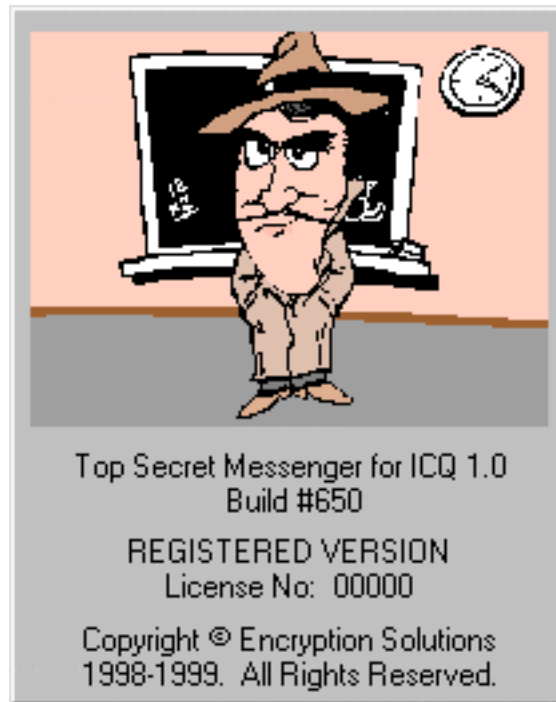


Top Secret Messenger for ICQ 1.0



This manual was written for use with Top Secret Messenger for ICQ 1.0. This manual and Top Secret Messenger for ICQ software are copyrighted, with all rights reserved. The information provided herein is subject to change without notice. In no event shall Encryption Software be liable to you or any other person for any indirect, special, incidental, or consequential damages of any character including, without limitation, any loss of revenue, loss of profits or other incidental or consequential damages arising out of the use or inability to use the information; Encryption Software makes no claim as to the suitability of the information.

All brand and product names are trademarks or registered trademarks of their respective owners.
Copyright © 1999 Encryption Software. All Rights Reserved.

Contents

| | |
|--|-----------|
| INTRODUCTION | 3 |
| TOP SECRET MESSENGER FOR ICQ | 3 |
| PUBLIC-KEY CRYPTOGRAPHY | 4 |
| GETTING STARTED | 5 |
| SYSTEM REQUIREMENTS | 5 |
| INSTALLATION | 5 |
| GENERATING PUBLIC/SECRET KEY PAIR | 6 |
| ENCRYPTING MESSAGES | 8 |
| DECRYPTING MESSAGES | 10 |
| DECRYPTING MESSAGE HISTORY | 11 |
| PUBLIC KEY MANAGEMENT | 12 |
| IMPORTING PUBLIC KEYS | 12 |
| EXPORTING PUBLIC KEYS | 12 |
| REMOVING PUBLIC KEYS (REGISTERED VERSION) | 12 |
| CHANGING PUBLIC KEY ID (REGISTERED VERSION) | 13 |
| ADVANCED FEATURES | 14 |
| AUTOMATIC ENCRYPTION | 14 |
| AUTOMATIC DECRYPTION | 14 |
| TECHNICAL SUPPORT | 15 |

Introduction

Top Secret Messenger for ICQ

Top Secret Messenger for ICQ (TSM) is a secure public-key encryption program that acts as an ICQ instant messenger's add-on to provide instant and easy access to powerful and virtually unbreakable encryption right from ICQ's message dialogs.

There are various reasons for encrypting all messages sent through ICQ network:

- All messages sent through ICQ are sent in completely unencrypted form and can be easily intercepted and read by anyone with the help of some special hacking tools.
- There are also a lot of tools that make it very easy for anyone to send you a "spoofed" message, a message that looks like it came from someone else (someone you know, perhaps). If all your conversations with your friends and colleagues are encrypted, on the other hand, messages sent to you can no longer be forged to look like they came from someone you know.

Public-Key Cryptography

In public-key cryptosystems, everyone has two complementary encryption keys: one public key and one secret key. The public key can be (and should be) safely distributed to everyone that you intend to have a secure conversation with. The secret key, on the other hand, should be stored in a private secure place and not revealed to anyone.

The message in a public-key cryptosystem is encrypted with both keys. For instance, in Elliptic Curve Cryptography algorithm that is used by TSM, a message is encrypted with both sender's secret key and recipient's public key. A message is then decrypted with recipient's secret key and sender's public key.

Getting Started

System Requirements

It is highly recommended that your system meet the following system requirements in order to get the best performance out of TSM:

- **Pentium 133Mhz or better**
- **16 MB of RAM**
- **Microsoft Windows 95/98/NT**
- **ICQ99 Build #1700 or better**

Installation

To install TSM, perform the following steps:

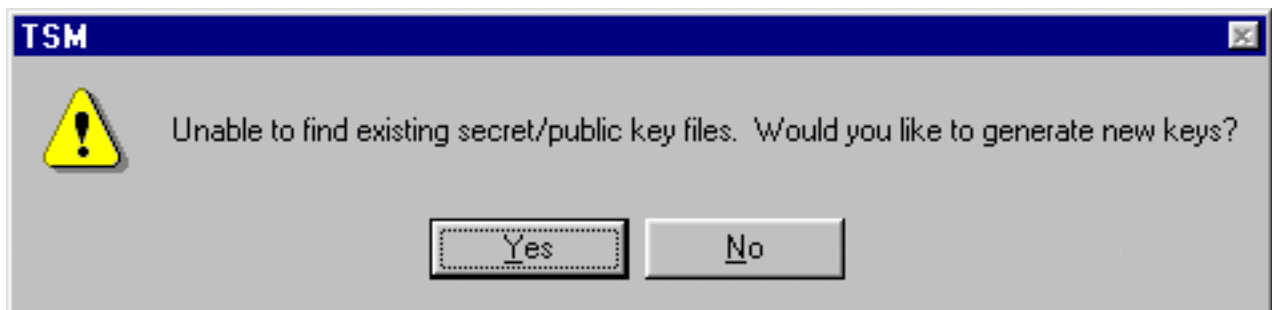
1. It is recommended to exit all applications (especially TSM) that you are currently running before starting the installation.
2. Double-click on the TSM executable file to start the installation program.

3. Click on the **Setup** button after the first information screen comes up.
4. Follow the rest of the installation directions provided by the installation program
5. Once the installation program finishes and quits, you should see a "Top Secret Messenger for ICQ" icon on your desktop. Double-click on it to start TSM.

Generating Public/Secret Key Pair

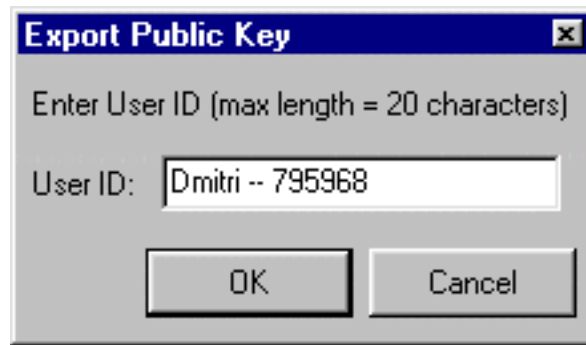
After you have installed TSM, double-click on the "Top Secret Messenger for ICQ" icon on the desktop.

1. If this is your first time installing TSM, you will be prompted to generate new public and secret keys:



2. To generate new keys, click the **Yes** button and TSM will prompt you to enter Public Key ID.

*If this is not your first time using TSM and you already have old key files, that you want to use, saved somewhere, click the **No** button and select the location of the old key files.*



Your Public Key ID is an identification that can be used to differentiate your key from others.

Registered version: If you want to take advantage of Automatic Encryption, you need to include the UIN number in the Public Key ID. Here are some examples of what your Public Key ID can be:

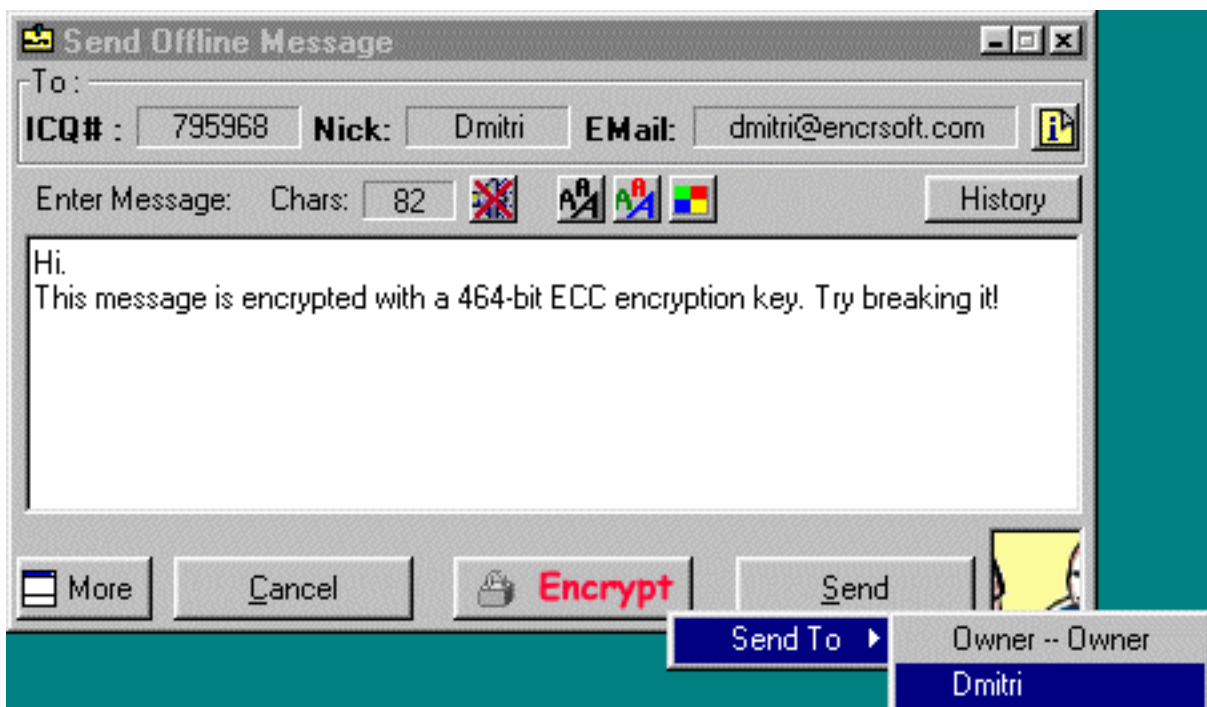
- *John Smith (654321)*
- *Nick*
- *Charles - 123456*
- *000007 - James Bond*

3. Once you type in the ID and click the **OK** button, you will be prompted to save your Public Key and then your Secret Key in separate files with extension *TSM*.

Encrypting Messages

To encrypt an ICQ message, do the following:

1. Type up your message as usual in ICQ's message dialog
2. Click on the **Encrypt** button in the Send Message dialog and select the name of the person that you wish to send an encrypted message to:



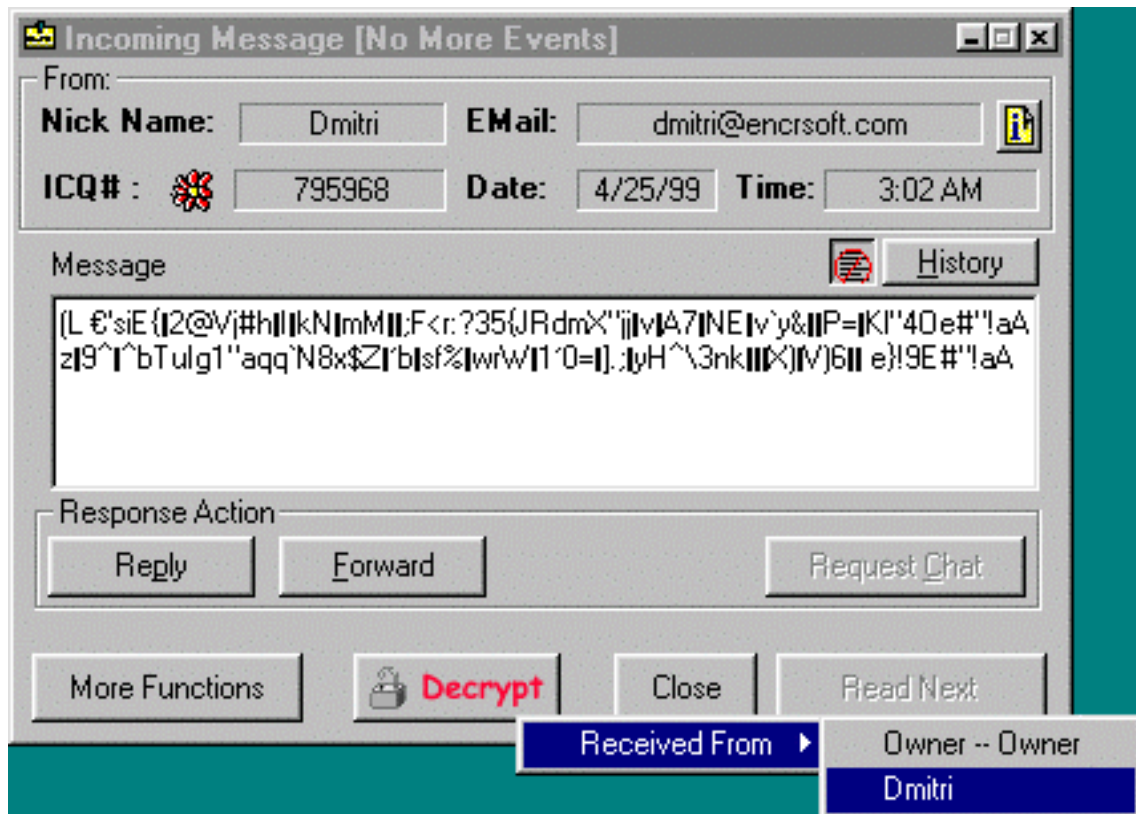
3. You should now see a bunch of unreadable symbols appear in your message window.

4. At this moment, you can safely click on the **Send** button, as usual, and your encrypted message will be sent to its destination.

Decrypting Messages

To decrypt an ICQ message, do the following:

1. Click on the **Decrypt** button in the Incoming Message dialog and select the name of the person that sent you this encrypted message:



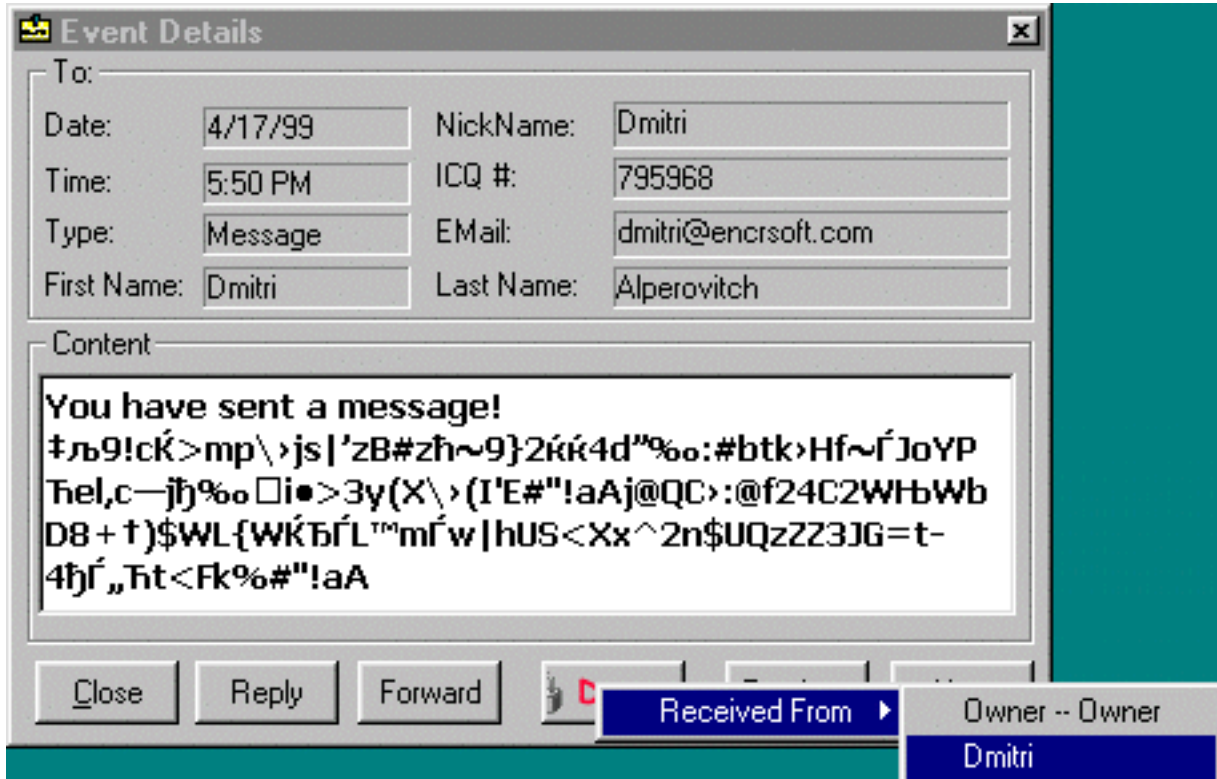
2. At this time, the message will be decrypted and you should see the readable message once again.

Decrypting Message History

(Registered Version)

To decrypt a message stored in ICQ's Message History, do the following:

1. Open Message History for the desired user in ICQ in the normal fashion.
2. Double-click on the encrypted message to open it.
3. Click on the **Decrypt** button and select the name of the person that sent the message.



Public Key Management

Importing Public Keys

To import someone else's public key into your public keyring, click on the **Import** button in Public Key Manager and find the key (file with extension *TSM*) that you want to import.

Exporting Public Keys

Whenever you want to send a public key to someone (whether it is yours or not), never send your PUBLIC.TSM file, since it contains not just the key that you want to send but all the other public keys that you might have.

Instead, select the key that you want to export in Public Key Manager and click on the **Export** button. TSM will prompt you for a Public Key I.D. that will be associated with that key and then for a filename to save that key as.

Removing Public Keys (Registered Version)

To remove a public key from your keyring, simply select that key in Public Key Manager and click on the **Remove** button.

Beware: The key will be permanently removed from your keyring. You will not be able to restore it later, unless it is backed up somewhere.

Changing Public Key ID (Registered Version)

You can change the Public Key ID associated with any public key in your keyring any time. Select that key in Public Key Manager, click on the **Change ID** button and type in the new ID.

Advanced Features

(Registered Version)

Automatic Encryption

Automatic Encryption feature makes encryption of ICQ messages easier than ever. Essentially, it takes over the task of clicking on the **Encrypt** button and selecting the recipient's public key. When Automatic Encryption is enabled, you only have to click on the **Send** button, as you would normally do, and the message is going to be automatically encrypted with the correct key and sent to the recipient (Note: The message will only be encrypted if you have the receiver's public key in your public keyring and it is named correctly -- See *Generating Public/Secret Key Pair* for more information).

Automatic Decryption

Automatic Decryption feature, similarly to *Automatic Encryption*, performs the tedious task of clicking on the **Decrypt** button and selecting the appropriate sender's key for you. If the sender's public key is in your keyring and it is named correctly (See *Generating Public/Secret Key Pair* for more information), all incoming encrypted messages will be decrypted on-the-fly without the need for you to perform the decryption steps.

Technical Support

Encryption Software

P.O. Box 237

Rossville, GA 30741-0237

E-mail: support@encrsoft.com

WWW: <http://www.encrsoft.com/>

To report bugs, please send us a detailed message describing your problem and your system (be sure to include the Operating System, Processor, Amount of Memory, ICQ version, and TSM version) at bugs@encrsoft.com