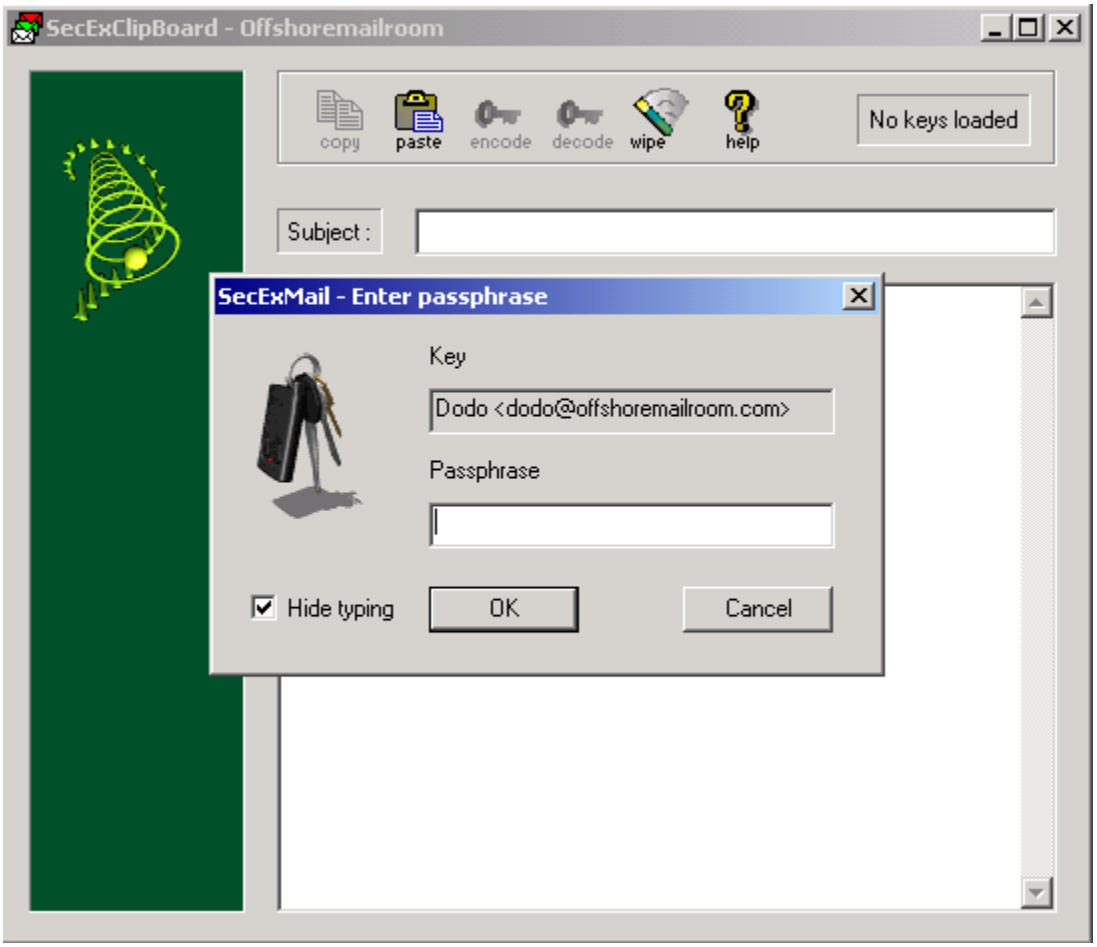
- **Working with Web-based mail.**

Receiving Messages

If you receive an encrypted message via Hotmail or any other web-based mail, select the body of the message and copy it to the clipboard. You can use ctrl-c or the copy icon of your browser to do this. Maximize SecExClipboard and click the Paste icon. The cypher text should now appear in the window. Click Decrypt to read your message.

Sending Messages

To send an encrypted message, you can either type the message directly into SecExClipboard or use a word processor and copy/paste it to SecExClipboard. Once you have the plain text message in the SecExClipboard window, click Encrypt. SecExClipboard will ask you which recipient you wish to encrypt the message to. A typical dialog is shown below.



Choose the recipient from the list and click OK. The cypher text will now appear in SecExClipboard window. Click the Copy icon and then paste this into a new mail message in your web-based email.

When the recipient receives the message, they can either use SecExMail or SecExClipboard to decrypt and read the message.

1.4 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/ "
```

- **SecExMail/SecExClipboard Cipher**

  Chris Kohlhepp and Mark Robertson, Bytefusion Ltd.

2 About

2.1 About SecExClipboard

SecExClipboard
Version 1.5

2.2 About Bytefusion Ltd.

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

Inquiries: sales@bytefusion.com

Index

- A -

- B -

- G -

- H -

- S -

- T -