

## Hiron 3.1.7.13



# Hiron 3.1.7.13

## E-Mail Privacy Protection System

---

*by Academia*

*«Hiron» is designed to provide the highest-level, long-term security to personal information sent over e-mail.*

*The Project's goal is to assure a protection that could stand all kinds of feasible attacks by use of available computing facilities during years to come, bearing in mind the estimated technological progress.*

*To achieve this goal, «Hiron» employs a sophisticated cryptographic system that involves a series of strongest known cryptographic algorithms (such as Rijndael, Twofish, ...), which are incorporated as building-blocks within an innovative encryption technology. A higher-order elliptic curve is used for asymmetric (public key) encryption.*

*The program was designed and implemented by a professional theoretical physicist who also is an experienced cryptography programmer.*

## Hiron 3.1.7.13

© 2009 Academia

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Printed: November 2009 in Canada.

### **Publisher**

*Academia*

### **Managing Editor**

*Project Developer*

### **Technical Editors**

*Designer*

*Technical Editor*

### **Cover Designer**

*Project Manager*

### **Team Coordinator**

*Prof. Theor. Phys. Dr. Hiron*

### **Production**

*Academia Inc.*

### **Special thanks to:**

*All the people who contributed to this document by assistance or advice*

# Table of Contents

Foreword	7
<b>Part I Installation</b>	<b>10</b>
1 Security Issues.....	10
2 Disclaimer.....	11
3 Overview.....	12
4 System Requirements.....	14
5 Installation Instructions .....	15
6 Known issues.....	17
7 Uninstalling Hiron.....	18
<b>Part II Registration</b>	<b>20</b>
1 Registration Procedure: Step 1 .....	20
2 Registration Procedure: Step 2 .....	23
<b>Part III Key Management</b>	<b>30</b>
1 About the Keys.....	30
2 Key Generation.....	30
3 Sending your open key.....	33
4 Receiving open key in attachment .....	35
5 Receiving another person's open key.....	37
<b>Part IV Encrypting documents</b>	<b>42</b>
1 Typing in a text to the document.....	42
2 Documents composing and encryption.....	42
3 Encrypting the contents of the active document.....	43
4 Information displayed on the Statusbar .....	45
<b>Part V Sending a message</b>	<b>48</b>
1 Sending a message, encrypted or not .....	48
<b>Part VI Encrypting files</b>	<b>56</b>
1 Encrypting disk files .....	56
<b>Part VII Decrypting documents</b>	<b>60</b>
1 Document decryption.....	60
2 Receiving an encrypted message.....	60
<b>Part VIII Decrypting files</b>	<b>64</b>

1 Decrypting disk files .....	64
<b>Part IX Signing disk files</b>	<b>68</b>
1 Signing disk files.....	68
2 Verifying disk file's signatures .....	69
<b>Index</b>	<b>0</b>

# Foreword

«The information age has seen the development of electronic pathways that carry vast amounts of valuable commercial, scientific, and educational information between financial institutions, companies, individuals, and government organisations.

Unfortunately the unprecedented levels of access provided by systems like the Internet also expose this data to breaches of confidentiality, disruption of service, and outright theft. As a result, there is an enormous (and still growing) demand for the means to secure these online transactions. One report by the Computer Systems Policy Project (a consortium of virtually every large US computer company, including Apple, AT&T, Compaq, Digital, IBM, Silicon Graphics, Sun, and Unisys) estimates that the potential revenue arising from these security requirements in the US alone could be as much as US\$30-60 billion in the next few years, and the potential exposure to global users from a lack of this security is projected to reach between US\$320 and 640 billion.

Unfortunately the security systems required to protect data are generally extremely difficult to design and implement, and even when available tend to require considerable understanding of the underlying principles in order to be used. This has led to a proliferation of "snake oil" products that offer only illusionary security, or to organisations holding back from deploying online information systems because the means to secure them aren't readily available, or (in the case of some [...] products) because they employ weak, easily broken security which is unacceptable to users.

Peter Gutmann  
July 2003

Hiron is a program that is intended to provide an answer to the problem mentioned above, with respect to an individual user's personal purposes.

It was designed and implemented by a professional theoretical physicist, who also is an experienced cryptography programmer. Originally, the product was developed by the author for his own personal needs and use.





**Hiron 3.1.7.13**

**Part**



# 1 Installation

Overview, system requirements, installation instructions, known issues, uninstalling Hiron.

## 1.1 Security Issues

### Security Issues

«The information age has seen the development of electronic pathways that carry vast amounts of valuable commercial, scientific, and educational information between financial institutions, companies, individuals, and government organisations.

Unfortunately the unprecedented levels of access provided by systems like the Internet also expose this data to breaches of confidentiality, disruption of service, and outright theft. As a result, there is an enormous (and still growing) demand for the means to secure these online transactions. One report by the Computer Systems Policy Project (a consortium of virtually every large US computer company, including Apple, AT&T, Compaq, Digital, IBM, Silicon Graphics, Sun, and Unisys) estimates that the potential revenue arising from these security requirements in the US alone could be as much as US\$30-60 billion in the next few years, and the potential exposure to global users from a lack of this security is projected to reach between US\$320 and 640 billion.

Unfortunately the security systems required to protect data are generally extremely difficult to design and implement, and even when available tend to require considerable understanding of the underlying principles in order to be used. This has led to a proliferation of "snake oil" products that offer only illusory security, or to organisations holding back from deploying online information systems because the means to secure them aren't readily available, or (in the case of some [...] products) because they employ weak, easily broken security which is unacceptable to users.»

*Peter Gutmann  
July 2003*

**Hiron** is a program that is intended to provide an answer to the problem mentioned above, with respect to an individual user's personal purposes. It was designed and implemented by a professional theoretical physicist, who also is an experienced cryptography programmer. Originally, the product was developed by the author for his own personal needs and use.

[Overview](#)

## 1.2 Disclaimer

### Lisence

The author ("developer") hereby grants you ("user") a non-exclusive personal license to use the standard version of the **Hiron** ("Product") subject to the following disclaimer, terms and conditions:

**USER AND ANY INVOLVED PARTIES ARE NOT ALLOWED, AND EXPLICITLY AGREE NOT TO DISASSEMBLE, MODIFY, PATCH OR ALTER IN ANY OTHER POSSIBLE WAY, IN WHOLE OR IN PART, THIS AND ANY SUBSEQUENT VERSION OF THE PRODUCT OR ITS DOCUMENTATION.**

### Disclaimer

The developer has made every effort to ensure the reliable, stable, and efficient functioning of the Product. The Product has been tested on various machines, under different Windows Operating Systems, during a largely extended period of time.

**THE CURRENT RELEASE OF THE PRODUCT CONTAINS NO KNOWN BUGS  
IN MANY HUNDREDS ENCRYPTION-DECRYPTION CYCLES  
PERFORMED WITH RESPECT TO VARIOUS MESSAGES AND FILES  
NOT A SINGLE ONE FAILED**

Yet the developer makes no warranty or representation that the operation of the Product (**Hiron**) will be flawless on every specific computer. In particular, the developer is under no obligation to provide any services, by way of maintenance, update, or otherwise.

**THE DEVELOPER DISCLAIMS ALL WARRANTIES,  
EITHER EXPRESSED OR IMPLIED,  
INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES  
OF FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO  
THE SOFTWARE OR DOCUMENTATION.**

**IN NO EVENT WILL THE DEVELOPER BE LIABLE  
FOR ANY DAMAGES WHATSOEVER ARISING OUT OF THE USE  
OR THE INABILITY TO USE THIS PRODUCT  
EVEN IF THE DEVELOPER HAS BEEN ADVISED  
OF THE POSSIBILITY OF SUCH DAMAGES.**

**IN PARTICULAR, THE DEVELOPER SHALL HAVE NO LIABILITY  
FOR ANY DATA STORED OR PROCESSED WITH THIS SOFTWARE,  
INCLUDING THE COSTS OF RECOVERING SUCH DATA.**

**AS A RESULT, THIS SOFTWARE AND DOCUMENTATION**

**ARE LICENSED 'AS IS' AND YOU, THE USER,  
ARE ASSUMING THE ENTIRE RISK  
AS TO ITS QUALITY AND PERFORMANCE.**

**The product is not licensed for use by governments,  
governmental institutions, governmental organizations, and  
government's employed agents, when on execution of their duties.**

### [Overview](#)

## **1.3 Overview**

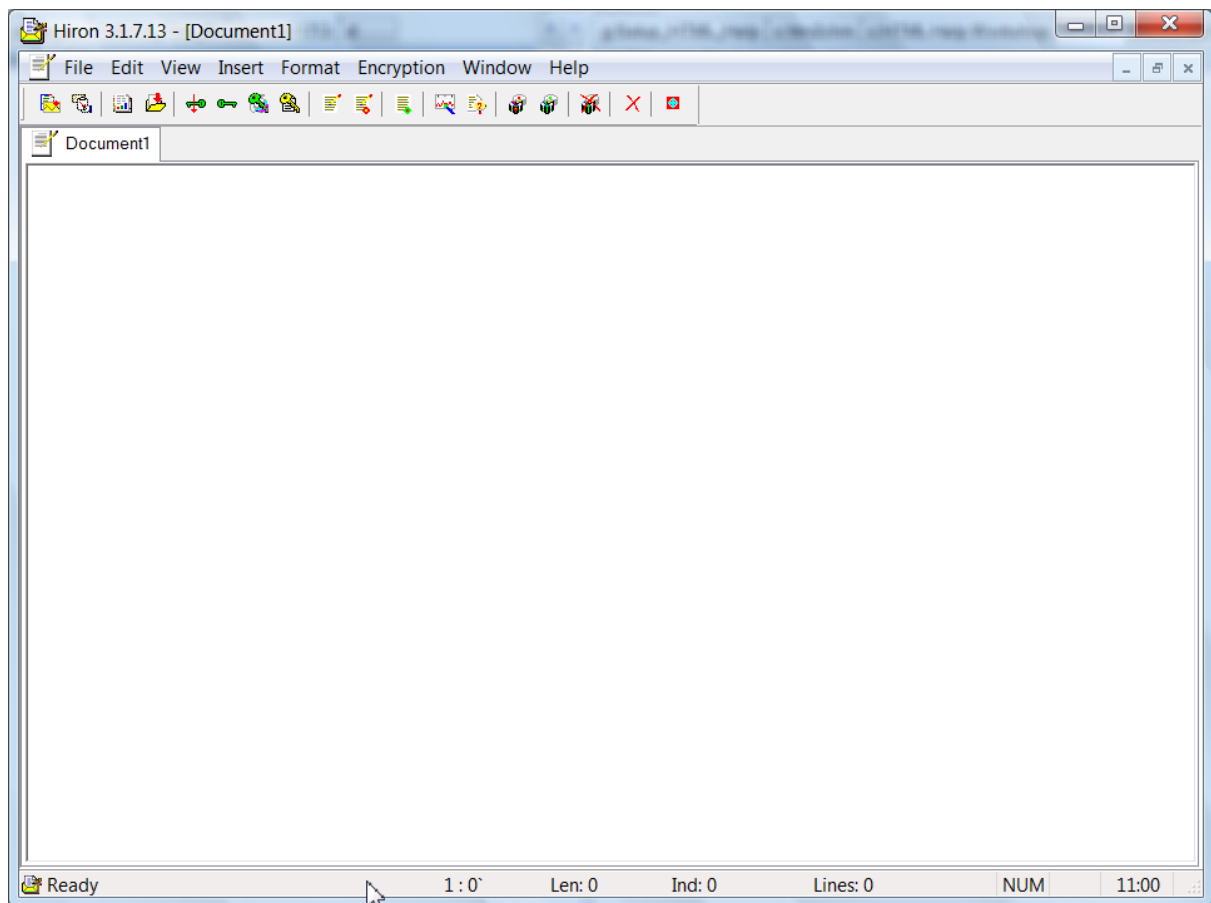
### **Overview**

**Hiron** is designed to ensure privacy of the user's personal e-mail communications.

This is achieved by encrypting, and then encoding the Sender's message in a special way at one end of the communication line before dispatching it by ordinary e-mail channels via Internet. At the other end of the communication line, the received message is decoded, decrypted and translated into a human-readable form.

All of the Sender's messages are treated as "Documents".

The program's Main Window is of the MDI (Multiple Documents Interface) type, which allows the user to open and handle several documents simultaneously. Each open document is composed and saved in the RTF (Rich Text Format) format, thus offering the user a variety of options as to the fonts, type faces, letter sizes, and colors to apply to the text of the document. All of the basic commands of a Word Processor, such as Copy, Cut, Paste, Undo, Redo, and Drag-and-Drop, as well as their conventional keyboard shortcuts, are supported by the **Hiron**.



**Fig 1. Hiron.** The Program's Main Window with the Special Toolbar displayed

When working on a document, the essential information about the document's current state, such as the total number of lines, current cursor position, the number of characters in the document, is displayed in real-time mode on the Main Window's [Statusbar](#).

To [encrypt](#) documents, the program takes advantage of an asymmetric ([Public Key](#)) Elliptic Curve encryption scheme, also enabling the user to [sign](#) his own documents or files digitally, as well as to verify other user's digital signatures. [Exchanging Public Keys](#) between users is quite simple: in most cases they can be sent as an attachment to a message's text.

To facilitate [handling e-mail messages](#), **Hiron** has a built-in MailDispatcher, which is a unit for sending e-mail messages in a fast and safe way, both plain and encrypted, with significantly extended functionality.

Also, **Hiron** can work in conjunction with Microsoft's Outlook Express e-mail client. This makes all of the tools incorporated into the Outlook Express, including Microsoft's Windows Address Book, available to the user when handling documents by means of «Hiron».

Every composed document, whether encrypted or not, can easily be [Sending a message](#) by simply clicking an appropriate button on the Main Window's Toolbar. This can be done in two

ways: the document's text can either be automatically inserted directly into the e-mail message window or it can be automatically compressed and put into the attachment to the user's e-mail message.

Besides, the **Hiron** offers the possibility of [Encrypting disk files](#) saved on the user's hard disk. An encrypted file can then immediately be sent over e-mail as an attachment to the user's message.

The **Hiron** is protected against disassembling, reverse engineering, debugging, or tracing the program's normal functioning, as well as against tampering with the program's code. After its installation and registration, the **Hiron** becomes locked to the licensed user's specific computer and can no longer be transferred to any other machine.

In order not to compromise the Product's protection, Help system has not been incorporated in the program's code, so it cannot be accessed from within the running program.

However, the compiled Help file **Hiron.chm** is included in the distribution and can easily be accessed any time you wish by going to **Start-> All Programs -> Hiron** and clicking on the **Hiron Help** menu item.

#### [System requirements](#)

## 1.4 System Requirements

### System Requirements

System Requirements to install and run the **Hiron** are minimal:

- Pentium® III class processor of 400 MHz or higher;
- Microsoft® Windows® Operating System:
  - Windows NT 4.0 with Service Pack 5 or 6 (Service Pack 6 recommended), or
  - Windows 2000 with Service Pack 3, or
  - Windows XP Professional Edition,
  - Windows Vista Ultimate (or Business) Edition;
- 512 MB of RAM;
- 10 MB of space available on your hard disk;
- Floppy 3.5" drive or a slot for a USB Flash/Hard Drive;

---

#### Note:

Network connections are required for the program to run. This does NOT imply that the program would only run when the user's computer is connected to the Internet. In fact, certain DLL files, which are placed into the Windows System Directory when installing Windows Network

Connections, are invoked by «Hiron» for its internal purposes.

**MAKE SURE THE WINDOWS NETWORK CONNECTIONS  
ARE INSTALLED ON YOUR COMPUTER**

**YET AN ACTIVE CONNECTION TO THE INTERNET IS  
NOT REQUIRED FOR «HIRON» TO RUN**

---

In order for the Hiron application to operate on your machine properly, the **Microsoft Enhanced Cryptographic Provider v1.0** must be installed on your Windows Operation System. To check whether this CryptoProvider is installed on your computer, a small utility **GetInstalledCryptoProviders.exe** is included in the Distribution Package. You may find it in the Installation Folder you defined during installation. This is a console application, which, when launched, displays **Provider Types, Provider Names**, and the **Default Provider Name** installed on your machine, along with the list of the latter's **supported algorithms**, which are available on your machine.

You should be able to locate the **Microsoft Enhanced Cryptographic Provider v1.0** among the listed **Provider Names**, no matter what the displayed **Default Provider Name** is.

**Note:**

This utility will not work on Windows NT Operation Systems. The reason is that the older library «advapi32.dll» supplied by Microsoft with its Windows NT 4.0 Operation System does not support certain functions called by the executable **GetInstalledCryptoProviders.exe**.

[Installation Instructions](#)

## 1.5 Installation Instructions

### Installation Instructions

[Overview](#)

[Security issues](#)

[System requirements](#)

---

**WARNING!**

**IF THE OPERATION SYSTEM INSTALLED ON A COMPUTER IS  
WINDOWS 2000,  
or WINDOWS XP, or WINDOWS VISTA, ONLY ADMINISTRATORS CAN  
INSTALL  
OR RUN THE HIRON APPLICATION!**

**USERS HAVING A «LIMITED» ACCOUNT TYPE MAY NOT BE ABLE TO  
INSTALL  
OR TO RUN THE HIRON APPLICATION ON SUCH COMPUTER.**

---

Therefore, if your Windows Operation System is Windows 2000, or Windows XP, or Windows Vista, make sure **you are logged on as Administrator** or, if a User, **you have the rights of Administrator**.

To install **Hiron** on your Windows system, run the installation program **Setup31713.exe**. This can be done, for instance, by clicking **Start -> Run -> Browse...** on the Window's Taskbar, then locating the executable file **Setup31713.exe** on your hard disk (in the folder you have chosen to unpack the original package), and finally clicking the **OK** button.

The installation program proceeds as follows.

- a) First, a **Message** Box will prompt you that you are going to install **Hiron** application on your computer. If you wish to continue, click **YES**.
- b) Second, the **LICENSE AGREEMENT** Window opens up, displaying the Developer's declaration as to the respect of the user's privacy and the reliability of the product, as well as **LICENSE**, **WARNING** and **DISCLAIMER** Sections.
- c) If you accept the agreement, click on the **CheckBox** to confirm that you have read the Agreement and WARNING, and accepted them. Then click on the **Next>** button to proceed; otherwise click **Cancel** to stop the installation process.
- d) Clicking on **Next>** brings up the next **Dialog** Window asking you to choose the **Destination Folder**. In the **Destination Folder** field you have to specify a Folder on your hard drive where to place the files of the **Hiron** application. By default, the **"Program Files\Hiron31713"** folder on your computer is set by the Installer as the **Destination Folder**. However, you may define any other folder you like, including a new one. Type in the desired folder's Name or browse you hard drive(s) to select one by clicking on the **Browse...** button.
- e) Then click the **Install** button to start the installation.
- f) The installation program unpacks two files **tasp32s.exe** and **taspdll.dll**; the



first is copied to the **Destination Folder**, whereas the second is copied to the **System Directory** of your Windows Operation System. Also the Installer creates on your hard disk a new folder with the **Name** that you defined as the **Destination Folder** at the previous step **d)**. Besides, for the application's further use, the installation program creates a folder named **Hml31713** in the Windows **System Directory**.

- g) In addition, icons named **Hiron** are placed on the Desktop of your computer, as well as on the **Quick Launch** Bar. Later on, the program can be launched by one of the following four ways:
  - i. Double-clicking the **Hiron** icon on the **Desktop**, or
  - ii. Single-clicking the **Hiron** icon on the **Quick Launch** Bar, or
  - iii. Going to **Start -> All Programs -> Hiron** and clicking on the **Hiron** icon, or
  - iv. Pressing (simultaneously) the **Ctrl+Shift+Alt+H** buttons on your Keyboard (may not work always, depending on the specific configuration parameters of your Windows System).
- h) The installation process takes a few (3 - 5) seconds. When it is finished, the **Help** Window is opened automatically, displaying the steps of the **Registration Procedure** that will begin. Read the description of the Procedure and close the **Help** Window.
- i) On closing the installation program's window, the application is started, and the **Registration Procedure** begins as described at the previous step **h)**.

#### [Registration procedure](#)

## 1.6 Known issues

### Known issues

On **Windows XP Professional** Operating Systems, when trying to encrypt/decrypt several messages and files one after another **within one and the same session**, the program (**Hiron**) may suddenly close down.

[This should not be confused with the case when the program closes down during **decryption** as a consequence of a wrong password supplied to it. Such a behavior is normal.]

This phenomenon appears to be due to a hidden bug in the memory management employed by **Windows XP Professional** Operating Systems, as it has never occurred on Windows Vista Operating Systems.

None the less, even on **Windows XP Professional** Operating Systems this sudden closing down has never resulted in an error with respect to encryption or decryption operations on individual files or documents—these have always been completed successfully.

As a result, if on a **Windows XP Professional** Operating System the program suddenly closes down, simply restart it and resume encryption/decryption.

[Disclaimer](#)

## 1.7 Uninstalling Hiron

### Uninstalling Hiron Application

**Hiron** application can easily and safely be removed from your computer.

To remove **Hiron** from your Windows system, follow **one** of the following two ways.

- Go to **Start -> Programs -> Hiron** on your Window's Taskbar, and click the **Uninstall Hiron** icon, or
- Go to the **Control Panel** of your Windows Operation System, and
  - Click on the **Add or Remove Programs** icon,
  - Locate the **Hiron** icon and click on it.

---

#### **Note:**

The Uninstaller does not destroy your License Information. It will be kept on your machine so long as your Hardware and the Windows System remain essentially the same

If later on you decide to reinstall the Hiron application on the same computer and the same Windows System, you will not have to register the application again.

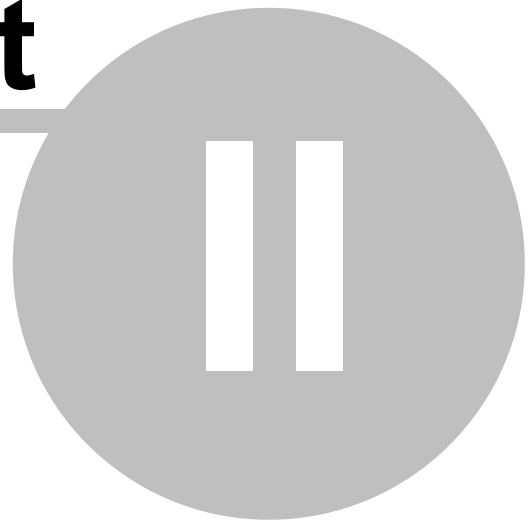
---

[Disclaimer](#)

**Hiron 3.1.7.13**

**Part**

---



## 2 Registration

Registration steps to get Hiron running

### 2.1 Registration Procedure: Step 1

#### Registration Procedure

[Overview](#)

[Security issues](#)

[System requirements](#)

When **Hiron**'s installation is finished, the main program will start automatically. The Registration Procedure begins.

The Registration Procedure takes two steps.

To complete it, you will have to communicate with the developer by e-mail TWICE.

#### First Step

1. First, the **REGISTRATION INFORMATION** Dialog Box is displayed:

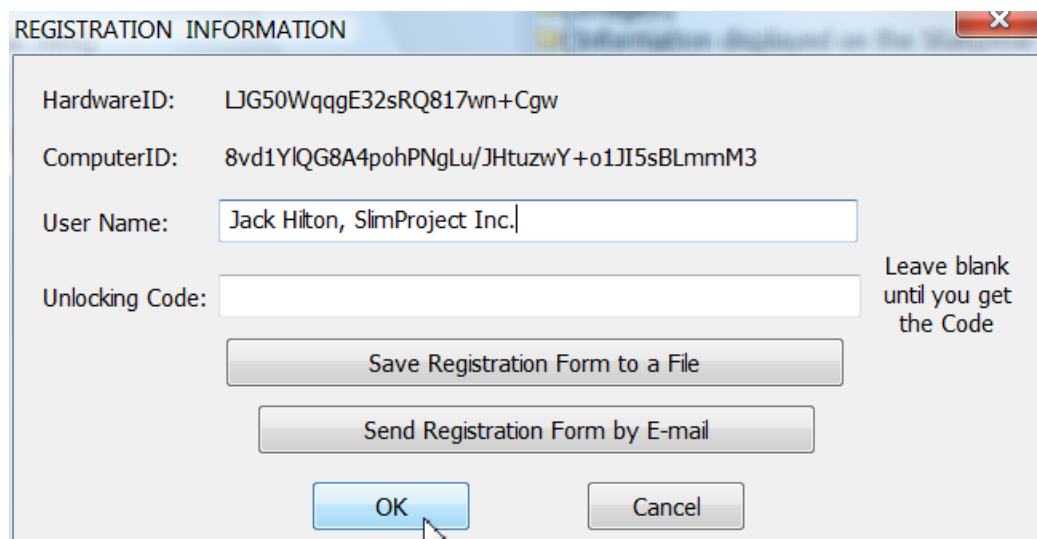


Fig 1. First Registration Dialog Box

The first two fields **HardwareID** and **ComputerID** of this Dialog Box are filled by the program automatically by the precomputed data specific for every particular machine. The data cannot be changed by the user.

The third field **User Name** of the Dialog Box is also filled automatically and

contains the *User's Name* and the *User's Organization* who are the Registered Owners of the Windows Operation System that runs on the machine. However, the user may edit this field by filling it with the desired name of the person whom **Hiron** software should be licensed to.

The fourth field **Unlocking Code** is to be left empty, at the moment.

1. After editing the third field **User Name** of the Dialog Box, you have to generate your Registration Form by clicking either one of the two buttons available on the Dialog Box: **Save Registration Form to a File** or **Send Registration Form by E-Mail**.

- a) If the button **Save Registration Form to a File** is clicked, the program automatically generates the Registration Form and stores it on your hard disk in a file named "**C:\HironRegForm\_for\_Your Name.txt**". You have then to open the file in a Text Editor like **Wordpad**, and to edit it by filling the required fields of the Registration Form *without modifying those filled in by the program automatically*. Example:

---

R E G I S T R A T I O N   F O R M

This Registration Form is to be filled and mailed  
to the developer's current e-mail address  
as the first step in registering Hiron 3.1.7.13 application  
=== Fields marked by asterisk «\*» are mandatory ===

---

GENERAL INFORMATION

\*Your Name: \_\_\_\_\_

\*Reference Number of your AUTHORIZED order: \_\_\_\_\_

Phone Number: \_\_\_\_\_ Fax: \_\_\_\_\_

\*Email Address: \_\_\_\_\_

Street: \_\_\_\_\_

\*City: \_\_\_\_\_ State/County: \_\_\_\_\_

\*Country: \_\_\_\_\_ \*Postal Code: \_\_\_\_\_

---

W A R N I N G!

THIS SECTION WAS GENERATED AUTOMATICALLY  
DO NOT MODIFY THE REGISTRATION DATA!

HardwareID: LJG50WqqgE32sRQ817wn+Cgw  
ComputerID: 8vd1YlQG8A4pohPNgLu/JHtuzwY+o1JI5sBLmmM3  
User Name: Jack Hilton, SlimProject Inc.

---

Fill in the Form and mail it to the developer.

Your Form will be processed as soon as your order is confirmed.

---

The prepared Registration Form is to be sent over e-mail to the

developer in order to get the **Unlocking Code** in reply.

b) Should the button **Send Registration Form by E-Mail** be clicked, the Outlook Express' New Message Window is opened, and the generated Registration Form is automatically placed in the text area of this New Message Window.

**REGISTRATION FORM**

This Registration Form is to be filled and mailed as the first step in registering the Hiron application  
 === Fields marked by asterisk <\*> are mandatory ===

---

**GENERAL INFORMATION**

\*Your Name: \_\_\_\_\_

\*Reference Number of your AUTHORIZED order: \_\_\_\_\_

Phone Number: \_\_\_\_\_ Fax: \_\_\_\_\_

\*Email Address: \_\_\_\_\_

Street: \_\_\_\_\_

\*City: \_\_\_\_\_ State/County: \_\_\_\_\_

\*Country: \_\_\_\_\_ \*Postal Code: \_\_\_\_\_

---

**W A R N I N G!**

THIS SECTION WAS GENERATED AUTOMATICALLY  
 DO NOT MODIFY THE REGISTRATION DATA!

HardwareID: dpQuWk1Ab2/AZj27KdzGqdM6  
 ComputerID: qbg195/M9V7K+TzfHxHh3T9geY8Cvz1pNGeoAQgO  
 User Name: Your Name

---

Fill in the Form and mail it to the developer.

You have to fill the required fields of the Registration Form and send it to the developer as you would send any other e-mail message. The developer's e-mail address is entered into the field **To:** of the New Message Window automatically.

The first step in registering your **Hiron** software is thereby finished.  
 You have to proceed to the second step as follows: *click the link below.*

[Registration: Step 2](#)

## 2.2 Registration Procedure: Step 2

### Registration Procedure: Second Step

In reply to your sending the filled Registration Form to the developer by e-mail, you will get an e-mail message with your **Unlocking Code** and instructions as to how to proceed with your Registration. The message's text may look as follows:

```
...

Please find your Registration Data as follows:

HardwareID:  LjG50WqqgE32sRQ817wn+Cgw
ComputerID:  8vd1YlQG8A4pohPNgLu/JHtuzwY+o1JI5sBLmmM3
User Name:   Jack Hilton, SlimProject Inc.
Unlocking Code: g93co9u8eq0K6lIQ3blI5OP9FemGQfNUF9t7xVR=

-----

Run the program and enter these data exactly as they appear
above
into the appropriate fields of the First Dialog Box. Then
click OK.

The Second Dialog Box will appear, showing your "Hardware
fingerprint" and containing two additional fields: "Name" for
the user's name, and the "Key" field, which is empty.

...
```

**Fig 1. Response message to your sending the Registration**

#### Form

1. On receiving this message, start **Hiron** (by double-clicking its icon on the desktop of your computer). The First Dialog Box (as shown in Fig. 2 below) will reappear.

REGISTRATION INFORMATION

HardwareID: LjG50WqqgE32sRQ817wn+Cgw

ComputerID: 8vd1YlQG8A4pohPNgLu/JHtuzwY+o1JI5sBLmmM3

User Name: Jack Hilton, SlimProject Inc.

Unlocking Code:

Leave blank until you get the Code

Save Registration Form to a File

Send Registration Form by E-mail

OK Cancel

**Fig 2. Registration: First Dialog Box**

Use the data indicated in the relevant fields of the e-mail message in Fig. 1 to fill the two fields **User Name** and **Unlocking Code** of the Dialog Box shown in Fig. 2. The best way to do this is to use the Copy–Paste procedure.

**WARNING:**

Make sure there are no other characters on the right-hand side of pasted data strings in the fields of the Dialog Box. The fields **User Name** and **Unlocking Code** of the Dialog Box shown in Fig. 2 should contain no characters or symbols beyond those appearing in the Reply message exemplified in Fig. 1.

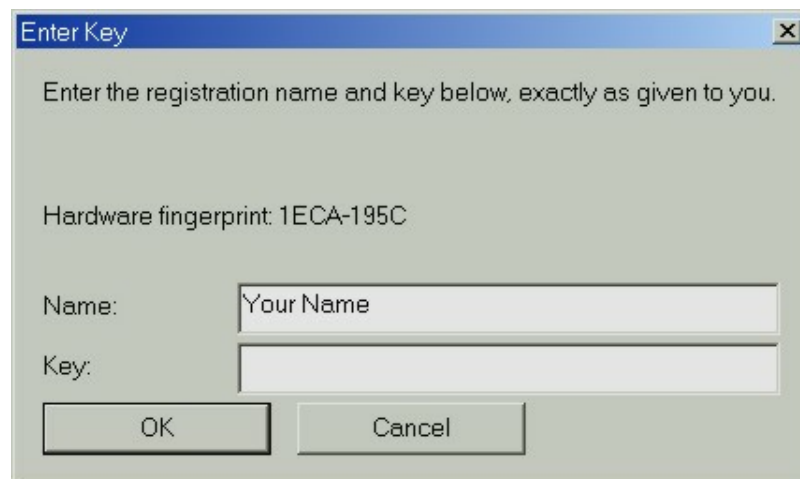
Then click the **OK** button on the Dialog Box. You will be prompted to restart the program. Do this.

2. First, a Message Box named **Key required** will appear informing you that

This program requires a security key. If you have one, select OK to enter it. After entering a valid key, you will not be prompted again.

Click **OK**.

3. The Second Dialog Box named **Enter key** will open with a filled, non-editable line **Hardware fingerprint** and two empty fields: **Name** and **Key**:



**Fig 3. Second Dialog Box**

At this stage, all you have to do is to notice and write down your **Hardware**



**fingerprint** displayed on this Dialog Box. The **Hardware fingerprint**, which is specific to your computer, is to be sent to the developer along with your (User's) **Name**.

Select the **Hardware fingerprint** on the Dialog Box, and copy it to the Clipboard by pressing Ctrl-C keys on your computer's Keyboard.

Then click the **Cancel** button on the Dialog Box.

4. Open once again the e-mail message received from the developer, and write or paste your **Hardware fingerprint** into the corresponding field of the message's text. An example is given in Fig. 4 below:

```
...  
  
Then use the Hardware fingerprint to fill the first  
line  
of the following three lines:  
  
    Hardware fingerprint:1ECA-195C  
  
    Name: Jack Hilton, SlimProject Inc.  
  
    Key: _____  
  
_____  
  
For the moment, leave the last line "Key" blank.  
  
Send the filled Form back to the developer as Reply  
to this message.  
  
...
```

**Fig 4. Filling the second part of the Response message**

The field **Key** in the text of the message should be left blank as shown above in the Figure.

5. Send the message as Reply back to the developer. In response you will get the same message with the last field **Key** (which was left blank above) filled with the required Key string.

```
...  
  
Then use the Hardware fingerprint to fill the first  
line  
of the following three lines:  
  
    Hardware fingerprint:1ECA-195C  
  
    Name: Jack Hilton, SlimProject Inc.  
  
    Key: _____
```

```
Key:00013F-CC051Y-G5ABQW-Z83XQM-KWN0QK-9DGAZ8-  
DD7A1U-WN626F
```

---

Run the Hiron application and enter the Name and the  
Key, supplied  
just above, into the respective fields of the  
appearing Dialog Box.

This will complete your Registration.

...

**Fig 5. Getting the Key to fill the Second  
Dialog Box**

6. Start the program once again. You will first be prompted by the same Message Box **Key required** that

**This program requires a security key....**

7. Click **OK** button. The Dialog Box shown above in Fig. 3 will reappear. Use the **Name** and **Key** data indicated in the text of the last message (see Fig. 5) to fill the **Name** and **Key** fields of the Dialog Box.

Then click the **OK** button on the Dialog Box.

8. After a few seconds, the Message Box named **Key Valid** opens up informing you that

**Key is valid, and has been stored.**

Click **OK**.

9. Double-click the icon **Hiron** (which is on your computer's desktop) once again. In a couple of seconds, the program's Main Window opens up. The delay is normal; it is due to necessary checking, and also caused by starting various protection routines that prevent the running program from being traced, debugged, or modified. During this preparatory process, an image is displayed showing the experimental setup used by Cavendish to measure the gravitational constant.

The program's Main Window is entitled like this:

**Hiron 3.1.7.13 - [Document1]**

---

**NOTE:**

All these steps of the Registration Procedure are performed only once. As soon as the procedure is completed successfully, the program can be started by double-clicking the icon **Hiron** placed on your computer's desktop. Neither Message Boxes nor Dialog Boxes will ever bother you further on, **so long as your Hardware is not modified substantially.**

---

---

### **WARNING!**

**IF YOU MODIFY YOUR HARDWARE SUBSTANTIALLY,  
YOUR CURRENT REGISTRATION KEY WILL BECOME  
INVALID!**

**IF SO, YOU SHALL HAVE TO REGISTER AGAIN!**

---

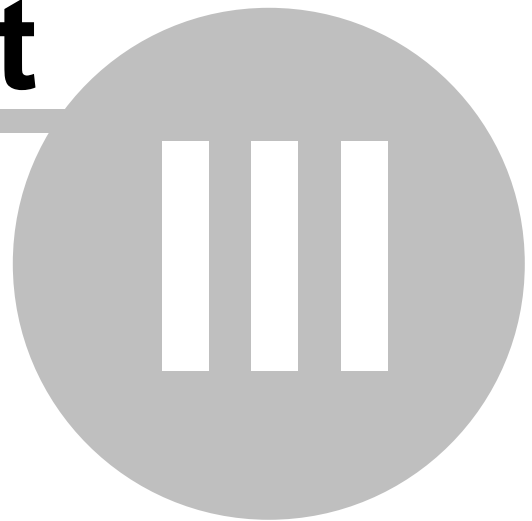
[Key Generation](#)



**Hiron 3.1.7.13**

**Part**

---



## 3 Key Management

Key generation, sending open keys, receiving and placing other persons open keys.

### 3.1 About the Keys

About the Keys

1. The **hidden** (or **private**) key is stored in a specially encrypted format on a removable media alone. It may be a USB Flash Drive, or a USB Hard Drive, or the 3.5" floppy diskette. The **hidden** key does not need any special care. You will never have to worry about it, nor will you pay any particular attention to its contents.

*It is on the known USB Flash Drive that you have to insert when you want to decrypt a message, or sign a message or a file*

—that is all you normally have to keep in mind about the **hidden** key—as well as the password you gave to access it when generating your key pair.

2. The **open** (or **public**) key is quite a different matter. It is stored at two locations: first, on your hard disk where it is accessed by the program each time as needed, and, second, its copy is stored on the same removable media (a USB Flash Drive, or a USB Hard Drive, or the 3.5" floppy diskette) as the **hidden** key. The **open** key is stored in the plain text (ASCII) format, though its contents are essentially binary in nature. For this reason the **open** key is fragile and requires an especially careful handling.

[Sending your open key to others](#)

### 3.2 Key Generation

#### Key Generation

After installing and registering the program, and prior to being able to use its cryptographic functions, you have to generate a coupled pair of **keys** that are needed for the **Hiron** to operate.

---

#### NOTE on the Keys:

- One of these keys, the **open** (or **public**) **key**, is stored in the file named **@opn.bnk** both on the computer's hard drive and (its copy) on a removable media. It serves to **ENCRYPT** documents and e-mail messages.

**THE OPEN (PUBLIC) KEY IS OPEN TO PUBLIC**

**IT MAY BE FREELY AND OPENLY DISTRIBUTED  
THROUGH ALL AVAILABLE CHANNELS  
WITHOUT ANY RESTRICTION**

- The other **Key** is **hidden** (or **secret**, or **private**)—it is stored in the file named **@hdn.bnk**. This file is of vital importance for **DECRYPTING** e-mail messages and documents that have previously been encrypted by **Hiron** using the matching **open** key. The **hidden** key is stored only on a removable media, which can be a USB Flash Drive, or a USB Hard Drive, or a 3.5" floppy diskette. The removable media should be assigned **Drive Letter A:**.

**THE HIDDEN KEY IS SECRET!**

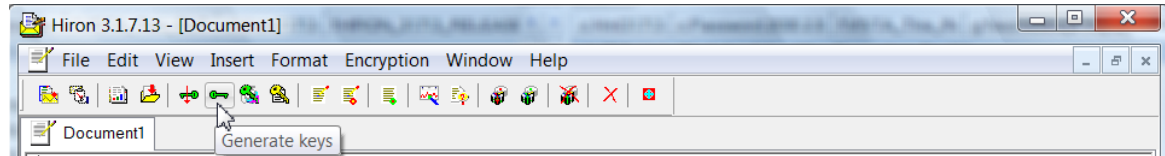
**AVOID EXPOSING IT TO ANY PERSON!**

**YOU WILL NEVER NEED TO GIVE OR SEND  
THE HIDDEN KEY ON TO ANYONE ELSE**

---

To start the **Key Generation Procedure**, follow these steps:

- On the **Special Toolbar** of **Hiron**'s Main Window locate a green icon in the form of a horizontal key (the 6-th from the left). Place the mouse's cursor over the icon and wait a second - a tip, i.e., a tiny window, with a text **Generate keys** will appear right under the cursor).



**Fig 1. Generating user's personalized key pair**

Click on the icon.

- A Message Box opens reminding you to insert a removable media (a formatted 3.5" diskette or a USB Flash Drive marked as A:). There should be about 100 Kilobytes free space on the media. Make sure the media is inserted and click **OK**.

To generate a key pair, an elliptic curve must be supplied to **Hiron**. There are two ways to supply it.

- ❖ The first is to use the default (built-in) elliptic curve;
- ❖ Alternatively, a user-selected, custom-built elliptic curve can be supplied to **Hiron** so as to provide the desired encryption strength to cryptographic algorithms employed by **Hiron**. This kind of elliptic curve must be supplied with its parameters packed into a specific file, which is placed on the same removable media as the one used to store the generated key pair. The file is prepared by the developer and sent to users on their explicit orders. If **Hiron** does not find the file with the reserved name on the prescribed location, it silently uses the default

elliptic curve for key generation purposes.

While each user can employ at will his individually selected elliptic curve, the number of different elliptic curves in use is unlimited: all of them are supported by the current version 3.1.7.13 of **Hiron**.

---

**NOTE:**

A fully qualified elliptic curve is only necessary to produce a matched key pair.

On the other hand, a public key alone is needed for **Hiron** to encrypt a message or document.

---

In what follows, the key pair generation with the default elliptic curve is described.

- Wait a little (normally 10 - 20 seconds depending on the speed of your computer). Then a new information window **SETTING YOUR PASSWORD** appears suggesting that you prepare your **PASSWORD**.
- 

---

**NOTE on the password:**

This password is VERY important. It will be used, first of all, to generate a UNIQUE pair of your own Keys. Besides, it will be required each time when:

- You want to **DECRYPT** any encrypted document or message sent to you;
- You want to **SIGN** (i.e. produce your digital certificate for) any file, message, or document.

The password **SHOULD BE LONG ENOUGH**, not less than 10 characters long, and may contain any printable letter, numeral, space, or any other character available on your computer. The password is CASE SENSITIVE.

**Hiron** will not accept passwords less than 10 characters long (spaces are included).

---

**WARNING!**

**KEEP YOUR PASSWORD WELL!**

**Do not show it to anyone whom you do not trust as much as to yourself!**

**Hiron** employs sophisticated cryptographic algorithms,  
with their strength pushed to their utmost.



**There are no backdoors, no reserved or hidden ways to break texts encrypted by use of this Product!**

**So KEEP WELL IN MIND THAT:**

**IF YOU FORGET, or LOOSE, or DAMAGE  
YOUR PASSWORD or any of your KEY FILES,  
THERE WILL BE NO MEANS TO RECOVER DOCUMENTS  
ENCRYPTED BY Hiron.  
THEY WILL BE LOST IRRETRIEVABLY!**

- 
- On preparing your password, click **OK** on the open information window. The Key generation process resumes. You will have to wait about 30 seconds (more or less of that depending on the speed of your machine). On the **Statusbar** you can watch the progression of the Key Generation process.
  - After that, the program will inform you that the Key generation has been completed successfully; it will show what files have been generated, where they have been placed, and how much time has this taken. The **hidden** key is stored on the removable media in drive A: in the **BINARY FORMAT**, in file **@hdn.bnk** along with its copy **@hdn\_copy.bnk**. The **open** key is stored in the **TEXT (ASCII) FORMAT** at two locations: in file **@opn.bnk** in a special directory on your hard disk, while its copy is located on the same removable media as the hidden key.
  - On completion, **Hiron** is ready to use for encryption purposes.

---

**TIP:**

The **Key Pair** is generated at random. This means that if you repeat the key generation with the same elliptic curve and the same **PASSWORD**, the generated **Keys** will nonetheless be different. In particular, the length of the **Open Key** may slightly vary.

- 
- As the next step, it would be a good practice to check whether the installed Product functions well on your machine.

Proceed as follows: [Documents composing and encryption](#)

### 3.3 Sending your open key

#### Sending your open key

The most reliable way to pass your **open key** over to other persons without corrupting it, is either to send your **open key file as it** is stored on your computer, or a specially prepared file

containing your **open key** along with its description, while placing the **file** in the **ATTACHMENT** to your e-mail message. In what follows, the second way is described, which is the recommended way to exchange **open keys**.

However,

---

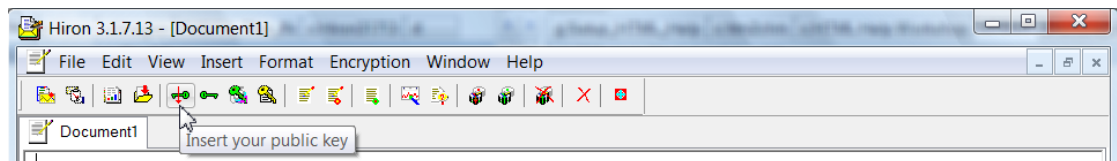
**Technical Note:**

The open key may also be sent as a direct inset into the text of an e-mail message. However, the integrity of the open key transferred in this way **cannot be guaranteed**. The unsafety derives from the fact that various text processors, including word editors built into the most popular e-mail clients, may handle formatting (invisible) characters in different ways, using different symbols to mark ends of lines, for example. These word editors treat the **open key text** as a plain text, trying to preserve only its visible letters, while handling other symbols in the editor's own fashion and reformatting the text as they believe the best. Some word editors remove leading spaces at the beginning of each line, or trailing spaces at the end of line, others do not. Yet **Hiron** expects well defined types of formatting symbols as used while first creating the original key file.

In any event, the **open key file ONE CREATES** to store another person's **open key** must be identical with corresponding open key **file** originally created by the person himself using his own copy of **Hiron**.

Therefore, in order to be sure that the open key sent to you has been saved correctly at the predefined location on your computer, and is ready for use by **Hiron**, follow these steps:

1. Start **Hiron**;
2. Click on the fifth (from the left) icon (horizontal green key with a thin vertical red arrow) on the **Special Toolbar**.



**Fig 1. Inserting your own open key in the active document**

This results in automatically pasting the contents of your **open key** file into the text of the active document.

3. In addition to pasting the **open key** itself, which is encoded and put in the ASCII format, the operation also generates a special description of the open key, such as the user and computer names and the checksum, and pastes it in the active document as well. The document is given the property of being read-only, so it cannot be edited or modified any more.

4. The active document with your open key, generated by Hiron, is to be placed in an attachment to a message and sent over e-mail. To do this, click on the **Send document in attachment** button, and proceed as described in [Sending a message](#) chapter.

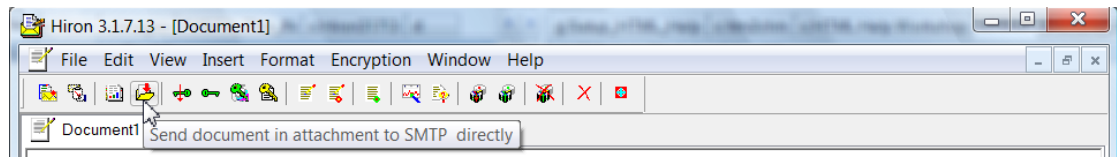


Fig 2. Sending the document in an attachment

5. Optionally, you may want to save the active document for repeated use. This is easily done by pressing **Ctrl+S** keys on your keyboard. The name and location of the saved document will be suggested to you by default, yet you are free in selecting those according to your choice. The saved document becomes the filename extension **.hcf**, and the file is made read-only.

#### [Receiving another person's Public Key](#)

### 3.4 Receiving open key in attachment

#### Receiving an open key file in an attachment

An alternative way of sending to others your own **open key**, is to send your **open key file** as it is. Originally, this file is named **@opn.bnk** and located at a reserved folder in your Windows System directory (Windows\System32\Hml31713). You might want to rename the file giving it a proper name suggesting your ownership, and then send the key file attached to an e-mail message.

On the other hand, on receiving from a person a message with an attachment containing his own **open key file**, i.e., a file having the filename extension **.bnk**, you will only have to give the file an appropriate name as you like, and place the file in the reserved directory at a predefined location on your hard disk (Windows\System32\Hml31713\Public Keys).

To facilitate doing this, **Hiron** offers a built-in utility that automates the process.

Follow these steps:

1. Open the received e-mail message with another person's **open key file** attached to it. You may do this using any e-mail client you usually use to send and read e-mail messages;
2. Save the attached **key file** in any folder you wish;
3. Close the e-mail client;
4. Start **Hiron**;

5. On **Hiron's Special Toolbar** click on the green button called **Store friend's public key** (the 7<sup>th</sup> one from the left and the middle one in the block of three adjacent **Key** icons).

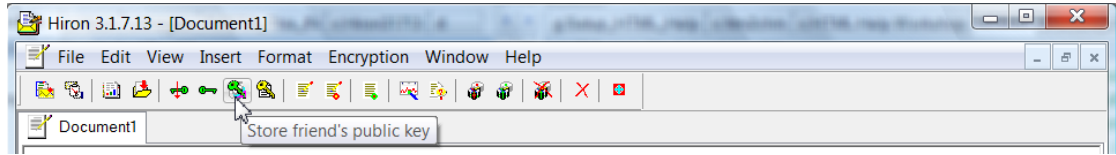


Fig 1. Save the open key as a key file at predefined location

6. A **Message Box Open Public Key File** appears, prompting you that you are going to OPEN the public key received from another person. Click **OK**;
7. The **Open Public Key** File Dialog Box opens letting you select the open key file to store; the **File name** field in the dialog shows the **Key File Name** phrase with filename extension **.bnk** and is highlighted by default;
8. Browse your hard drive and look for the key file **that you have saved an Step 2 above**; select it by giving it a single left-mouse click, and then click **Set key** button;
9. The File Open Dialog closes, and you are immediately taken back to **Hiron's** Main Window. The content of the just opened key file is automatically pasted into the active document. In addition, a Message Box named **Store Public Key on Disk** prompts you that you are going to store this public key as a **key file** in the reserved directory on your disk. You will have to give this **key file** a name you like. Click **OK**;
10. A File Save Dialog opens up at the proper directory, asking you to give a name to the new **key file**. Type in any name you wish.

For example, if you received the **key file** from **James**, just type in **James**, without giving it any extension. Then click the **Save** button on the **Save Public Key** File Dialog window;

11. A Message Box appears, informing you that the new **Public key** has been stored in a file, and displays the name of the stored **Key file**;

Click **OK**. That is all.

**It would be a good idea to check the authenticity of Open Keys you receive.**

**Why is the checking advisable?**

**How to make the verification?**

[Sending your message](#)

### 3.5 Receiving another person's open key

#### Receiving another person's open key

The recommended way to communicate your **open key** to another person, so as to enable the person to send protected messages to you, was described in Ch. [Sending your open key](#). There it was indicated that for the purposes of communication, every open key is encapsulated in message text of a specially designed format containing the sender's user name and computer name as well as the checksum of the original open key. The entire message text is to be saved on disk and transferred in its entirety (for instance, in an attachment to an e-mail message) as a **Hiron**'s protected file (a read-only file having extension **.hcf**). An example of such an open key encapsulated in a message text is:

---

```
The Public Key of "Jack" on "ABCD1234567" is :
=====

G'j1X_cmdztbiFfjqfwbFAR'Xdq-wguEti(kwFD>lvncv<fdxFVMdQDsA
yFtv-q.UTNQMuBmhfIun.keGrTqMrcbGH'hAzQFhkDXqud5cv~Bb00.G
.ddRAIb_j*,ljixMa0vT1cYJah6eYqAu;j<vjFBsmrFvtLkcDpPFPn(wG
OeExQ~grIQRfndL29ToEgmFr*o<q(ZmkfF-DjG!NmOuyV20Zu0.MYAhfg
)OtP1lepvc<(rgOGjMAQQBFcfefR,uddgWviIqCQWcthlTesLXFJ7AzFDb
MXD,tvjB_fNngbrbwvT_jQX5GJvBvhdDO_)cXF*f~MpgvMnXkmrh-gLqxn
1LyjkAZpbqMFJJZGcl,MrLQdGN,qDkYDmyOAnxQncxn?giPjG1lIacLGq
buVMm<mqzslXcvQa(.ZrQXfY*wxCD5-BpPmdtegNrjRdbwYVjQ-qdEmqg
MQrodagXANKtd.`JD5zYgbSv)j0KdjvzFuQFME1`z5XdvfXNchg4mcDcI
X.DYjDgioZq'zcjgbrIyDumqzmiGu0jJZ(czQD1lnbWfozlg1-cjFeFX:
cFqvdfFhkqdrDZzxdgzqzRjh!iQg*ZWl,qbl!~po:d,ZuCfcc*BkInBBG
jucwz>mTGufYRDpeWrz<cc8cchqlM.weNmzpIzrn)DDi,BQMfbXFUBs;x
;rc-Mnne2wduhinQj4vjv~M!i'zbrg`,OX0YBsFJjzEFjOyMfeIkfokDn

=====
[ Checksum:  AC3802EB5520123B38D3C7E8992454EC ]
```

---

It is essential to send the entire block of text contained between the red lines above, without exceptions or modifications. [Sure enough, the user name «Jack», or the computer name «ABCD1234567», or both of them may be changed or replaced by whatever names desired, and this either before dispatching the message or afterwards.]

On receiving a message containing such an encapsulated **open key**, you will have to

- extract the contents of the key,
- place it into a proper **Key file** at a predefined location on your hard disk, and
- verify that the newly saved key file is identical to the one stored on the computer disk of the sender.

To perform those operations without error, **Hiron** offers a built-in utility that automates the process.

Suppose that you have received an e-mail message with an attachment containing the file named «Jack-ABCD1234567.hcf».

Follow these steps:

1. Open the received e-mail message with its attachment. You may use any e-mail client that you usually use to send and read e-mail messages.
2. Save the file in attachment in a folder on your hard drive. [Optionally, you may view the contents of the file (in any way you know), then copy the entire contents to Clipboard, and finally paste the copied contents into a blank active document of **Hiron** application.]
3. Start **Hiron** application.
4. On the **Special Toolbar** of **Hiron** application, click on the yellow button called **Save key file from TEXT** (the 8-th one from the left and the last one in the block of four adjacent **Key** icons).

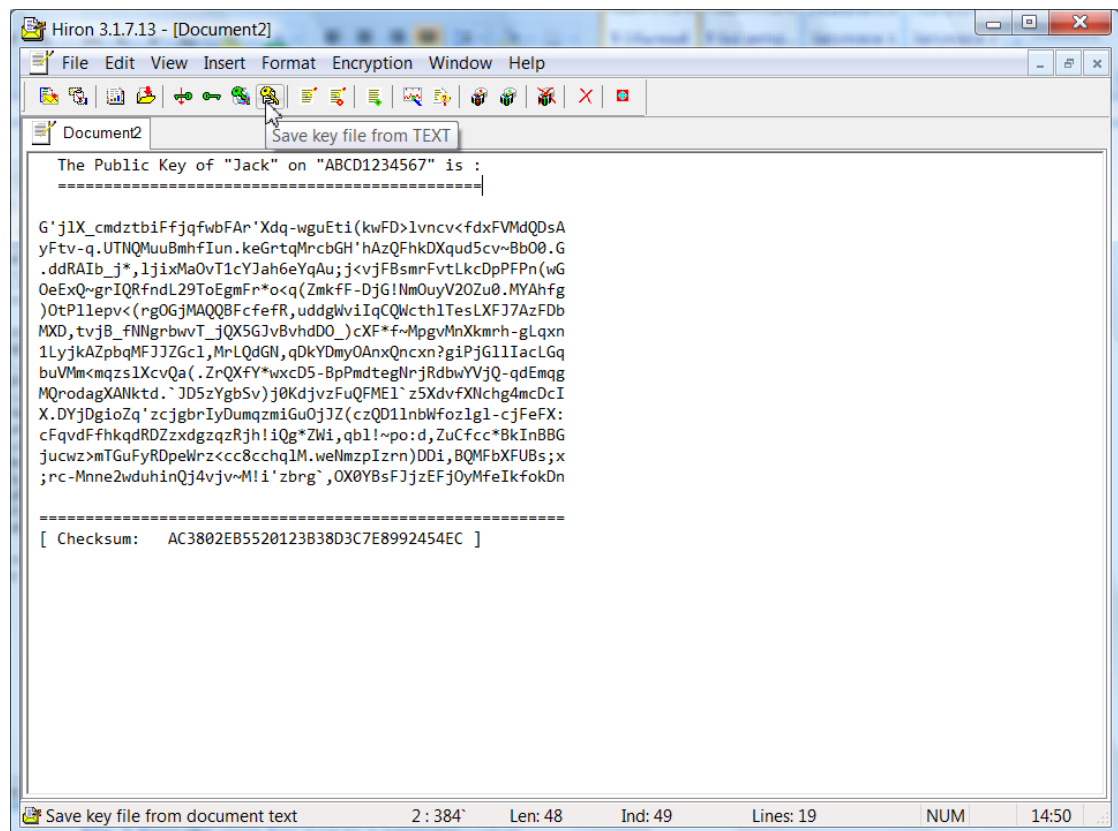


Fig 1. Save the open key text to a proper location

5. A **Message Box** appears prompting you that you are going to store the public key on you hard disk. Click **OK**;
6. The **Save Public Key** File Dialog Box opens letting you give the name to the new key file; the **File name** field in the dialog is highlighted by default;
7. **Without touching any other key on the keyboard**, immediately type in a name for the new **Key file** (without extension).
8. For example, if you received the **Key** from your friend named **James**, just type in **James**, without giving it any extension. Then click the **Save** button on the **Save Public Key** File Dialog window;

- 
9. A Message Box appears informing you that the new key has been stored in a file, displays the name of the new **Key file**, and informs you that the checksum has been verified and found correct;
- 

### **WARNING!**

**If the checksum is not found correct, the open key has not been stored on your disk properly. Communicate with the sender and ask him to send you his open key once again by placing it in the attachment to his e-mail message.**

[Receiving another person's Open Key in a file attached to e-mail message](#)

---

10. Click **OK**. That is all.

**It would be a good idea to check the authenticity of Open Keys you receive.**

**Why is the checking advisable?**

**How to make the verification?**

[Sending your message](#)





**Hiron 3.1.7.13**

**Part**

---



**IV**

## 4 Encrypting documents

Document composing, encrypting documents in Hiron, information displayed on statusbar.

### 4.1 Typing in a text to the document

Typing in a text to the document

Begin typing in a desired text into the active document window. For example, you may paste your **open key** into the blank document's window by clicking the fifth (from the left) icon (horizontal green key with a thin vertical red arrow) on the **Special Toolbar**.

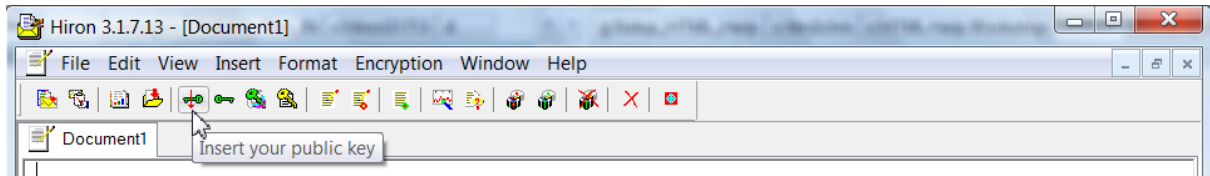


Fig 1. Inserting your public key

You may apply any text formatting tools that are built into the Editor of **Hiron**. This is the so-called «Rich Text Format» (RTF) Editor. It prepares and stores documents in the RTF format, which is widely supported by Word processors, such as MS Word, and e-mail clients, such as Microsoft's Outlook Express.

When you have finished typing in your text, save the document on disk. To do this, click Ctrl+S keys on your keyboard. You will be prompted for the filename and location.

---

#### NOTE:

Files stored by **Hiron** may have either an extension **.hcf** (for files encrypted by means of Hiron), or the standard extension **.rtf** (for unencrypted files).

---

#### [Encrypting the contents of the active document](#)

### 4.2 Documents composing and encryption

#### Documents composing and encryption

To compose a document, first press the **SPACE** bar on your keyboard. This activates the document's window.

**NOTE on activating document windows:**

Each time you create a new document, or open an existing document from a file stored on disk, you have to **ACTIVATE** the new window by pressing the SPACE bar. If you forget or omit this, the first character typed in to the document will be lost. Retype it if needed.

Typing in a text to the document

### 4.3 Encrypting the contents of the active document

#### Encrypting the contents of an active document

To encrypt the text of an active document, keeping all of its format settings, click the **Encrypt** button on the **Special Toolbar** (the 9-th one from the left on the Toolbar—a white envelope icon).

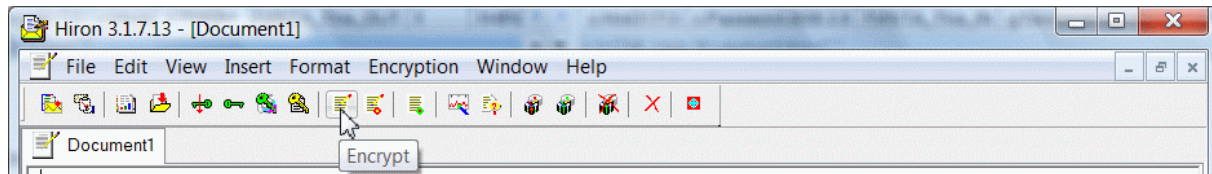


Fig. 1 Encrypt an active document

Alternatively, in order to **encrypt and sign** the active document, click the **Encrypt and sign** button on the same Toolbar. This will produce your electronic signature and embed it in the encrypted document so as to enable the recipient to verify the authenticity of the encrypted text he received.

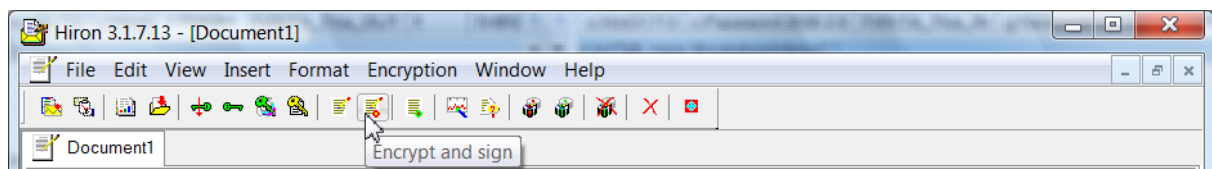


Fig. 2 Encrypt and sign an active document

A Message Box will appear prompting you to set a **PUBLIC** key to encrypt with. Normally, you will have many different public keys sent on to you by your recipients; all of these public keys are stored at a special location on your hard disk—in the folder named «Windows\System32\Hml31713\Public Keys». This folder is opened automatically each time the program has to look for a public key.

**To encrypt a document, you will have to select the Public (OPEN)**

key belonging to the recipient **TO WHOM** you are going to **SEND** the encrypted document.

On the open Message Box click **OK**—a File Open Dialog named «Set Public Key for Encryption» will display the folder mentioned above. Left-click on the desired public key name, then left-click the **Set key** button; optionally, to use your own public key, click the **Default key** button. A new Message Box will inform you about the public key selected for encryption.

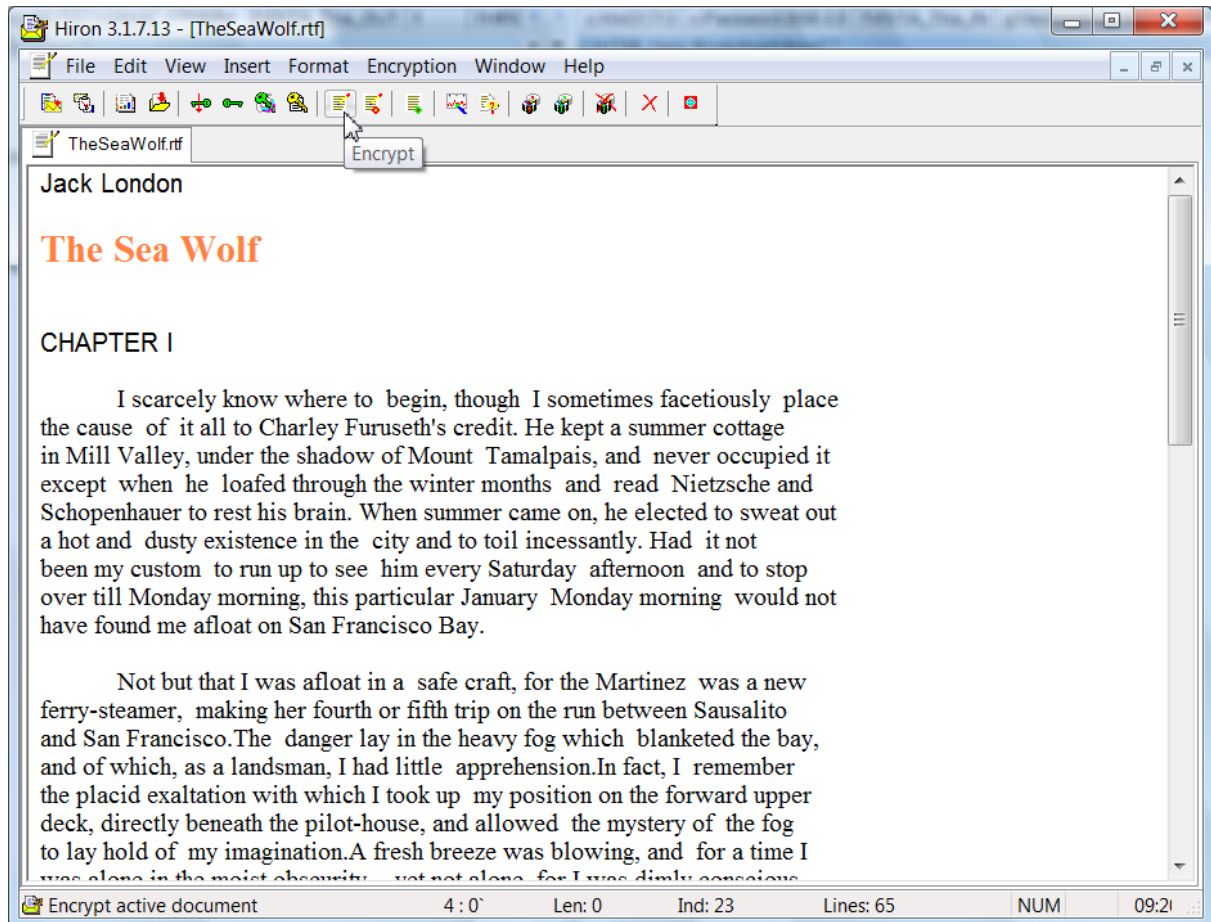


Fig 3. Encrypting active document with rich text formats

Click **OK**. The encryption process starts. It may require some time depending on the size of the document as well as the speed of your machine. On the **Statusbar** you can watch the progress of the encryption process.

When the encryption ends, the plain text in the active document is automatically replaced by its encrypted form. In this state, the document is locked—the Editor prohibits any further changes to the encrypted text.

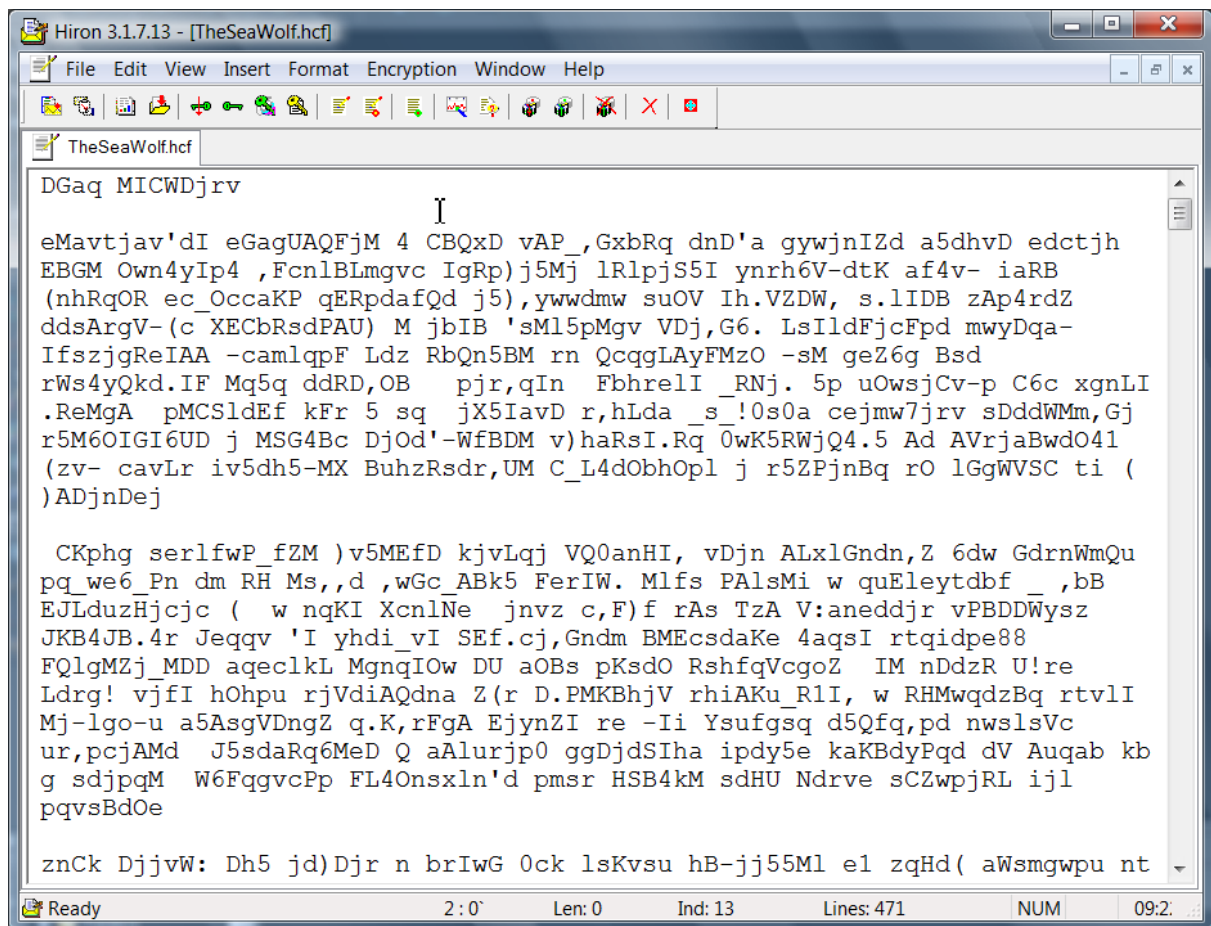


Fig 4. Encrypted contents of the previous document on Fig 3.  
Note the filename extension **.hcf** given to the encrypted document

You may either save the encrypted text on disk, or you may want to send the encrypted document on to the owner of the public key used for encryption.

To save the encrypted document, click **Ctrl+S** on your keyboard. A File Save Dialog box will open suggesting you a name for the encrypted document to store. There is just one available filename extension **.hcf**, which is used for all documents encrypted by means of **Hiron**. By default, the File Save Dialog opens the folder where a file was saved last time.

#### [Document decryption](#)

## 4.4 Information displayed on the Statusbar

Information displayed on the Statusbar

The following information is displayed on the **Statusbar** of the program's Main Window (from the left to the right):

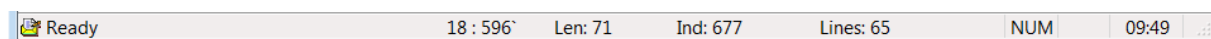


Fig. 1 Information displayed on the Statusbar

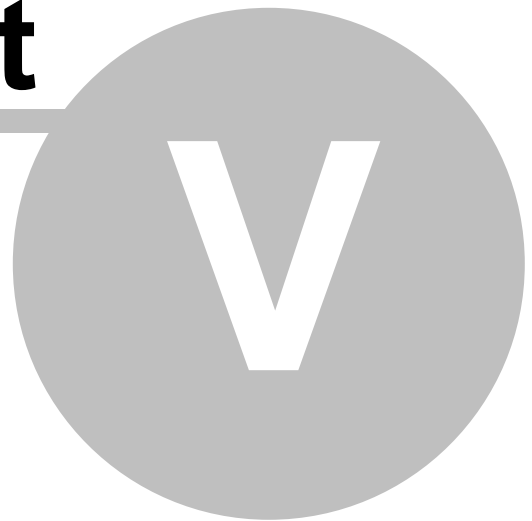
- The **Ready** message, informing you that the program is running and ready to be used;
- **THE CURRENT CURSOR POSITION** within the active document window: **18:596** (some distance away to the right from the **Ready** text). The position is displayed as two adjacent numbers separated from each other by a colon:
  - The number **18** on the left of the colon indicates the line number for the line where the cursor is currently placed;
  - The number **596** on the right of the colon indicates the distance of the cursor from the left edge of the active document's window (in **pixels**). If the cursor is currently placed outside the visible part of the text, the number on the right of the colon is replaced by the word **out**;
- **THE LENGTH OF THE LINE** where the cursor is currently positioned: **Len:71** (measured in characters);
- **THE INDEX OF THE LINE CONTAINING THE CURSOR: Ind:677.**  
This is the total number of characters contained in all preceding lines of the active document, starting with the first one but excluding the line where the cursor is currently positioned; spaces are included in the number of characters, whereas empty lines are excluded;
- **THE TOTAL NUMBER OF LINES** the active document contains: **Lines:65.**
- The **NUMLOCK** indicator: **NUM**;
- **THE CURRENT TIME: 09:39.**

[Uninstall Hiron](#)

**Hiron 3.1.7.13**

**Part**

---



## 5 Sending a message

Sending messages, encrypted or not, by means of Hiron.

### 5.1 Sending a message, encrypted or not

Sending a message, encrypted or not

Once a message is composed as a document of **Hiron**, it can be sent as an e-mail message right from the program's **Main Window**.

---

#### NOTE:

You may want to encrypt the composed document and/or store it on disk before dispatching it by e-mail.

---

A document, encrypted or not, can be sent via e-mail from within **Hiron directly**—either as a plain message (the text of the document is thereby inserted in the text field of the message), or as an attachment to an e-mail message (the text of the document is inserted into the attachment to the e-mail message). Both these operations are accomplished by a single left-mouse click on an appropriate button on the **Special Toolbar**. There are two ways to perform these.

First, as an older way preserved in the current version of **Hiron**, dispatching e-mail messages by means of Outlook Express is still enabled. Yet it is not the recommended way to send e-mail messages from **Hiron**. The latter has now a built-in utility named MailDispatcher, which is a special unit with advanced functionality designed to provide an independent, fast and secure way of sending e-mail messages. In particular, when using MailDispatcher:

1. There is no need for any external e-mail client installed on the user's machine;
2. There is no need to create user's accounts in order to be able to send e-mail messages;
3. There is no need for finding out the mail server IP addresses, neither POP3 nor SMTP, prior to sending the e-mail message: contrary to nearly all other e-mail clients, the servers' IP addresses are determined and resolved by MailDispatcher automatically from the e-mail addresses given in by the user;
4. There is a block imposed on every superfluous private information included into the body of an e-mail message (which is not the case with every popular e-mail client);
5. There is a possibility of bypassing the sender's SMTP server by sending e-mail messages directly from the sender's computer to the receiver's SMTP server (which is not the case with every popular e-mail client);
6. There is a logging of the (usually hidden) answer-response communication between e-mail servers, which underlies every process of dispatching an e-mail message, the logging being enabled for the purposes of reviewing and checking (which is not the case



with every popular e-mail client).

To send a document, encrypted or not, by e-mail in the first way—i.e., by means of Outlook Express,—by placing its contents into your message **directly**:

1. Make sure Outlook Express is installed on your machine, and user's account is created;
2. Click the icon 'Send mail as message' (a **YELLOW** envelope) on the Main Window's **Toolbar** (the first one on the left edge of the **Special Toolbar**)

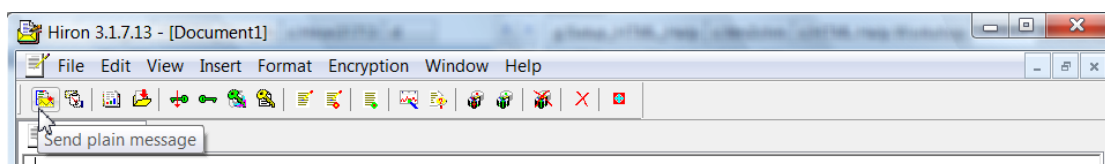


Fig 1. Sending an e-mail message by means of Outlook Express

3. The standard Outlook Express' Message window opens up with your default e-mail address typed into the field **From:**, and the contents of the document (composed in the **Hiron**) inserted into the message's text area. You will have to fill in the fields **To:** and **Subject:**, and attach a file or files (if there are some) to the message;
4. Make sure that you are connected to the Internet and then dispatch the prepared message by clicking the **Send** button on the **Outlook Express' Toolbar**. (If you press the **Send** button while not connected to the Internet, the Windows Operating System will prompt you to connect.);
5. An information window will open, displaying the progress of mail sending process. Then the Message window will close, and you will be taken back to **Hiron's** Main Window.

---

### IMPORTANT NOTE:

Please be advised that within the framework of the fight against the spam, some mail servers employ advanced anti-spam software. If so, the installed SpamCheckers, AntiAbuseCheckers, and SpamAssassins scan texts of incoming and outgoing email messages and automatically evaluate the Spam Score of every message according to their own built-in algorithms. It is possible that if you place your encoded document right into the message's text, it will be automatically estimated to be a spam and then **immediately deleted by the server without even notifying you**.

To avoid such an unexpected annoyance, it might be more appropriate to send your encoded document by placing it into the **ATTACHMENT** to your email message as described below. (Attachments are currently not scanned by SpamCheckers.)

---

To send a document, encrypted or not, by e-mail in the first way—i.e., by means of Outlook Express,—by placing its contents in the **ATTACHMENT** to your message, rather than into the message's text:

1. Click the icon **Send mail in attachment** (the second one from the left) on the Main Window's **Special Toolbar**.

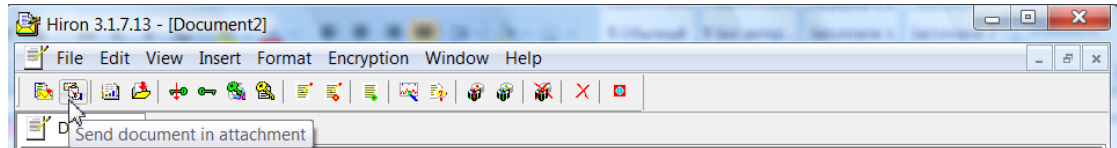


Fig 2. Sending the text of a document in an attachment by means of Outlook Express

2. Then follow the steps as described above in this section.

To send a document, encrypted or not, by e-mail by means of MailDispatcher, by placing its contents into your message **directly**:

1. Click the icon 'Send mail as message' (a **YELLOW** envelope) on the Main Window's **Toolbar** (the first one on the left edge of the **Special Toolbar**):

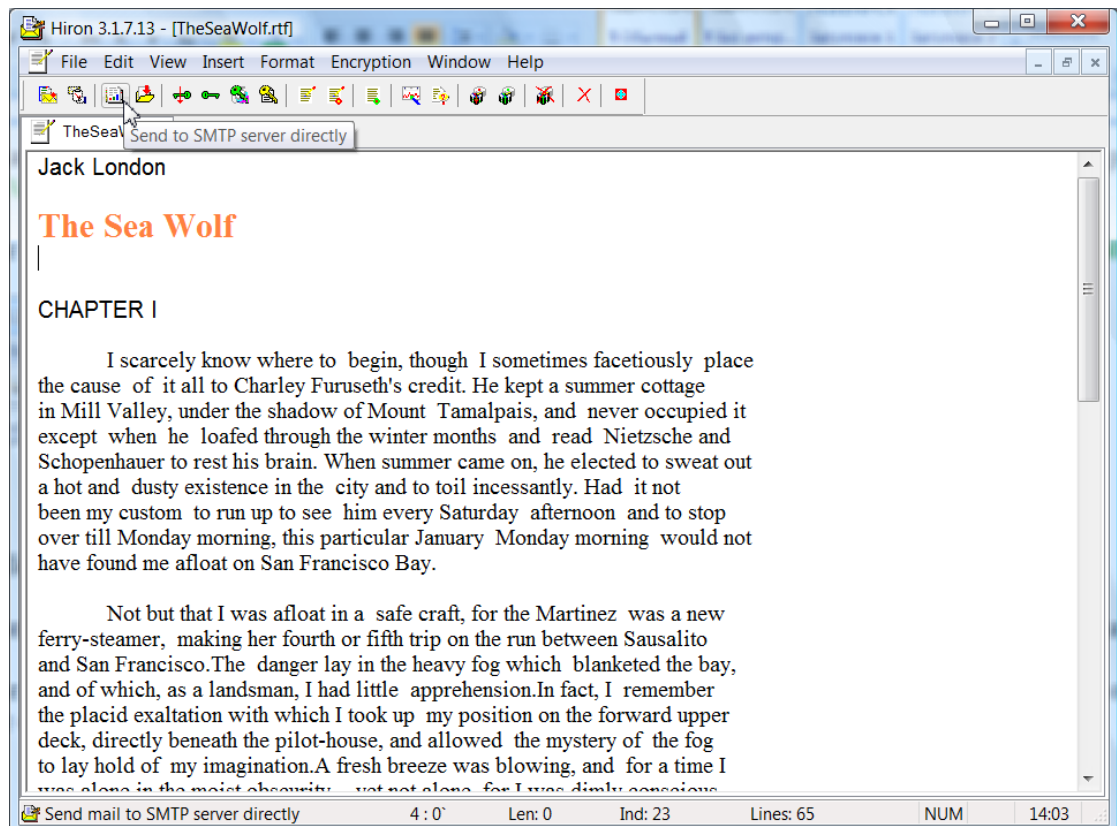


Fig 3. Sending e-mail message by means of MailDispatcher

This results in showing up the **MailDispatcher Dialog Box**:

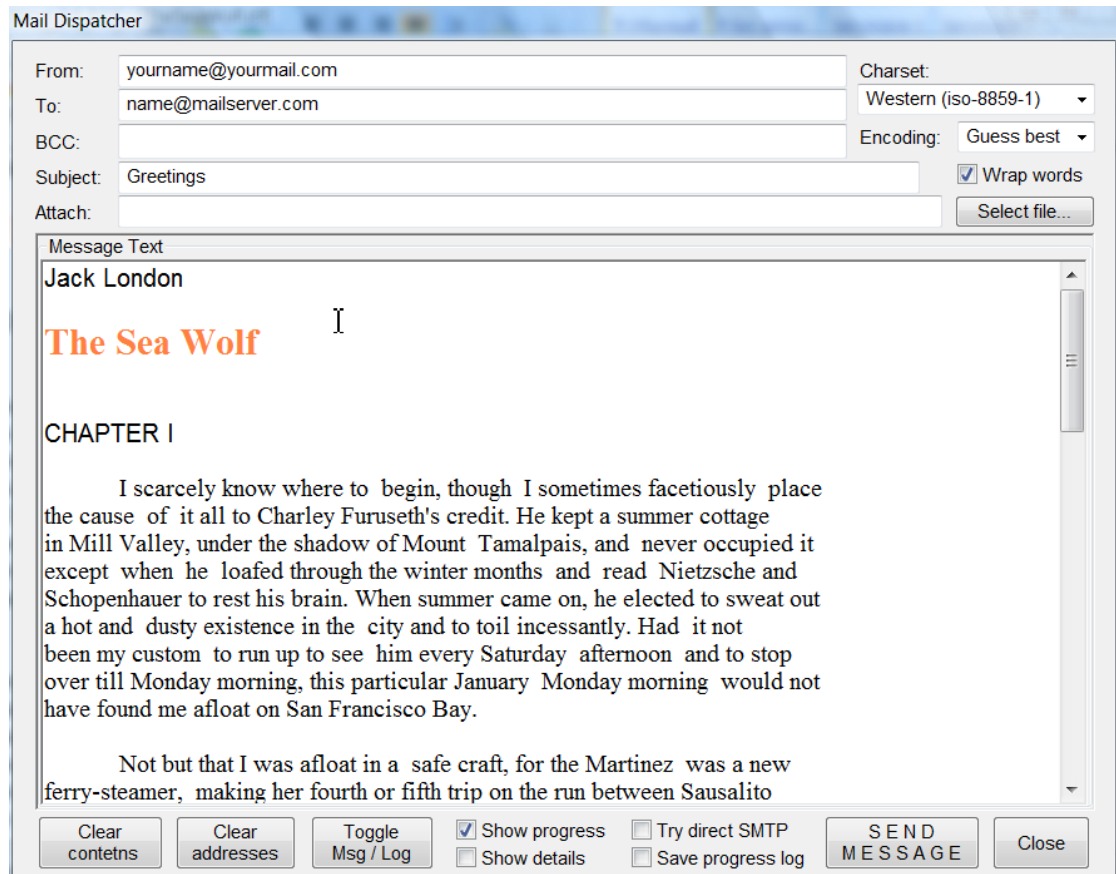


Fig 4. MailDispatcher's Dialog Box

The text composed in **Hiron**'s active document, either encrypted or not, is automatically inserted—with all its formatting features—into the **Message Text** window of MailDispatcher. You will have to type in the e-mail addresses (eventually, the BCC address—Blind Carbon Copy address), and subject, to select the desired charset and encoding or leave the default ones,—and finally click on **SEND MESSAGE** button.

That is all. There is no need for finding out the mail server IP addresses, neither POP3 nor SMTP: contrary to nearly all other e-mail clients, the servers' IP addresses are determined and resolved by MailDispatcher automatically from the e-mail addresses given in by the user.

2. On clicking **SEND MESSAGE** button, a new window shows up displaying the communication messages exchanged between mail servers while negotiating the e-mail

send-receive process. If you want to see every detail of the latter, check **Show details** radio-box prior to clicking on **SEND MESSAGE** button.

3. If the radio-box **Try direct SMTP** is unchecked, as is shown on Fig 4, the e-mail message is first sent to the SMTP server determined by Sender's e-mail address; the server then takes over the task of transferring the message further to the Receiver's POP3 server.
4. If, on the other hand, you check the radio-box **Try direct SMTP**, MailDispatcher will try to send your e-mail message **directly** from your computer to the Receiver's POP3 server, thus bypassing the SMTP server determined by Sender's e-mail address. **Note, however, that many mail servers, especially those maintained by big companies like Hotmail or Gmail, do not accept e-mail messages sent from personal computers.**
5. If you check the box **Save progress log**, the progress log will be saved on your hard disk C:.
6. A file may be attached to your message at will.
7. Note, however, that the message's formatting features will be lost when sending it this way. The message will be sent in the plain-text format. This is due to the fact that standard e-mail clients do not support direct reading of RTF-formatted texts. Supplying to such an e-mail client a text in the RTF format would result in displaying unreadable sequences of special symbols.

In order to send an e-mail message with full support of its formats, the formatted text should be placed in the attachment to your e-mail message.

---

To send a document, encrypted or not, by e-mail by means of MailDispatcher, by placing its contents in the attachment to your message:

1. Click on **Send document in attachment to SMTP directly** button:

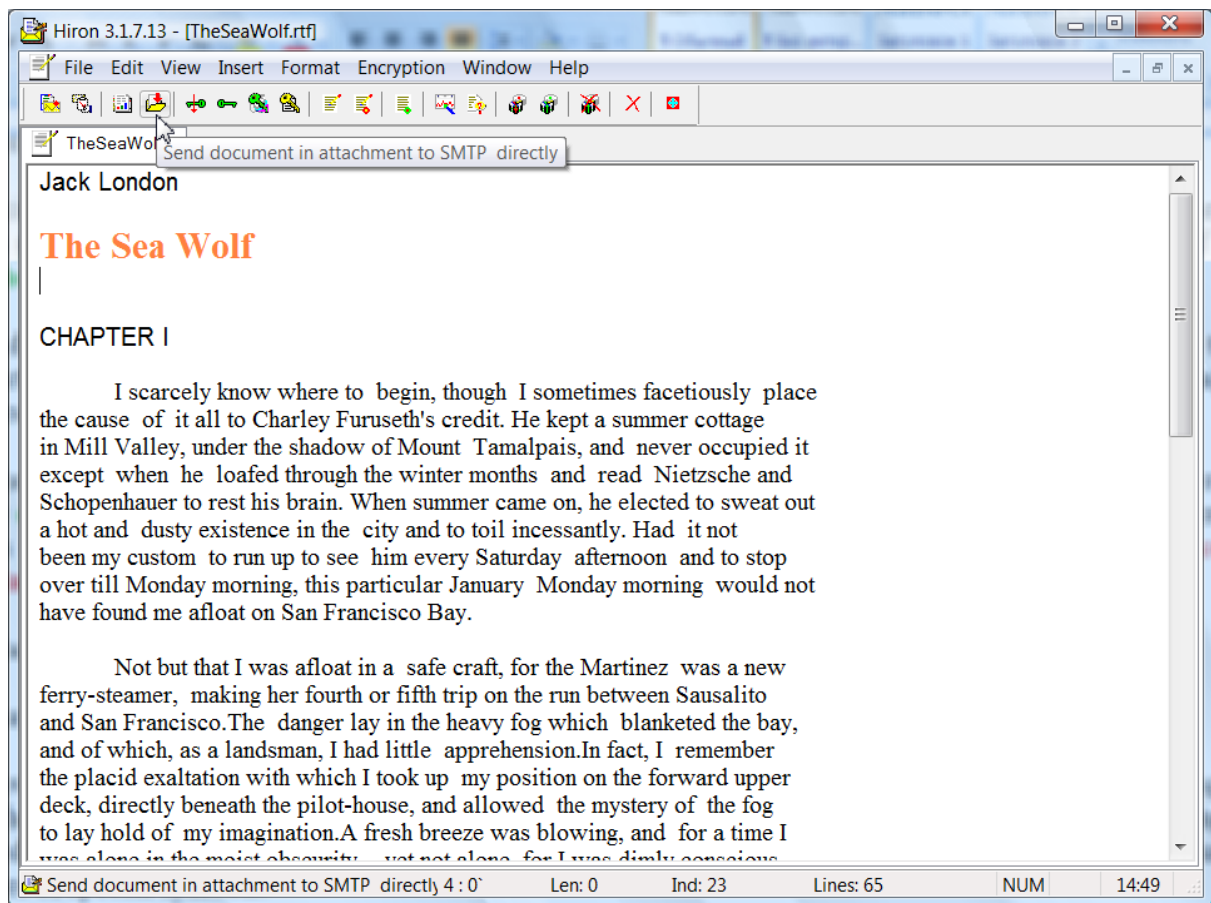


Fig 5. Sending a document by MailDispatcher in attachment

**MailDispatcher's Dialog Box** will open; the text of **Hiron**'s active document is thereby automatically compressed, with all of its formatting features preserved, and placed in the attachment to the outgoing e-mail message as a file with randomly selected name:

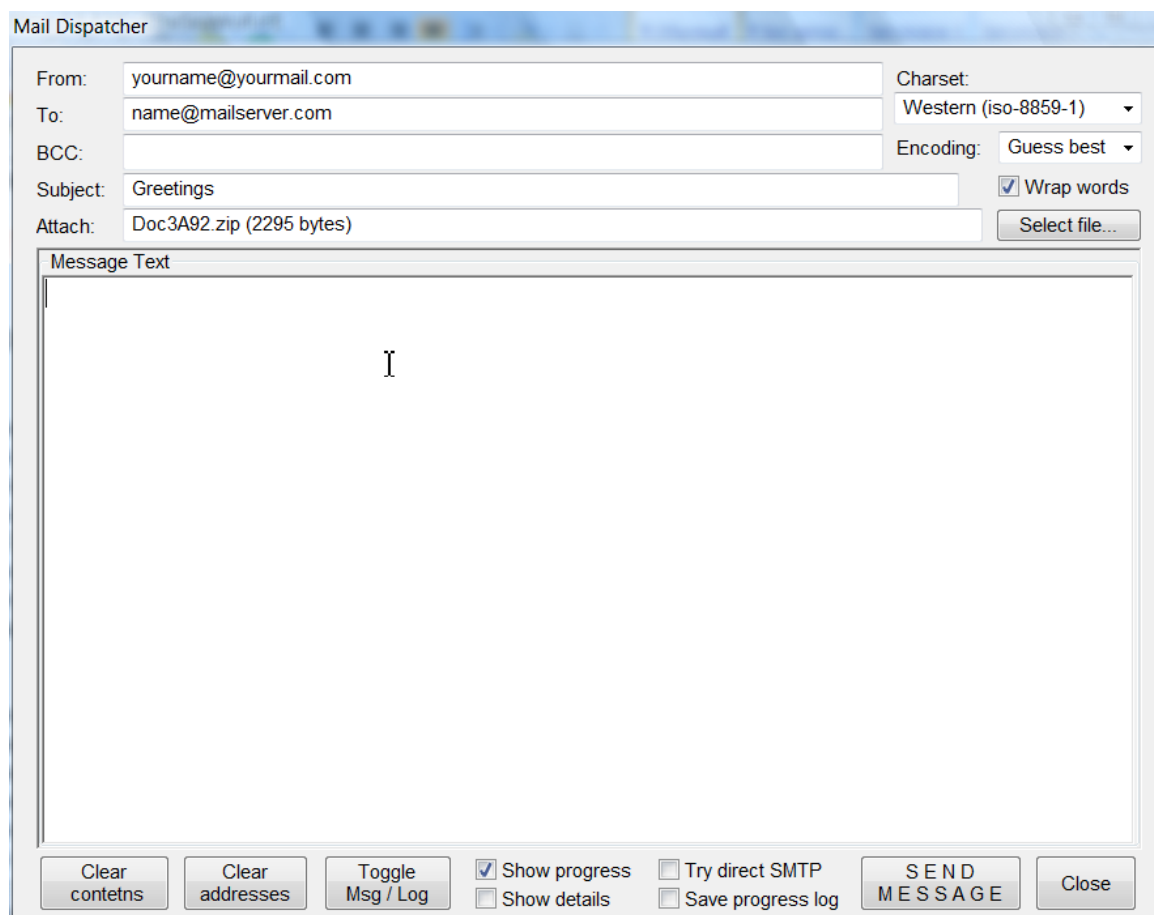


Fig 6. The document has been compressed, given a random name, and put in the attachment

You may type in additional text in the Message Text window, add e-mail addresses and select other settings from within the ones offered by MailDispatcher. Finally, click on **SEND MESSAGE** button to dispatch the message.

[Receiving an encrypted e-mail message](#)

**Hiron 3.1.7.13**

**Part**

---



**VI**

## 6 Encrypting files

Encrypting disk files

### 6.1 Encrypting disk files

Encrypting disk files

To **ENCRYPT** a **file stored on disk**, follow these steps:

1. Start **Hiron** (by double-clicking its icon on your computer's desktop);
2. On the **Special Toolbar** of the program's Main Window click the icon **Encrypt a file stored on disk** (the 14-th from the left edge of the Toolbar)

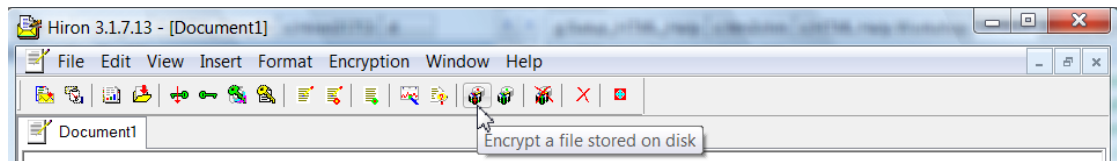


Fig 1. Encrypt a file stored on disk

3. First, a File Open Dialog, named «Select File to Encrypt» opens, allowing you to browse for the desired file to encrypt. Select the file and click **Open** button.
4. A Message Box appears prompting you to set the **PUBLIC KEY** for encryption. Normally you will select:
  - Either your own **OPEN Key** (if you intend to encrypt a file for the purposes of your own use), or
  - The **PUBLIC KEY** of the recipient to whom you are going to send the encrypted file.

Click **OK**;

5. The File Open Dialog, entitled «Set Public Key for Encryption», is displayed offering you a choice of **public keys** installed on your computer; select one of them and click the **Set key** button (clicking **Default key** button selects your own open key);
6. A new Message Box opens up displaying the next action the program will start along with information about the selected file and public key; you may click **OK** to continue, or **CANCEL** to stop operation. Click **OK**;

---

#### NOTE:

The name of a file encrypted by means of «Hiron» is made up by prepending **E\_** at the beginning of the name of the original file, and also appending the filename extension **.D**.



For example, if you encrypt the file named **MyFile.txt**, the encrypted file will get the name **E\_MyFile.txt.D**.

---

**WARNING!**

**THE CONTENTS OF THE ORIGINAL FILE WILL NOT BE  
MODIFIED.**

**THE PROGRAM CREATES NEW ENCRYPTED FILE**

---

7. The encryption operation will begin; its progress is displayed on the **Statusbar**. The operation may take a few dozens of seconds. On completion, the program will inform you about the success of encryption and show the full name (including its path name) given to the encrypted file. Click **OK**;
8. New Message Box will inquire whether you wish to send the encrypted file by e-mail as an attachment to a message. Click **YES** or **NO** as you like.
9. If you click **YES**, the dispatch operation begins; for more details see Section IX [Sending your e-mail message](#) .

[Decrypting disk files](#)



**Hiron 3.1.7.13**

**Part**

---

**VII**

## 7 Decrypting documents

Decrypting documents in Hiron

### 7.1 Document decryption

#### Document decryption

To decrypt the text in the active document, click on the **Decrypt** button located on the **Special Toolbar** just on the right of the **Encrypt** button (a white envelope with a GREEN seal).

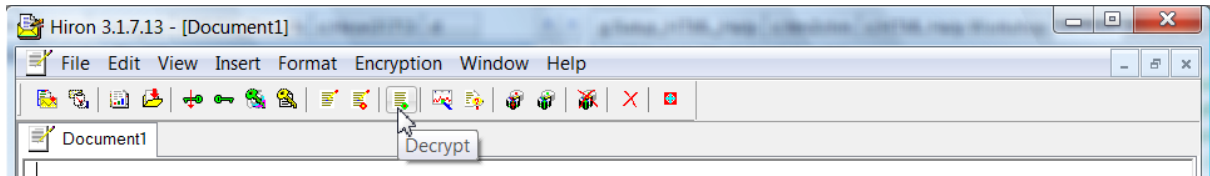


Fig 1. Decrypting active document

First of all you will be prompted to make sure that the media with your **SECRET (HIDDEN) KEY** is inserted into your computer, and it is assigned the appropriate drive letter (A:).

---

#### NOTES:

If you start the decryption process without having a media with the **HIDDEN KEY** inserted in drive A:, OR THE KEY IS NOT CORRECT, the program will prompt you about that, then the operation will be cancelled.

---

**MAKE SURE THE MEDIA (USB FLASH DRIVE)  
WITH YOUR CORRECT HIDDEN KEY  
IS PROPERLY INSERTED AND ASSIGNED DRIVE LETTER A: !**

Then click **OK**. After about 10 seconds a password window opens. Enter your password twice and click **OK**.

Some time later on, when the text decryption process is finished, the encrypted contents of the active document will be replaced with its decrypted form ready to read it.

#### [Key management](#)

### 7.2 Receiving an encrypted message

Receiving an encrypted message

You may receive messages encrypted by means of **Hiron** using **any** e-mail client, preferably

### Microsoft's Outlook Express.

To **DECRYPT** a message, follow these steps:

1. In the text of the received message, locate the encrypted block, **SELECT** it, and then copy the block to Clipboard by pressing **Ctrl+C** keys on your keyboard;
2. Open the **Hiron** (by double-clicking its icon on your computer's desktop);
3. Paste Clipboard's contents into the blank new document's open window by pressing **Ctrl+V** on your keyboard;
4. Decrypt the contents of the document by clicking the **Decrypt** button located on the **Special Toolbar** (a WHITE envelope with a **GREEN** seal, or the 11<sup>th</sup> one from the left):

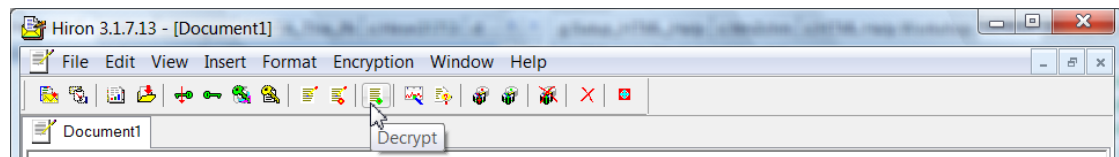


Fig 1. Decrypting a document

Refer to Section " [Document decryption](#) " for more detail.

### [Signing disk files](#)



**Hiron 3.1.7.13**

**Part**



## 8 Decrypting files

Decrypting disk files

### 8.1 Decrypting disk files

Decrypting disk files

To **DECRYPT** a **file stored on disk**, which was previously encrypted by use of **Hiron**, follow these steps:

1. Start **Hiron** (by double-clicking its icon on your computer's desktop);
2. On the **Special Toolbar** of the program's Main Window click the icon **Decrypt a file on disk** (the 15-th from the left edge of the Toolbar)

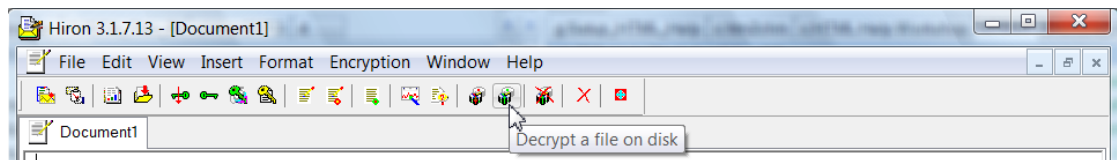


Fig 1. Decrypting a file stored on disk

1. First, a Reminder Message Box appears asking you whether the media (USB Flash Drive) with your **HIDDEN KEY** is in drive **A:**. Insert the media (USB Flash Drive) if it is not yet there. Click **YES**;
2. A File Open Dialog opens suggesting that you select a **file to decrypt**. Select the file and click the **Open** button;
3. A new Message Box opens up displaying the next action the program will start along with information about the selected file; you may click **YES** to continue, or **CANCEL** to stop operation. Click **YES**;
4. After a few seconds the **Password Dialog Box** will invite you to enter your password. Enter it twice and click **OK**;
5. File Decryption Process starts; its progress is displayed on the **Statusbar**.
6. After completion, the program will inform you about success and the name given to the **DECRYPTED** file. The name is obtained by removing the extension **.D** at the end of the encrypted file's name as well as deleting the first letter **E** at its beginning.

### **WARNING!**

**THE CONTENTS OF THE ORIGINAL ENCRYPTED FILE**



**WILL BE OVERWRITTEN AUTOMATICALLY!**

**THE PROGRAM DOES NOT CREATE BACKUP COPIES  
OF ORIGINAL FILES TO DECRYPT!**

**HOWEVER, BEFORE OVERWRITING, THE PROGRAM CHECKS  
WHETHER THE FILE WAS DECRYPTED CORRECTLY.**

---

7. Click **OK**. That is all.

[Information displayed on the Statusbar.](#)



**Hiron 3.1.7.13**

**Part**

---



**IX**

## 9 Signing disk files

Signing disk files digitally, and verifying digital signatures in Hiron.

### 9.1 Signing disk files

Signing disk files

To **SIGN** a disk file, that is, to produce your own **personal digital certification** called the **SIGNATURE** of the file, follow these steps:

1. Start the **Hiron** (by double-clicking its icon on your computer's desktop);
2. Click the **Generate digital signature** icon on the Special **Special Toolbar** (the 12<sup>th</sup> one from the left edge of the Toolbar, on the right of a WHITE sheet icon with text and a GREEN seal)

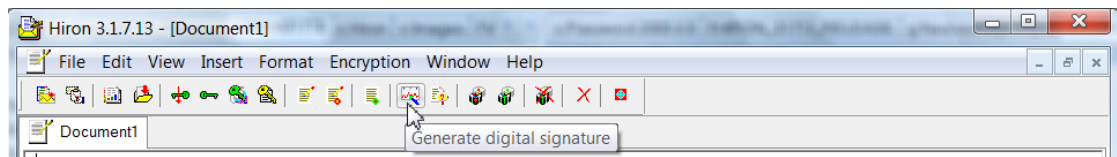


Fig 1. Generating your own digital signature for a disk file

3. A Message Box **Choose file to sign** will open up prompting you to select a disk file you wish to sign.  
Click **OK**;
4. The File Open Dialog appears letting you select a file to sign. Select a file and click **OK**;
5. A new Message Box opens up displaying the next action of the program along with information about the selected file; you may click **OK** to continue, or **CANCEL** to stop operation;
6. If you click **OK**, a new Message Box will prompt you to insert the media (i.e., a USB Flash Drive) with your **Secret key**; make sure the media is inserted and click **OK**;
7. You will then be asked to enter your **PASSWORD twice**; do this and click **OK**;
8. The signing operation begins; its progress is displayed on the **Statusbar**. The operation may take a dozen of seconds;
9. After completing, the program will inform you about the success, while the contents of the active document will be automatically **REPLACED** by the digital signature you have just produced;
10. The digital signature of the selected file is at the same time saved on your disk in the same

folder as the one containing the selected file. The name of the signature file is made up by appending to the name of the file to sign the extension **.signature**.

For example, if you sign the file named **Myfile.txt**, the name of its signature file will be **Myfile.txt.signature**.

### Verifying disk files

## 9.2 Verifying disk file's signatures

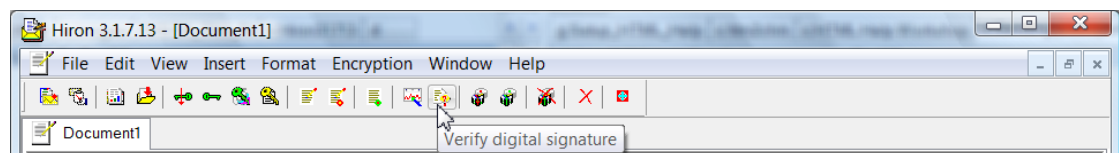
### Verifying disk file's signatures

You will have to **VERIFY** the digital signature of a file that was sent or given to you by someone else along with the file's digital signature, which was produced by that person to certify the file's authenticity.

**TO VERIFY THE SIGNATURE PRODUCED BY ANOTHER PERSON  
YOU SHOULD HAVE THE PERSON'S OPEN KEY  
INSTALLED ON YOUR COMPUTER**

To **VERIFY** a disk file's **SIGNATURE**, follow these steps:

1. Place the file you are going to verify, **along with its digital signature file**, in **one and the same** folder on your hard disk;
2. Start **Hiron** (by double-clicking its icon on your computer's desktop);
3. Click the **Verify digital signature** icon on the **Toolbar** (the 13<sup>th</sup> one from the left edge of the **Special Toolbar**)



**Fig 1. Verifying digital signature of a disk file**

4. A Message Box **Select file to check signature of** will open up prompting you to select a disk file you wish to verify the signature of. Click **OK**;
5. The File Open Dialog appears letting you select a file to verify. Select a file and click **Open**.

**Be sure to select the file you want to verify,  
NOT ITS DIGITAL SIGNATURE FILE  
HAVING THE EXTENSION .signature**

6. A new Message Box opens up displaying the next action of the program along with information about the selected file; you may click **OK** to continue, or **CANCEL** to stop operation. Click **OK**;
7. A Message Box appears prompting you to choose **PUBLIC KEY** belonging to the person whose signature you want to verify. Click **OK**;
8. A new Message Box opens up displaying the next action of the program along with information about the selected file; you may click **OK** to continue, or **CANCEL** to stop operation;
9. The verification operation begins; its progress is displayed on the **Statusbar**. The operation may take a few seconds;
10. After completing, the program will inform you whether the signature is **AUTHENTIC** or **WRONG**.

[Encrypting disk files](#)

Endnotes 2... (after index)

Back Cover