



The Hacker's Nightmare

How to keep hackers, worms and other germs out of your PC

This complimentary chapter from
The Hackers Nightmare
is bought to you by



with permission of the author.

For more information on encryption products and services, and to order your own complete copy of *The Hackers Nightmare*, please visit

<http://www.ArticSoft.com/THN>

Chapter 22: Code Rings and Secret Handshakes



In the early part of this chapter I'll be talking about how difficult the implementation of powerful encryption can be if you don't know all the options that are open to you.

Please don't let this put you off.

The purpose of the introduction is to explain why I have chosen to take the path I adopt later in the chapter – a path that makes the implementation of useful encryption quite easy for any computer user.

I originally intended to treat the subject of encryption as a sub-section of another chapter covering a few miscellaneous considerations. However, thinking back over my past experiences with clients who felt they had a need for encryption, I was reminded of just what a difficult subject it can be to understand, implement and use.

Encryption is the process of turning ordinary text or images into a random, meaningless jumble of characters. **Decryption** is the reverse process, converting the encoded message back into its original form

As I solicited more and more opinions it became clear that there was a real need for a step-by-step treatment of encryption, presented in simple terms that required no expert knowledge to implement. I sincerely hope this chapter will address that need.

By "difficult to understand" I'm not referring to the *theory* of encryption, which can boggle even the best of minds. Encryption is rooted in mathematics and probability theory and goodness knows what other esoteric disciplines, an understanding of which is not at all necessary in order to *use* data encryption. The point is, if you aren't going to use good, strong encryption, there is not much point in using encryption at all.

My first instinct was to introduce and discuss the very same encryption standard that all other writers on the subject seem to lead with. Encryption has become synonymous with the acronym **PGP** – so named because developer Phil Zimmermann thought his algorithms made for *Pretty Good Privacy*. That turned out to be an understatement indeed, as PGP has become *the* encryption standard globally. It is so secure that governments and security agencies everywhere were having kittens wondering how they could prevent or control its use.

The history of the development of PGP and the battle to get it into the hands of ordinary computer users is an interesting story and one well worth following up for interest's sake alone. There are plenty of references on the World Wide Web to keep you entertained for some time. Search for the keywords: *Zimmerman PGP NSA|CIA|FBI*. By including the agencies in the search it will tend to return more "interesting" results, as it was the concerns of governments and law enforcement agencies that caused most of the furor.

Note: In the Google Search engine a vertical bar | signifies **OR**. Thus the search term above means:
*Zimmerman **AND** PGP **AND** at least one of the following: NSA **OR** CIA **OR** FBI*

If you haven't already decided that you need it, you may be wondering *"I'm not a secret agent – why would I want to use encryption?"*

The answer may well be that you don't! Then again, you may really have a need for increased security of sensitive data (particularly via eMail), but until now you haven't been aware of just how at-risk your data and correspondence are.

Possible reasons for using encryption are many and have been more than adequately addressed by many commentators, so I won't rehash it all again here. However, you may gain some understanding of the possible repercussions of indiscreet or incorrectly addressed plain-text eMails by visiting this web page:

<http://HackersNightmare.com?res=digitalblunders>

If you are a person of "delicate sensibilities", do heed their warning about "likely to offend", won't you!

I'll leave you to explore examples of "digital blunders" without further comment, other than to justify its inclusion by repeating a paragraph from one of their own pages:

"So while they may provide some great amusement there is obviously a serious issue here - with at least one sixth of the workforce running the daily risk of getting the sack for committing a Digital Blunder."

I also recommend you take a moment to do a Google search for the phrase *"why use encryption"*. As you can see from Figure 1, you'll get over 200 documents returned, of which at least a few should give you some food for thought. Just one word of warning though: Don't get too absorbed by the more paranoid positions of some authors. "They" probably aren't really out to get you at all ☺



Figure 1

Now although PGP is the de facto standard for encryption, many would-be users of such software have discovered to their frustration and disappointment that it is not a simple thing to implement. PGP developer Phil Zimmerman himself was clearly aware of this when he said*:

"For the past decade PGP has been the gold standard for email encryption but we've always had trouble expanding beyond the power users because of ease-of-use problems".

Since this book is aimed at teaching average, every-day PC users how to protect their privacy and their data, I felt a pressing need to find a product, service or method that met the prerequisite of "designed for computer **users**, not for technologists".

But, at the same time, I didn't want the encryption strength to be substandard or the price to be too high.

Your Privacy is Assured with *FileAssurity*TM

The product I eventually settled on fits all my requirements and then some. Developer *ArticSoft* has three inexpensive software packages that are suitable for use as personal encryption tools. One of those packages has what is called *OpenPGP* support.

OpenPGP is the most widely used email encryption standard in the world. It is defined by the OpenPGP Working Group of the Internet Engineering Task Force (IETF) Proposed Standard RFC 2440. The OpenPGP standard was originally derived from PGP (Pretty Good Privacy), first created by Phil Zimmermann in 1991.

The OpenPGP Alliance is a growing group of companies and other organizations that are implementers of the OpenPGP Proposed Standard. The Alliance works to facilitate technical interoperability and marketing synergy between OpenPGP implementations.

Phil Zimmerman is a key player in the ongoing development of the OpenPGP standard.

Too techo? Don't worry about it. It's not stuff you really need to know anyway.

In order to keep your introduction to encryption as simple as possible I have opted to acquaint you with ArticSoft's standard package, which does **not** incorporate OpenPGP.

Why did I choose the non-PGP option? I actually questioned ArticSoft on why they developed and supported the two different encryption methods used by *FileAssurity* and *FileAssurity OpenPGP*. The detailed reply from ArticSoft support included the following:

"It is generally admitted, even by the CEO of PGP Corp, that PGP is difficult to use. At the same time it has been the market leader (and was the first PK product available to the public since June 91) and is the dominant standard for encrypting files. Our customers tell us that our products are very much easier to use and to understand, and that their cost of ownership is significantly lower than that of PGP. So you would buy our OpenPGP product if you had friends using PGP (or any OpenPGP compliant product) and needed to receive files from them or, [if you] were part of a group that included those users as members. If

* ZDNet UK article, February 20, 2001 <http://HackersNightmare.com?res=zdnetaarticle1>

there was never going to be a need to interact with OpenPGP users then you would buy the straight FileAssurity product."

All of ArticSoft's encryption technology is highly secure and the only benefit the average individual or small business will gain from the OpenPGP package is the ability to communicate with others who use a straight PGP implementation or an OpenPGP variant.

But, for the beginner considering the use of encryption, it is important to ask how often that will be the case?

In my experience, people who perceive a need for very secure communications usually need to communicate with just one or two known others, or members of a small group. When action is finally taken to satisfy this need for enhanced privacy, the individuals involved will usually all adopt a common platform between them.

So, to recap ... if you want to communicate with an established group already using a PGP-based encryption product, you would choose *FileAssurity OpenPGP*. Otherwise, you'll almost certainly be better off going for the standard *FileAssurity* product, and building your own user group around that option.

One of the advantages of using a *FileAssurity* product is that you continue to use your usual eMail client. That is, if your eMail program of choice is say Outlook 2002, then you continue to use Outlook and you can continue to use the same local mail storage structure you already have in place. All your saved messages – sent and received – are stored in Outlook and are available to you whether you are on- or off-line. In other words, its business as usual – nothing changes. It is not the eMail itself that is being encrypted, but a document attached to the eMail

Incidentally, secure one-way messaging with individuals who don't have the *FileAssurity* program is also quite possible, thanks to a free *FileAssurity* "reader" program. Any owner of one of the full *FileAssurity* programs can send encrypted messages and/or files to others who have only the free *FileAssurity* Reader. Obviously, those people with only the Reader can't reply with encrypted content of their own. For those who need it, the *FileAssurity* Reader is available for free download from:

<http://HackersNightmare.com?res=articsoftregister>

Note that each of the ArticSoft products requires the use of a different Reader, but all Readers are available as a free download from that same page.

Why not just encrypt the eMail?

Newcomers to encrypted communications often wonder why they can't just enter their message into the body of an eMail as usual and have the eMail itself encrypted before transmission.

The answer is that, with certain "plug-in" software products, you can do just that. But it is an idea that makes security professionals shudder.

One of the reasons we have to consider encrypting our communications at all is because the eMail clients themselves are inherently unsafe. The various incarnations of Microsoft Outlook and Outlook Express are the classic examples. Outlook has been hacked and compromised so often it would be sheer folly to rely on it for assured confidentiality. Internet Explorer is also rife with vulnerabilities and, because of its close integration with Outlook, the eMail client is susceptible via Explorer's weaknesses as well as its own.

No serious and dedicated security developer would ever consider trying to plug a security module into an inherently insecure product.

The highly secure attachment suffers from none of these inherited susceptibilities.

As with most non-trivial applications, it pays to print and read the user guide. The *FileAssurity* manual is a HTML (web page style, viewed in your web browser such as Internet Explorer) guide installed with the program and accessed from within *FileAssurity*. Because it consists of a series of HTML pages you can print it out all at once by employing the following browser printing trick.

When the *FileAssurity* Help opens in your browser (Figure 2) click on the “Contents” link in the right-hand pane (marked with a black circle).

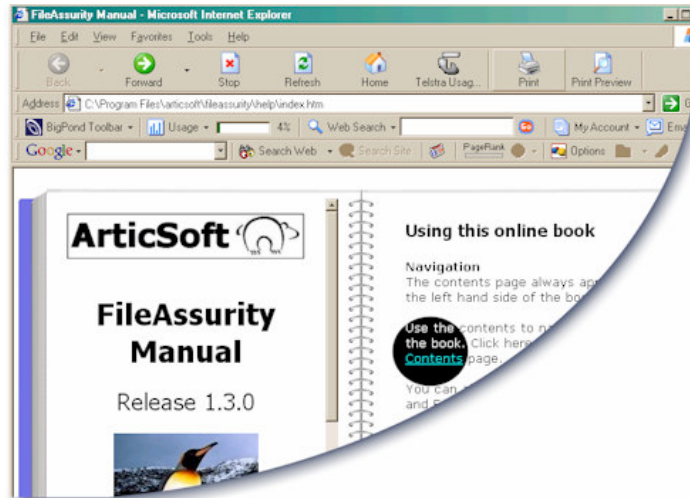


Figure 2

The guide's Contents page will fill the left-hand frame as shown in Figure 3.

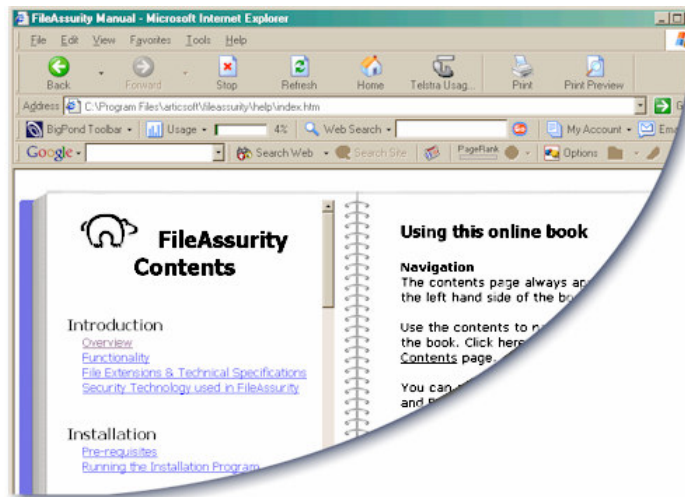


Figure 3

Click once on the left-hand frame of the Contents page, but **not** on a blue hyperlink – the Polar Bear's back-side will do fine 😊

Now click *File > Print* from the browser's menu bar, select a Printer, then click the Options Tab on the print dialog.

With the options set as shown in Figure 4, the Contents page will print, followed by all the documents linked on that page – which are, of course, all the subsequent pages of the guide. You now have a hard copy of the on-line manual.

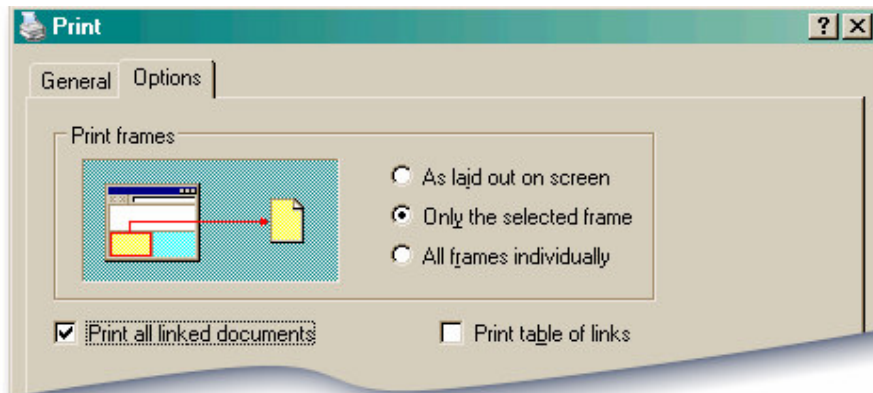


Figure 4

There is little point in going into great detail here on the *general* use of *FileAssurity* – you really do need to have at least a quick read of the manual. It's 60 pages when printed as described above, but it's an easy read and you won't need to cover the lot anyway.

If you are contemplating an encryption application I suggest you start with a trial of *FileAssurity* (standard) and go on from there.

Although I have concentrated here on the standard *FileAssurity* product, there's no guarantee that what suits me will be best for you. Although for security design reasons the keystores aren't interchangeable between the different versions, the products themselves are quite similar in operation. Similar enough that you certainly won't be wasting your time by starting with the standard *FileAssurity* then moving to *OpenPGP* or *ContentAssurity* if you find one of those more suited to your needs.

What is a keystore?

A keystore is a protected file (a database, in fact) where your own encryption keys are stored, as well as those you have imported from other people with whom you communicate securely.

Your keystore is managed with the Key Manager module from within *FileAssurity* (select Key Management on the Security menu).

The keystore is specific to your Windows logon name, so it is possible for multiple people to share the same PC and all to use *FileAssurity* securely, as each will have his/her own keystore.

Obviously for this to work all users must have their own individual Windows login ID and password.

For me personally *FileAssurity* standard is quite adequate at this time, but you should make the most of the 15-day free trial to sort out your particular requirements without cost or obligation.

Note: As is my habit before recommending software, I found a reason to contact ArticSoft's tech support, as much to test their willingness as anything else. Not only was the reply prompt, courteous and detailed, but their follow up convinced me I'd made the right choice.

On the assumption that most people researching encryption will initially be interested in securing their eMail correspondence, what follows is a detailed, step-by-step guide to getting started quickly, simply and at no cost.



eMail Encryption for Dummies: the Step-by-Step Guide

If you want to exchange highly secure eMail with a friend or colleague, this is the most detailed description you'll find to get set up and secret-eMailing to your heart's content. The application we will use to encrypt our correspondence has the added advantage of being able to encrypt any and all other stored data, from single files to entire directories.

★ Note ★ Note ★ Note ★

If you take a sneak peek ahead now you may be a little intimidated to see that the tutorial covers over 30 steps and fills the best part of eight pages. That's only because I'm leaving nothing to chance – I don't want even the rawest beginner to be left wondering or confused, so explanations are very detailed and supported with numerous illustrations. Step through this tutorial with me once and you'll be executing the exact same sequence in seconds the next time around. **To become an encrypted communications pro, start here...**

1. At the very least, close all programs. Better still, read and follow the general software installation instructions to be found in Appendix 2: Tips on Installing & Removing Software.
2. Download the free trial version of *FileAssurity*.
<http://HackersNightmare.com?res=articsoftregister>
Be sure to choose the "*FileAssurity 15-day Trial*" (**not** "*FileAssurity OpenPGP*").
3. When the File Download dialog box pops up, click the Open button (you don't need to download the program first).
4. Click "I Agree" on the License Agreement window.
5. Click Install.
6. Click Start *FileAssurity*.
7. Enter a good password. *The Hackers Nightmare* addresses the topic of password selection on page 217. Remember ... weak security is no security.
8. When the *FileAssurity* program window opens, make the following selection from the menu bar: Security > Key Management > My Own Keys.
9. The 4th button from the left on the Key Manager's button bar along the top of the Key Manager window is the button to create a secure key for yourself (the icon is a set of keys on a ring). Click that button now.
10. Complete the form in full. The only optional field is "Notes for this Key". Figure 5 shows a typical completed form. The name and address details you provide to this form become part of the certificate and are distributed to everyone who receives it. But rest assured that the private encryption key that is generated remains at your PC, and is not sent anywhere outside.

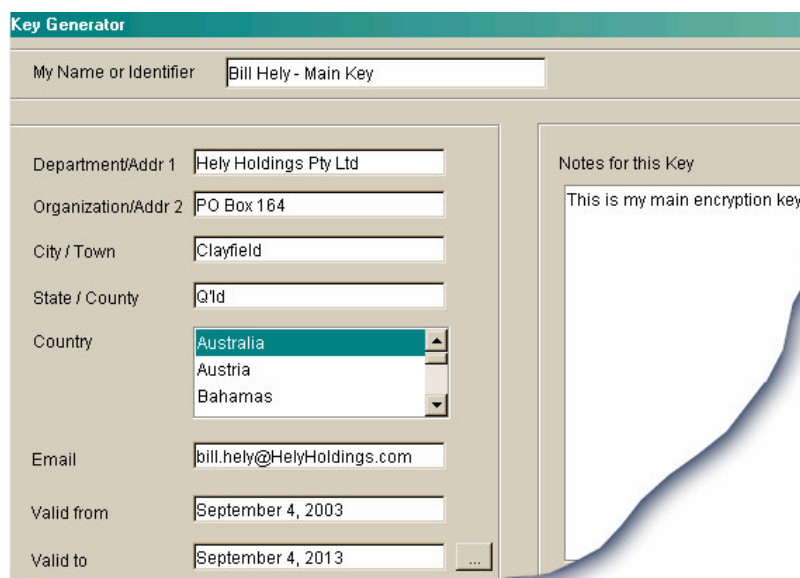
The default validity period is 1 year. For illustrative purposes only I decided to extend this to a decade (see bottom of Figure 5). You may not be able to extend to such a long period if you opt to purchase a Certificate from a registered *Certificate Authority* (CA). The CAs are in the business of selling Certificates and they'll generally want you to cough up every year.

For readers of *The Hackers Nightmare*, who I assume are predominantly individuals and small business operators, I really can't see any point in immersing yourself in the mire of Certificate Authorities and Registration Authorities – not at the outset anyway. If a group you are joining requires you to have a registered Certificate, you'll soon be told, and that group is the place to get assistance. If you want to know more about Certificates, Certificate Authorities and Digital Signatures, start here:

<Http://HackersNightmare.com?res=articsoftpkifag>

There is a wealth of other useful and informative material where that came from, on the ArticSoft articles page at:

<Http://HackersNightmare.com?res=articsoftarticles>



The screenshot shows a web-based form titled "Key Generator". The form has a teal header bar with the title. Below the header, there are several input fields and a dropdown menu. The "My Name or Identifier" field contains "Bill Hely - Main Key". The "Department/Addr 1" field contains "Hely Holdings Pty Ltd", "Organization/Addr 2" contains "PO Box 164", "City / Town" contains "Clayfield", "State / County" contains "Q'ld", and "Country" is a dropdown menu with "Australia" selected. The "Email" field contains "bill.hely@HelyHoldings.com". The "Valid from" field contains "September 4, 2003" and the "Valid to" field contains "September 4, 2013". To the right of these fields is a text area labeled "Notes for this Key" containing the text "This is my main encryption key."

Figure 5

11. With the form completed, click the Generate button and you'll see the message shown in Figure 6.

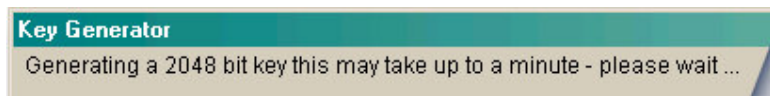


Figure 6

12. When that Key Generator dialog disappears, there'll be a new key entry in the top window of the Key Manager. The key I have created is called "Bill Hely – Main Key". There it is in Figure 7 with a tick ✓ against it.

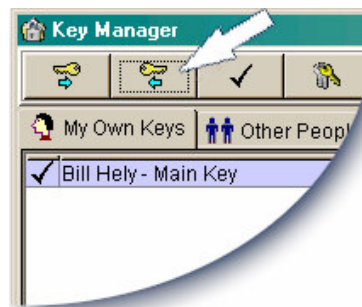


Figure 7

Now, what we have done so far is to create a security key for ourselves that other people will use to encrypt messages that can only be read by us. It is called your "public key" because you can give it to other people. There is nothing they can do with that key other than import it into their copy of *FileAssurity* to create secure messages for your eyes alone.

If you have heard of the term "private key" and are wondering where that fits in, rest assured that *FileAssurity* has created it and stored it safely on your computer. Your private key will never be available to other people.

Next we must save our new public key to a file we can pass to others, who in turn will import it into their copy of *FileAssurity*.

13. With your new key (in my case "Bill Hely – Main Key") highlighted, click the Export Key button (arrowed in Figure 7).
14. You now need to select a location on your hard disk and a name for the file that will contain the exported key.

Notice in the "Files of type" field the wording "...Public Key Certificate..." Let this be a reminder to you that you are exporting a *public key* that can be given to anyone else who has *FileAssurity*, so they can send encrypted files to you; files that only you can read.

Save this exported key file to somewhere you can easily find it, as you will shortly be attaching it to an eMail to send to your friend who is co-testing this encryption exercise with you. Do not add an extension to the filename – let *FileAssurity* take care of that. It will automatically add the mandatory extension of *.cer. For this example I have saved my exported public key to a file called:

`c:\Bill Hely Main Key.cer`

Note: A better place to save the file to would be:

`c:\Documents and Settings\BillHely\Personal\ Bill Hely Main Key.cer`

or your equivalent of that location. However, I want you to keep your attention focused on getting this encryption exercise finished, and not get distracted looking for storage locations you may not know about. If you can't quickly go to your equivalent of that personal folder, then save the file to C:\ instead. You can always use Windows Explorer to move it later.

15. Close the Key Manager.
16. You are now almost ready to go, but first you need to call in your co-conspirator☺. He must get his own trial copy of *FileAssurity*, perform the same steps that you have up to this point and send his public key to you. If your friend doesn't yet have

his own copy of *The Hackers Nightmare* to follow, he can download this *eMail Encryption Guide* and follow these same instructions. The download location is:

<Http://HackersNightmare.com?res=eMailEncryptGuide>

Very Important

You may NOT send a copy of *The Hackers Nightmare* eBook to your friend or to anyone else.

The Hackers Nightmare is copyrighted material. Selling, giving away, donating or lending copies is a violation of copyright law in all countries, and violations will be prosecuted to the fullest extent allowed by the law.

If you want to do your friends a favor please recommend the book to them. They can purchase their own fully legal copies at <http://HackersNightmare.com>

17. When you each have the others public key saved as a file, you need to Import the other person's key into your *FileAssurity* program. To do that you use the key manager module - click Security > Key Manager > Other People's Keys, then click the Import Key button (extreme left of button bar).
18. Using the Explorer-like interface now presented to you, find and import your friend's key file.



Once you and your correspondence partner have both reached this point, you are ready to start exchanging secure, encrypted eMail.

19. Well, almost. There's just one small step I suggest you take at this time to forestall possible confusion later on. With the *FileAssurity* program open, select *Security > Default Settings* from the Menu Bar.
20. When the Default Options window opens, check **both** of the check-boxes which are marked "Always use source folder".

This precaution just ensures that you won't get distracted by the un-encrypted and encrypted files ending up in different folders on your hard drive. In the interests of good housekeeping you may want them stored separately, but you can come back to the Default Options window later on and set the storage preferences any way you like. For now we want to keep things as simple as possible.

21. Click OK to close the Default Options window.
22. Now for something to send. Either create a new file or use an existing one, but make sure it is something you won't mind your partner seeing. You'll be encrypting this file and sending it off to the other person.

You can use MS Word, Windows Notepad, MS Excel - anything you like that produces a document of some sort. Make a mental note of where you save that file to.

For the sake of illustration I created a simple text file in Notepad and saved it to:

c:_EncTest\SecretFormula.txt

I used Windows Explorer to create the folder *_EncTest* just for this example.

The underscore at the beginning of the filename has no significance other than to make the folder appear high up in the directory tree where it is easy to find. You can see in Figure 8 that the folder *_EncTest* appears immediately below the AVG anti-virus vault folder which, because it starts with a "\$" sign, is earlier in the sort order.

23. If it's not still open, start *FileAssurity* and login using the password you chose in Step 7 above.
24. In the *FileAssurity* main window in Figure 8), browse to the saved file (*SecretFormula.txt* in my example). It's indicated by the big red 1.

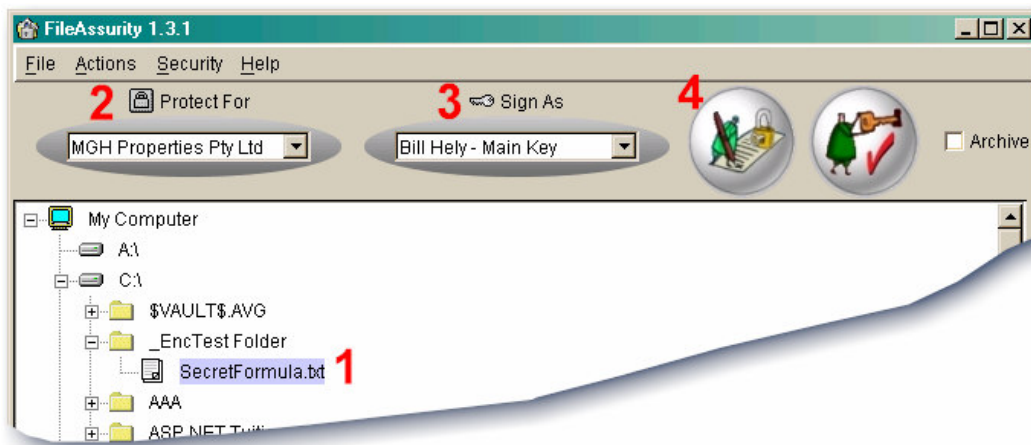


Figure 8

25. I'm going to encrypt this file for the person or company whose key I select in the "Protect For" drop-down list (Item 2 in Figure 8). You should encrypt your file for your encryption partner, so from the same drop-down list select your partner's key that you imported in steps 17 and 18 above.
26. I'm also going to have *FileAssurity* digitally sign the file so the addressee will know for sure that it came from me. So, for the "Sign As" option (item 3 in Figure 8), I'll select my own key that I created earlier.
27. Having made appropriate selections for Items 1, 2 and 3 in Figure 8, it's time to make it all happen by clicking the Protect/Sign button (Item 4). Alternatively, since Menu *icons* (e.g. the button) are just shortcuts for Menu *items*, you can select Actions > Protect Selected File(s)

28. A message box will appear telling you that "Your protected files have been stored in the same folder as the unprotected file. Total files protected 1". Click OK to clear that message.
29. Now look what we have in view. Compare the earlier Figure 8 with Figure 9 below. A new *encrypted* file named *SecretFormula.txt.fa_fsp* has appeared in the folder along with the original unencrypted file. If I select the new file with the mouse pointer, the pane on the right appears with information about the encrypted file. If I right-click on the entry in the right-hand pane, even more information will become available.

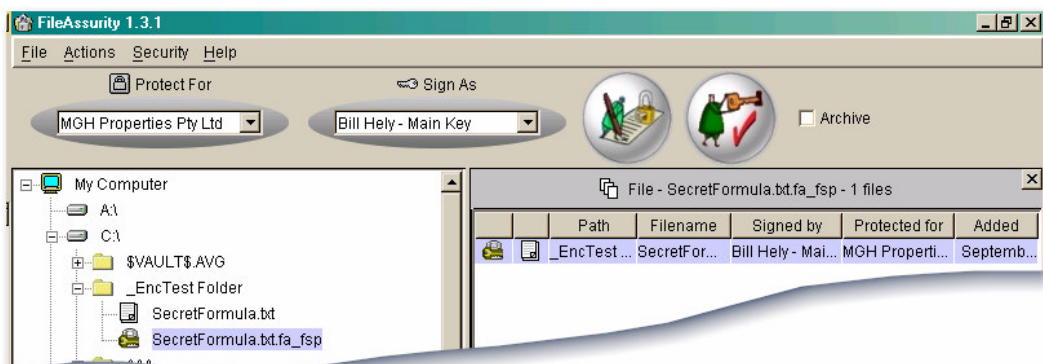


Figure 9


30. OK, now we have an encrypted file, so let's send it off to our partner. Simply right-click on the encrypted file in the left-hand pane and select *Send files to mail recipients* from the drop-down list.

Confirm that you do indeed "wish to send 1 files by e-mail" and you'll be presented with your eMail client program (e.g. Outlook), with the encrypted file already attached. Just complete the addressing fields and send the eMail as usual.

Also, don't forget to add some message text in the body of the eMail as well. It is poor "eMail etiquette" to just send a blank message with an attachment. Tell the addressee what you are sending. It's also a matter of safety - if the attachment somehow gets removed in transit at least your addressee will know there is something amiss, whereas a blank eMail tells little about itself!

That's it !

Phew! That took a bit of describing, but you should now be able to encrypt and eMail documents in your sleep!



When you receive the encrypted document that your friend has sent to you, you'll encounter it first as an attachment to a message in your eMail client (e.g. Outlook, Eudora, whatever).

In the final steps we'll look at viewing an incoming encrypted file.

31. Since Windows now knows (because the *FileAssurity* installation told it so) that a file extension of "*fa_fsp*" is associated with *FileAssurity*, opening the attachment will automatically pop up the *FileAssurity* login box.

Bug Report

There is a minor bug in *FileAssurity* version 1.3.1, in that you will be asked to login again and a new instance of *FileAssurity* will start up even if it was already running. Expect this to be fixed in the next version of *FileAssurity*, due sometime in the last quarter of 2003.

For safety's sake, look at the attachment's filename and note the extension before you attempt to open it. *The Hackers Nightmare* explains why it is so very important to always make this check with attachments. After double-checking that the extension does indeed end in *.fa_fsp* you can open the eMail attachment.

By the way, you *do* have your **AVG anti-virus program** installed and updated, don't you? If you haven't then I am getting very worried about you. You are way ahead of yourself just by being here! All is explained in *Chapter 15: Vanquishing the Virus*.

32. Anyway... *FileAssurity* will ask you to login, so please do so.
33. When *FileAssurity* opens it will automatically highlight the encrypted attachment file in the left-hand window pane and the file details will appear in the right-hand pane (Figure 10).

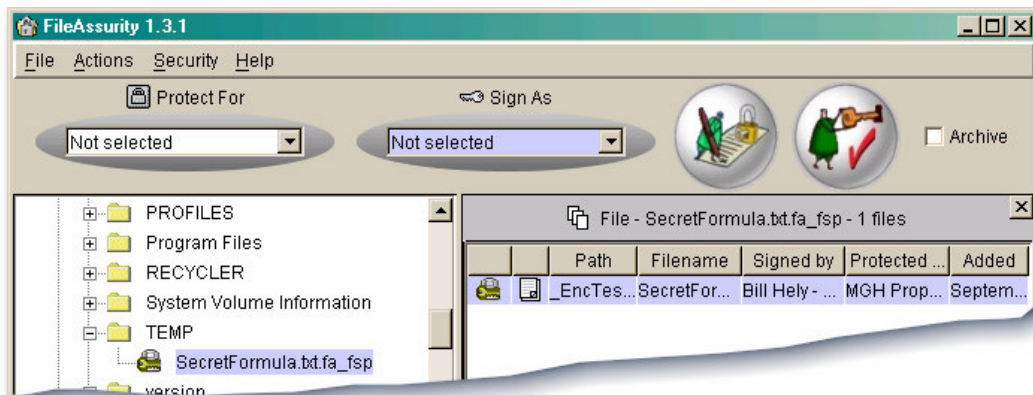


Figure 10

As is indicated by the *fa_fsp* filename extension, the file saved to the TEMP folder is still protected.

34. With the newly saved file selected in the left-hand pane, right clicking the entry in the right-hand pane will give you the option to *Unprotect selected file(s)*.

Do that now.

In response, *FileAssurity* will place an un-encrypted copy of the file in the TEMP folder (A in Figure 11).

At the same time, *FileAssurity* will also show you a log of the un-encryption event in the lower part of the right-hand pane. The log includes a link (B in Figure 11) to open the un-encrypted copy.

By virtue of the file associations built into Windows, clicking that link will open the un-encrypted file in whatever application is suitable for the file type. In the case of my .txt file example, the associated application would (by default) be Windows Notepad.

File associations should be largely automatic and should not be something you would normally have to concern yourself with.

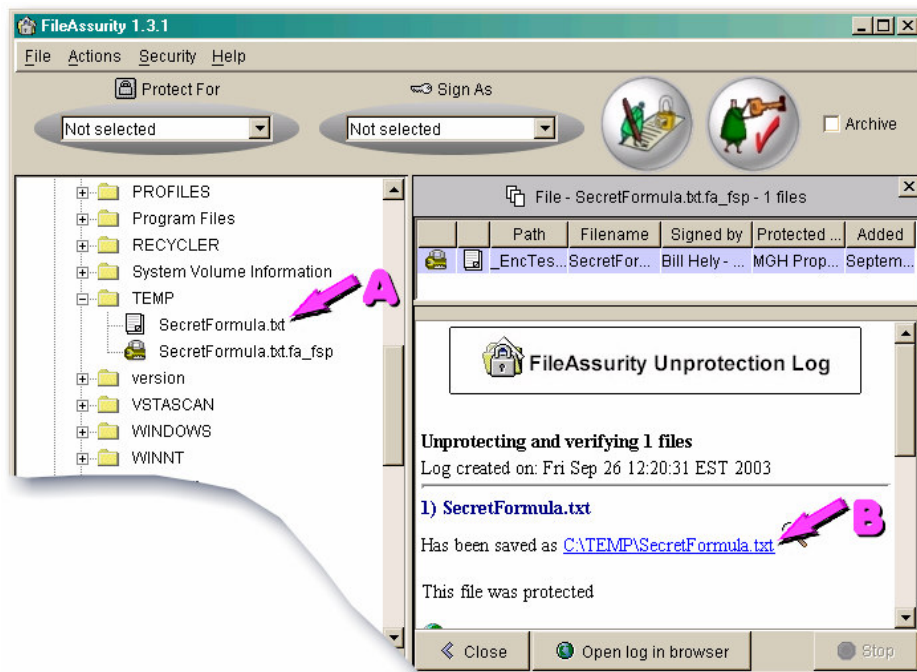


Figure 11

Well, that's it. The whole enchilada.

Encrypting – Sending – Receiving – Un-encrypting

You now know it all.

From here on in, you'll find encrypted communications just too easy.

But don't get too carried away!

Encryption, no matter how good, will do nothing to protect you from a whole raft of dangers that can threaten the security of your PC and its valuable data.

Encrypted files can be maliciously (or accidentally, for that matter) deleted, destroyed or corrupted like any other file.

You'll be amazed at some of the ways the gutter dwellers of cyberspace attempt to damage and compromise you.

Give yourself a fighting chance ...

Read, digest and apply the contents of The Hacker's Nightmare.

Before leaving applications that can do *file* encryption, I should mention ArticSoft's 3rd encryption package, *ContentAssurity*. This one will actually encrypt the contents of an eMail, or any other document for that matter. This screen shot from their Help file gives a good indication of what *ContentAssurity* does.

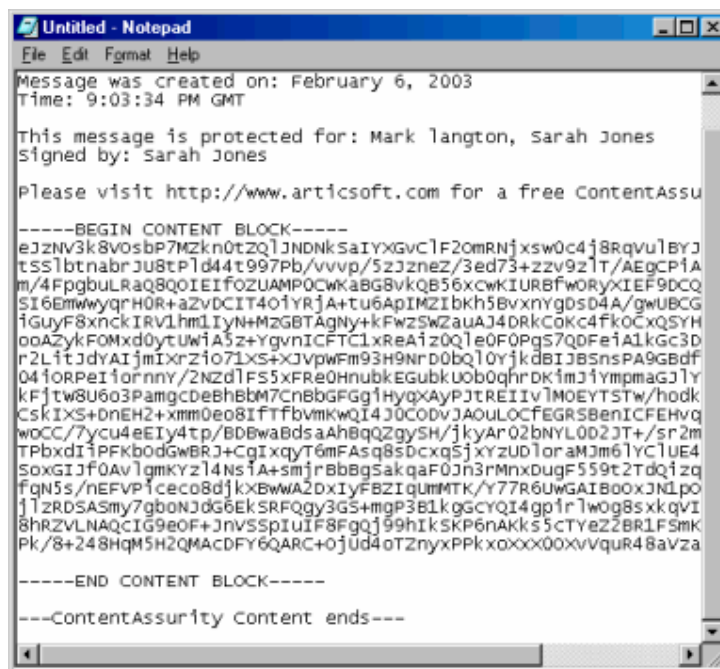


Figure 12

As the name implies, *ContentAssurity* can encrypt all or part of the *contents* of a document. The sample encrypted content in Windows Notepad in Figure 12 above could as easily be the body of an eMail, all or part of a Word™ document, part of an Excel spreadsheet, etc.

Pre-release Notice: By the time this book is available, ArticSoft will have released Version 2 of *FileAssurity OpenPGP*. This is particularly worthy of note to anyone whose testing has indicated that *ContentAssurity* may be the product for them. The new release of *FileAssurity OpenPGP* will, for the first time, incorporate a cut-down version of the *ContentAssurity* secure text editor. It won't boast all the features of the full blown *ContentAssurity* (audit trail and multiple signature support are not available) but it will allow you to send message text securely. As an added bonus, all operations can be performed from within Windows Explorer without having to use the *FileAssurity OpenPGP* application directly.

There is another fairly simple way to use encrypted eMail for communications, but it is restricted purely to eMail and does not provide any facilities for file encryption This method actually encrypts the contents of the eMail itself, rather than encrypting attached messages, but it does limit you to using *WebMail* (see sidebar below). Let's take a quick look at ...

HushMail

A service called HushMail is probably the easiest way of all to send and receive highly secure encrypted eMail, but it does have the disadvantage that some of your eMail is going to be stored locally on your PC (your normal, unencrypted POP mail - see sidebar) while your encrypted messages will be stored on the HushMail server and can only be accessed via your browser while connected to the Internet.

Note also that the HushMail service only encrypts the contents of the eMail. It doesn't allow you to encrypt files for secure storage on your hard disk or for attachment to the eMail. For those features you should look to one of the *FileAssurity* products discussed above.

For a quick introduction to HushMail check out the 4-minute TechTV video (it's a movie, so it might take a while to load on a slow connection):

<http://HackersNightmare.com?res=hushmailttv>

If that brief intro has aroused your interest, slip on over to the HushMail website and have a look around. By all means try out the free account offering first, but I think you'll soon grow weary of the adverts, which is why it's a free option. Fortunately, the Premium Service is very affordable at US\$29.99 per year, which includes 32MB of storage for secure messages you want to keep.

<http://HackersNightmare.com?res=hushmailhome>

The easiest way to set up a HushMail account is to follow the simplified directions I'll give you shortly.

But Do This First...

Before you sign up for a HushMail account, prepare yourself by reading this page:

<http://HackersNightmare.com?res=diceware1>

WebMail is a service that allows you to access your eMail through a web browser (e.g. Internet Explorer), rather than through an email program such as Outlook or Eudora. You simply browse to a web page assigned by your service provider (e.g. <http://mail.mydomain.com>) and enter your username and password.

Being web-based and not dependant on an eMail client, you can access WebMail from any computer anywhere, so long as it has a connection to the Internet. Very handy for travelers.

Hotmail and *Yahoo! Mail* are both WebMail services, though the use of such addresses doesn't present a very professional image of you or your business.

All the best hosting services and ISPs offer WebMail as well as POP mail (the one you are probably most familiar with, where you download eMail to your computer for viewing in your eMail program).

One weakness to keep in mind when considering any WebMail service is that websites do "go down" periodically. If the WebMail server is out of service for any reason you cannot even access your stored messages, let alone any new incoming.

HushMail is going to ask you to enter a "pass phrase" - which is NOT the same as a "password" - so it will save some time if you are prepared. As the opening paragraph on that web page says:

*"If you care enough about privacy to use encryption,
take a few minutes and learn how to do it right".*

And if you didn't already follow the link to the FAQ while reading that page, do it now:

<http://HackersNightmare.com?res=diceware2>

Step-by-Step Instructions for Establishing a HushMail Account

1. Browse to <http://HackersNightmare.com?res=hushmailhome>
2. Click the Go button for HushMail signup on the left-hand side of the page.
3. Read the Terms of Service then click the "I Agree" button.
4. Read the contents of the Account Creation window and click Next.
5. If you get a popup "Java Plug-in Security Warning", click "Grant always".
6. Enter a username for your HushMail eMail account. Something like "firstname.lastname" might be appropriate. Then select the domain you prefer from those available in the drop-down list. Your final HushMail eMail address will be something like *Nancy.Byrd@hush.com*. If you are entering a username yourself DO NOT click the Auto-generate Username button. Click next.
7. Read the instructions on creating random encryption keys, then click Next.
8. Keep moving and clicking as instructed until the window disappears.
9. Enter a pass phrase (it can take a while to process) then press Next.
10. Finally, you'll be presented with a dialog that asks if you would like to add HushMail to your Favorites list. Probably a good idea. Click OK.
11. The dialog disappears. Read the new info you are presented with in the browser, and then click Finish.
12. You'll now be taken to a page headed "Important Information". If you are just trialing HushMail, scroll all the way to the bottom of the page and click "Continue Standard". The Standard account is free but has the following limitations:
 - Only 2MB of storage space
 - There'll be annoying banner advertising
 - No technical support
 - Account will be terminated if left unused for 3 weeks

If you want better than that, fill out the upgrade form for HushMail Premium (US\$29.99 pa) then follow its button.

A Premium Account provides the same industrial-grade security as the standard HushMail account, with the following additional benefits:

- Your account will never be closed for inactivity
 - 32Mb of storage space - upgradeable to a maximum of 128MB.
 - You don't have to suffer banner ads or pop-ups
 - Dedicated servers for faster access & download times
 - Advance (sometimes exclusive) access to new products
 - Extended account preferences
 - Spam blocking
 - Premium technical support
 - One-click access to an "encryption toolkit"
13. Fill in your pass phrase to login and you'll be at the main mail page. The only thing to do from here is to get your friends and associates to join so you will have someone to securely correspond with!

Remember, to be able to correspond using encrypted eMail, both the sender and the recipient must have HushMail accounts.

Encryption Postscript

Mostly when clients approach me seeking information on encryption, their prime concern is to secure their eMail correspondence. As shown in this chapter, there are different ways to accomplish that end. However, there are definite advantages to choosing a method that also allows the encryption of files. Why?

We all know that it is a *Very Bad Idea* to store records pertaining to certain personal information in files on our computers. Some examples of information too sensitive to take any risks with are on-line banking accounts, Credit Cards, checkbook, insurance policies, birth certificates, passports, membership numbers and so on.

Yet we all do it anyway, don't we? We need to have backups of our hard copy documents and reminders about certain "stuff", and a computer file is an excellent way to store such information. After all, storing information is what computer's are all about.

But, as you are learning in this book, there are all manner of ways a stranger can get at anything you store on a computer. Sure, I'm giving you a series of lessons in ways to stop would-be intruders, but some data is just too important not to protect in every way possible. Remember our catch cry from the earlier chapters of this book... *Defense in depth*.

By encrypting the actual files that hold your most sensitive information, together with following the other recommendations in this book, you are rendering your personal data as inviolate as is humanly possible within the bounds of reasonable, workable precautions.

Thus, while an eMail-only encryption service certainly meets one need, it may not be the best solution for you.

And finally, a wake up call to some people who badly need it ...

Just how much sympathy do they deserve?

To press home the point of encryption, I thought it might be interesting to quote a few news articles as examples of the importance of securing sensitive data, and on laptop computers in particular.

However, my quest for such stories turned up so many that I decided to let you conduct your own search instead. Here's just one search term that will return over twenty-two thousand examples on Google. No, I'm not suggesting you read all 22,000 hits, but do pick and choose a few. There are some real eye-openers.

Cut and past this search term exactly as it appears below into your Google Toolbar search field. If you don't know what a Google Toolbar is, see the Special Note on page **Error! Bookmark not defined.** Here's the search term:

laptop stolen army OR navy OR marines OR military secret OR sensitive OR personal OR private

And that's essentially limiting the results to just the armed services. Makes you wonder how staggering the loss value is when corporate/commercial instances are included. One could take the mercenary viewpoint and say that, well, they're probably insured and equipment can be replaced. Sure ... and in many instances the stolen items are recovered intact.

So what?

Data that has found its way into someone else's head remains "stolen" no matter whether you regain physical possession or not.

If you are a tax-paying citizen of any country you should be very concerned that various arms of your government are placing sensitive information at risk by ignoring the simple and relatively inexpensive expedient of applying encryption.

Does it surprise you that your military (!!!) loses computers that contain sensitive, unencrypted data? Does it horrify you?

There was an incident in Australia around September 2003 where laptop computers assigned to the Department of Customs and Excise and containing information which was admitted to be "sensitive" were stolen from a government site. But ... Oh joy! Everything's OK. They eventually caught the thieves and recovered the laptops. Isn't that great? No harm done, eh? Everyone is forgiven.

Hmmm. Do you think maybe some of our minders are missing the point? This is Government we're talking about. Who has more resources? And the more resources you have at your disposal the fewer excuses you can be allowed.

What are these people and their hirelings thinking?

Whether it be government, military, corporate or personal, I think the lack of appropriate security and the absence of encryption when it is warranted is a costly, dangerous and unforgivable lapse of common sense.

A Note From The Author

Thank you for taking the time to read this sample chapter from my book *The Hackers Nightmare*. I hope you enjoyed and profited from it. The book itself is the result of much research – not only into the threats extant, but even more so into the simplest, least arcane ways to counter and protect against them.

In those instances where the most useful solutions are inherently complex by nature, much effort has gone into providing readable, jargon-free explanations and a wealth of illustrations and screen-shots. With even the most complex of solutions, implementation is almost a case of “*just connect the dots*”.

All products and services recommended in *The Hackers Nightmare* were independently “discovered” by me, assessed for suitability and partly written up before the publishers or service providers were approached. Only the providers of those products and services I considered worthy of recommendation were then asked to supply more information where I deemed it necessary.

No supplier was ever asked for remuneration or favors of any kind in return for inclusion, other than (in some cases) to provide a full copy of software for more in-depth assessment than could be made with a trial version.

The full edition of *The Hackers Nightmare* has been designed to empower and safeguard the data, computers and on-line activities of ordinary, everyday computer users.

I have taken great pains throughout to present security threats and their remedies in a simple, step-by-step manner. I firmly believe that this book will enable anyone, not just experts, to secure their computing environment against the many dangers that threaten personal and small business computing and spoil the Internet experience.

To order your own complete copy
of *The Hackers Nightmare* please browse to

<http://www.Articsoft.com/THN>

Wishing you safe and secure computing.

Bill Hely
Author – *The Hackers Nightmare*
Brisbane, Australia. November 2003.