GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

A Consumer Guide for Personal File and Disk Encryption Programs

GSEC Version 1.4b Option 1

Scott Baldwin

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Contents

Abstract	Page 3
Reasons to use an Encryption Program	Page 3
Encryption Basics	Page 4
Encrypting Files, Folders, Virtual Drives or Partitions	Page 5
Crypto Systems	Page 6
Symmetric Systems	Page 7
Asymmetric Cryptosystems	Page 7
Hybrid Cryptosystems	Page 8
Transferring Encrypted Information	Page 8
Ease of Use	Page 9
Cost	Page 10
Concealing Encrypted Information	Page 10
Backing up your Encrypted Information	Page 11
Laws, Regulations, and Company or Business Partner Standards	Page 11
Finding A File Encryption Product That is Right For You	Page 11
Summary	Page 12
References	Page 13
Appendix A	Page 14
Appendix B	Page 16

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Abstract
Encryption products are becoming a popular solution to maintain the confidentiality of digital information. Most encryption programs provide a wide range of features. For the average personal computer user, trying to understand and identify whether an encryption program is needed, and if so, which features they need can make choosing an encryption product a very frustrating task. This guide will give you the knowledge to select an encryption product that matches your needs. The following topics will be covered:

- Reasons you might want to encrypt the data on your personal computer
- Basic encryption concepts
- Basic and advanced features that personal encryption programs provide
- Issues to consider in selecting an encryption program
- Tips for finding an encryption program that has the features you need

Reasons To Use An Encryption Program

Some people question their need for encryption software because they assume that they have taken adequate steps to safeguard their sensitive data or that they do not have any sensitive data on their personal computer. I have also found that many people are not aware of the impact a skilled social engineer (person skilled at tricking people into providing information that they would not otherwise provide) or hacker could have on their business or personal life by obtaining their sensitive information. Encryption may be your last line of defense if your other security controls become compromised. As part of a multi-layered security strategy, you should have several layers of security. Your security strategy should include both physical and technical security controls.

Your data may not be as safe as you think. You may have a firewall between you and the Internet to prevent hackers from accessing your data. As you travel from one city to another, you might keep a tight grip on your laptop to prevent thieves from stealing it. When you are not home, your desktop computer is probably powered off and your windows and doors are locked. However, attackers get through firewalls. Mobile business professionals cannot keep an eye on their laptops 100% of the time. Computers get stolen from businesses and homes every day.

Many personal computer users do not realize that they have sensitive data on their computers. I suggest you stop and think about what applications you have on your computer and what data you have created or received from those applications. Do you have any e-mail with sensitive information? Did you do your tax return on your computer? Did you scan any documents that have sensitive information? You may have personal information that a skilled social engineer could use to con your bank, health care provider, or employer into providing the information they want. If your computer has sensitive business information stored on it and an attacker obtained that information, it could cost your company thousands of dollars.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Irwin Jacobs, who was the chief executive of Qualcom, was a victim of laptop theft two years ago. He had just finished giving a presentation to the Society of American Business Editors and Writers and was talking to journalist when he realized that his laptop, which had only been a few feet from him, was missing. He admitted to having financial statements, secret corporate data, years of e-mail, and pictures of his grandchildren on his laptop. [1] The incident not only had potential to cost Qualcom a significant amount of money but also to wreck havoc on Irwin Jacob's personal life.

What could someone do with the information on your computer? Regardless if they obtained business information or personal information, they may have adequate information to launch a successful social engineering attack against you, your friends, coworkers, business partners, or clients. You may have intellectual information saved on your computer that is valuable to others. The loss of intellectual or proprietary information cost companies millions of dollars every year.

Encryption Basics

Currently, many of us depend on encryption every day with out even thinking about it; if you do your banking on-line, most likely your web browser and the your bank's web site have established a secure connection using encryption. If you do on-line shopping, you will most likely depend on encryption. Your own business and many of the businesses you depend on for services rely on encryption. You probably do not want to know everything there is to know about encryption. However, understanding the following basic encryption concepts will significantly help you in choosing an encryption product.

Encryption is the transformation of text into unreadable ciphertext. In 1900 BC, the Egyptians used the first form of encryption known as hieroglyphics. [2] The early forms of encryption were carved into stones and written on scrolls. Later, mechanical devices were used to encrypt and decrypt information. The most famous mechanical encryption device was the enigma machine. It was used during World War II by the Germans to relay sensitive information. [3] Once the computer was invented, we had a tool to efficiently use very complex algorithms to encrypt and decrypt information.

An algorithm is a set of mathematical rules used to encrypt data. There are many well-known algorithms. Unlike the old popular decoder ring some of us played with as a kid, modern encryption algorithms are very complex. Algorithms employ multiple rounds of substitution, which is a substitution of characters with different characters, and permutation, which changes the order of the characters.

A key is a series of characters or instructions that algorithms use to encrypt and decrypt information. The key can be a password or a file. The length and complexity of the key are two critical factors that determine how well your

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

encryption algorithm can protect your information. If your key is a password and you use “00” as your key, than your encrypted information would be much easier to crack compared to a password of WAL2UCED. You might think WAL2UCED is hard to remember, but it is not; it is a pass phrase that stands for “We All Love 2 Use Cryptography Every Day”.

The key space is the total number of different values that can be used for the key. A typical briefcase lock has three dials. Each dial has digits from zero to nine. That would give you a total of 1000 different potential combinations to use. A 56-bit encryption key has 72 quadrillion possible combinations. [4]

Symmetric cryptosystems, also known as Secret Key systems, use a single key to encrypt and decrypt information. You can think of a symmetric key like the numbers you must set on a combination lock to open it. Asymmetric cryptosystems, also known as public key systems, use two keys. One is your private key that you do not share with others, and the other is the public key that is shared. Anyone who has access to your public key can use it to encrypt information, however, only your private key can decrypt that information. The public key can be thought of as a padlock that is available to everyone. Anyone can use it to lock information that is to be sent to you. However, only you have the key that can unlock the padlock.

Encrypting Files, Folders, Virtual Drives, or Partitions

Some encryption programs can encrypt files but not folders. If you only have a few files you need to encrypt**,** then this will not be an issue for you. This limitation is most common in freeware versions. The majority of the commercial encryption programs have the ability to encrypt files and folders. Some will even encrypt entire partitions.

Manual encryption involves selecting the files or folders you want to encrypt through the encryption program, assigning the password or encryption key that will be used to encrypt and decrypt them and destination path for the files, and then encrypting them. Some programs will let you bundle all the encrypted files into a single encrypted file. That is a nice feature if you plan to transfer or e-mail the files. One disadvantage of bundling all the files together is that you will have to decrypt all the files any time you need access to any of them. One mistake people make with manual encryption programs is that they will encrypt their data but leave the un-encrypted version accessible. Some programs provide the option to automatically delete the original document after it has been successfully encrypted (see appendix A for an example of a symmetric encryption program).

On-the-fly encryption is a feature that can add convenience and security. It will only decrypt information as you need it, and encrypt the data as you save it. It is a good alternative to manual encryption and decryption. On-they-fly encryption programs create a virtual drive, a designated folder that contains the encrypted information, or an entire encrypted drive. [5] Information gets decrypted as it is

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

accessed from the saved location and any data that is saved to a virtual drive or designated folder is automatically encrypted.

Virtual drive encryption programs create virtual drives that are linked to files commonly know as container files on unencrypted drives (see Appendix B for an example). In other words, you will end up with an apparent additional hard drive. That additional hard drive is really the contents of the container file. [6] The following example might clarify the concept. You have several folders of information you want to protect. You start your encryption program, enter 100 megabytes for size of the virtual drive you want to create, enter c:\encrypt.123 for the name and location of the container file, and you enter F as the default drive letter. Then you assign the password needed to access the container file. The next step is to mount the virtual drive. To do this, you typically double click on the container file. That will launch the encryption program that will prompt you for the password you assigned to the container file. Once you enter the correct password, your F drive will become available. After that, you can access, create, modify, and delete files and folders on your F drive just as you can on your C drive. To secure the files you have two options: dismount the virtual drive or shut down the computer. To access the virtual drive the next time, you simply follow the process as mentioned above to mount the drive. The mechanics behind virtual drive encryption may seem complex but, once you have configured the virtual drives, they are easy to use.

Encrypting an entire partition or disk may seem like a better option than using virtual drives or folders, however, its disadvantages should not be overlooked. Entire disk encryption as its name implies, will encrypt the entire partition or disk. Some full encryption programs allow all partitions including the system and boot partitions to be encrypted. With this, you would be prompted for a password when your computer boots. Once you enter the password, you will have access to all encrypted partitions. These types of encryption programs are more transparent to users than the other encryption options. One disadvantage to this method is that once you enter the password, your data is no longer protected by the encryption program until you shut down your computer or logoff. In other words, your computer would not be protected from remote attackers while you are using your PC or from physical access attempts if you leave your computer unattended after unlocking your encrypted information.

Cryptosystems

Another major consideration is the type of cryptosystem you want to use. You can choose from three primary types. They are symmetric, asymmetric, and a hybrid of the two. Each system has its advantages and disadvantages. As stated earlier, a symmetric key system uses the same key for encryption and decryption. Some known symmetric algorithms are DES (Data Encryption Standard), Triple DES, and Rijndael. DES is a popular, freely available algorithm, which has a 56 bit-key space.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Symmetric Cryptosystems

In 1999, a DES key was broken in less than 24 hours. [7] The need for a stronger algorithm was recognized. Triple DES was its replacement. Triple DES simply runs the DES algorithm three times. One disadvantage of Triple DES is that it takes three times as long to encrypt data. Other algorithms were created to address the shortcomings of the DES and Triple DES algorithms. In 1997, the National Institute of Standards and Technology worked to establish a new algorithm that could be recognized as a worldwide standard to replace DES and Triple DES. In 2000, the Rijndael algorithm was selected and is now also known as AES (Advanced Encryption Standard). AES was chosen for its strength, performance, and simplicity. Unlike it predecessor DES that has a 56 bit-key, the Rijndael algorithm can have up to a 256 bit-key. [8] Even though AES is the newest standard, DES and Triple DES are still widely used.

If you plan to share your encrypted files with others and you are using simple symmetric encryption, then you will have to provide them with the password or key file you used to encrypt the data. This can present several challenges. First, you will have to transmit the password or key file you used to encrypt the data to them in a secure manner. Second, you should not use the same password to encrypt information that you plan not to share with information you plan to share; if the same password is used and any of the recipients gained access to your other encrypted files, they could obviously decrypt them. Also, if they share your encrypted information with others, then more people will know the password that was used. There are several ways to address that problem.

While some symmetric encryption programs only allow you to secure information with a password, others allow you to also use a key file. A key file is a small file that can reside on a hard drive, floppy drive, USB token, or other available storage mediums. Some programs go a step further by using a strong key file to protect the data and then encrypt the key file with a password. When this method is used, you can share your encrypted information with others without having to provide them with the same password you use on information that is not destined for them. When a key file is created for someone else, you will have to provide a password but it can be unique to that key file. Unfortunately, only a limited number of symmetric encryption programs have this feature.

Asymmetric Cryptosystems

Asymmetric cryptosystems, also known as “Public Key” cryptosystems, are a more widely adopted technique to manage and distribute shared keys. Some popular asymmetric algorithms are RSA, Elliptical Curve, and Diffie-Hellman. As mentioned earlier, two keys that are related to each other are used: a private key and a public key. Public keys can be distributed to others and they can use them to encrypt information. However, only the corresponding private keys can decrypt that information. [9] This key management system enables the exchange of encrypted information in a more secure manner than with Symmetric cryptosystems.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Asymmetric Algorithms have some additional overhead compared to symmetric cryptosystems. For one, they are more computationally intensive and, therefore, take longer to encrypt and decrypt information. Secondly, there has to be a secure way to exchange keys; if you use the wrong key to encrypt information and the owner of that key obtains the information, the owner of that key would be able to decrypt the information. Many implementations of asymmetric cryptosystems depend on certificate authorities to manage the keys. Certificate authorities are computers that all parties involved in the exchange of encrypted information must rely on to securely store and distribute the keys.

Hybrid Cryptosystems

The third cryptosystem is a hybrid of the previously two mentioned systems. Symmetric algorithms are used to encrypt data and asymmetric algorithms are used to protect the symmetric keys. This option provides the performance of symmetric encryption and the key management features of asymmetric encryption. Some of the more advanced encryption products provide this feature.

Examples of some the more popular algorithms have been previously mentioned. There are many other good algorithms to choose from. However, avoid using proprietary algorithms. Established algorithms have been thoroughly tested and their strengths and weaknesses have been established. If you use a proprietary algorithm, you will run the risk that someone may find a new vulnerability within the algorithm and therefore significantly diminish its ability to keep your information secure.

Transferring Encrypted Information

If you plan to send encrypted files to other people, there are a few issues you should consider. First, your encryption program must support the transfer of encrypted files. Secondly, the recipient must have an encryption program that is compatible with the encrypted files you send them or you must send them a self-decrypting file.

Some encryption programs provide a self-decrypting option when you encrypt data. The decryption software gets embedded into the file or files that you encrypt. Typically, self-decrypting files are executables. In order for a recipient to decrypt a file, they simply run the program, get prompted to enter the decryption key, and a location for the files to save to once they are decrypted. Another nice feature of self-decrypting files is that if you encrypt data now and two years from now, you want to decrypt the data but your encryption program is not installed, you can still decrypt the information.

Asymmetric encryption technology has greatly facilitated the process of sharing encrypted information; you can distribute your public key to others, enabling them to encrypt information destined to you. Unlike symmetric algorithms, only you will have the key to decrypt the information. If you plan to exchange a lot of

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

information with other people, then you should consider using an encryption program that utilizes asymmetric or hybrid algorithms. Some asymmetric and hybrid encryption programs have good public and private key management tools and work with some of the more popular e-mail programs to provide a user-friendly process for sending encrypted information via e-mail.

Some encryption programs may support the transfer of encrypted information but the process to transfer the encrypted information may not be practical for you. Programs that encrypt the entire partition or hard drive can only be transferred in their encrypted format if an image (a copy of the partition) is created of the partition or drive. The image file could be very large. Also, the recipient will need a copy of the image software and an empty partition of equal or greater size to install the image.

On-the-fly encryption programs that use containers can be transferred as long as the size of the container file does not exceed the capacity of the media you plan to use to transfer it with and the capacity of the destination media. If you have a CD burner installed in your personal computer and you keep your container files under 650 Megabytes, than you will always have the option to copy, move, or archive container files to CDs.

Ease of Use

It is important that the encryption program you chose is unobtrusive and easy to use; if not, you will not use it, and therefore leave information unprotected. Some encryption programs integrate into the operating system and applications. Others are integrated into a suite of other tools. There should also be documentation that clearly explains the installation process and how to use the product.

Some manual encryption programs add encryption and decryption options to the Windows Explorer menu. That enables you to right click on files or folders and encrypt them verses having to open the encryption program and select the files (see Appendix A figure 1 for an example). Almost all encryption programs associate encrypted files with the encryption program. This enables you to double click on encrypted files, enter the decryption password and a destination path for the decrypted files and then proceed to decrypt them. That saves time because you do not have to manually launch the encryption program first.

Password caches save time if you have to encrypt or decrypt multiple files that use the same password. The program will remember the password so that you do not have to enter it each time. This feature should be used with caution because an attacker might be able to decrypt your encrypted information if the password is in the cache.

Most programs that have a password cache allow you to manually remove the information from cache and also automatically remove the cached information when you turn off your computer. Some of the programs will dump the cache

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

after a configurable period of inactivity or when the screen saver runs. Configuring these options allow you to balance ease of use and security.

At some, point you may want to change the password you used to encrypt your files. Some programs will require you to decrypt the information with the original password and then encrypt it again with the new password. If you are working with large files, it can be a time consuming process. Some encryption programs will save you the agony by allowing you to change passwords or key files without having to decrypt and re-encrypt the information.

Cost

File encryption programs range in price from free to over one hundred dollars. In the freeware range, you will find many file level encryption programs. Some of those are actually good programs; they have a polished interface, offer several algorithms to choose from, have the ability to create self-decrypting files, and other features. If you are looking for a solid on-the-fly encryption program that supports folders, virtual drives, or partitions, then you can count on spending from fifty to one hundred twenty dollars.

Concealing Encrypted Information

Encrypting your sensitive information is a good solution for maintaining the confidentiality of your sensitive data. Hiding it is another alternative, however, it does not provide as much security. Some programs enable you to encrypt and hide your information. There are two basic ways to conceal your encrypted files: change their file extension or use steganography.

By default, most file types have a unique extension to identify what type of file they are. If you see a file called mom.bmp, you would know it is a picture file. When you clicked on it, a picture viewer would start and then display the picture. Most encryption programs use a unique extension to identify their file type. This facilitates an attacker's efforts to find encrypted files and try to crack them. Many encryption programs allow you to change the extension of the encrypted files. As an example, you could change the extensions to .txt (a text file extension) and save the files somewhere you feel an attacker would not look for documents.

Steganography is the technique of hiding information within other information. Some encryption programs can encrypt information then blend it into picture files, sound files, and other types of files (see Appendix B figure 6 for an example). [10] This technique is a much stronger deterrent than simply changing the extension.

Concealing your encrypted information is a good precaution to take if you have highly sensitive information. There are a few disadvantages to concealing encrypted information. Both of the previously mentioned techniques create extra steps and time in the encryption and decryption process. Also, because the files are concealed, you will have to remember where they are. If you choose to use

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

steganography, you will have to have the appropriate types of files to insert the encrypted information into. Even though concealing your encrypted files adds an extra layer of security, many people feel the extra steps and time are not worth the increased security.

Backing Up Your Encrypted Information

If you use an encryption program that replaces files and folders with their encrypted versions**,** then it is simple to backup your encrypted files; just have the backup program copy the encrypted files to the backup destination. Your files will remain encrypted on backup media.

For on-the-fly encryption programs, the container file should be backed up. Because the container file contains the data in an encrypted format, the data will remain encrypted. The entire container file must be backed up, regardless of how many files were updated from your last backup. With that in mind, the backup media must have enough free space for the container file. There is another less secure way to backup files from a virtual file encryption system. You can mount your container files as drives and then backup selected files. This method is less secure because the backups will not be encrypted and must be secured in a secure location.

To back up an encrypted partition or drive, you must first unlock it. This will result in your backup saving an unencrypted version of your data. One advantage to this method is that you can choose which files you want to backup. Another thing to keep in mind is that if you have a backup program, it may have the option to encrypt the files as they are copied to the backup media. If you employ this technique, make sure that the strength of the backup program's encryption system is adequate for your needs.

Laws, Regulations, and Company or Business Partner Standards

Depending on what you plan to encrypt or to whom you plan to send the encrypted information to, you may have certain regulatory, company, or business standards that must be followed. Those rules could dictate what information you are and are not allowed to encrypt, what algorithms are allowed to be used, the minimum key size, the distribution of keys, the specific encryption applications that are approved, and more. Many companies have specific encryption products they use and specific standards that must be followed. [11] If you plan to use your encryption program for personal use, then you probably will not have any legal issues.

Finding A File Encryption Product that Is Right For You

Now that you are aware of many of the encryption features available and have identified the ones you need, you might be expecting to read about some recommended products. Encryption products are frequently updated with new features. In addition, new and better products are frequently available. Any product recommendations made today may not be you best option tomorrow.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

You now have the knowledge to choose the best product for your needs. The next step is to find a product that has the features you need.

I recommend you start by doing some research on the Internet. Most stores have a very limited selection of encryption programs. Second, you will most likely not find all the information you need about the product on the box. And third, unlike at stores, many encryption programs available on the Internet allow you to download a trial version. Trial versions typically disable some of the features the full versions have or they enable you to use all of the features but for a limited period of time, normally 30 days. If you use a trial version, make sure that you save an unencrypted version of any information you encrypt; once your trial period is over, if you chose not to purchase the program, you many lose the ability to decrypt the information you encrypted.

You can also try to find reviews for the products you are considering buying. I also recommend you check the vender's web site and see if they provide any kind of support. Some products support a wide range of operating systems however, not all the features work with all of them. You should ensure that the product and features you need are compatible with your operating system. If their web site does not provide the answers you need, then contact their marketing or support team. You can normally find those numbers on their web site.

Summary

Most of us know the value of our tangible assets. We lock our doors when we leave our houses. Some people take an extra step to protect their most valued assets by keeping them in a safe. You should understand the value of the digital information you handle, not only what it is worth to you, but also what it would be worth to others, and how much it would cost you if others obtained it. Encryption is a good solution to protect the confidentiality of your valued information. Now that you are familiar with the main features of file encryption programs, you should be able to effectively find a product that meets your needs.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References

[1] Mann, Charles C. “Where the Hell Is My Laptop?” Business 2.0 Mar.2001. URL: http://www.business2.com/articles/mag/print/0,1643,9294,FF.html (23 Nov. 2002).

[2] “Encryption: A History of Secret Communication.” URL: http://www.oli.tafe.net/library/guides/Sample%20Essay.pdf (23 Nov. 2002).

[3] Hart, Brian., and Michele Lombard. “Cryptography.” 14 July 2002. URL: http://starbase.trincoll.edu/~crypto/historical/enigma.html (23 Nov. 2002).

[4] Burnett, Steve., and Stephen Paine. RSA Security’s Official Guide to Cryptography. Berkeley: Osborne/Mc Graw – Hill, 2002. Page 32.

[5] “On-The-Fly Encryption: A Comparison.” 29 July 2001. URL: http://www.fortunecity.com/skyscraper/true/882/Comparison_OTFCrypto.htm (23 Nov. 2002).

[6] ‘Privacy Guide: Data Encryption.” URL: http://www.all-nettools.com/privacy/crypto.htm (23 Nov. 2002).

[7] Meserve, Jason. “DES Code Cracked in record time.” 20 May 1999. URL: http://www.nwfusion.com/news/1999/0120cracked.html (23 Nov 2002).

[8] Daeman, Joan., and Vincent Rijmen. “AES Proposal: Rijndael.” Document Version 2. 09 Mar. 1999. URL: http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf (23 Nov. 2002).

[9] Harris, Shon. All In One CISSP Certification Exam Guide. Berkeley: McGraw - Hill/Osborne, 2002. Pages 517-521.

[10] “Steganography.” URL: http://security.tao.ca/stego.shtml (23 Nov 2002).

[11] Bartman, Scott. Writing Information Security Policies . Indianapolis: New Riders Publishing, 2002. Pages 118-125.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix A

Ddcrypt is one of many freeware symmetric encryption programs. It was created by Miguel Garrido. For more information visit URL: http://home.nyc.rr.com/mgarrido/

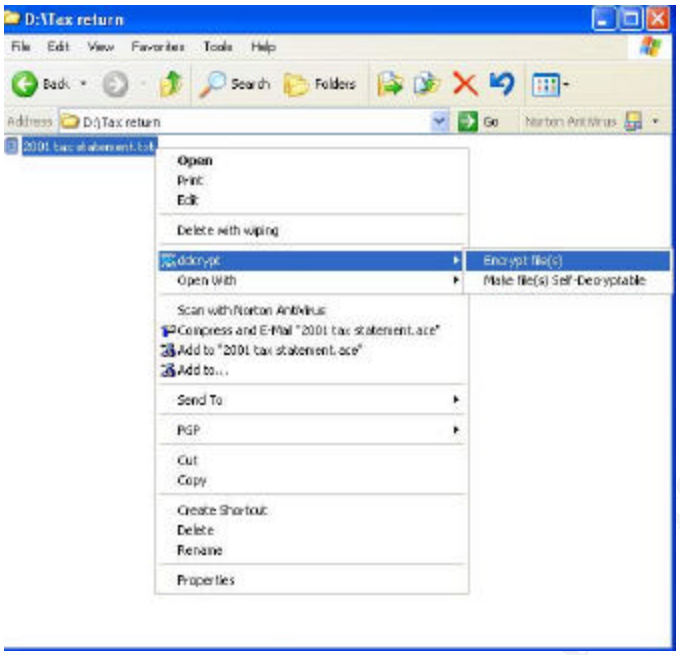

Figure 1

Figure 1 demonstrates how Ddcrypt, a freeware encryption program, enables you to right click on a file from the Windows Explorer and encrypt it.

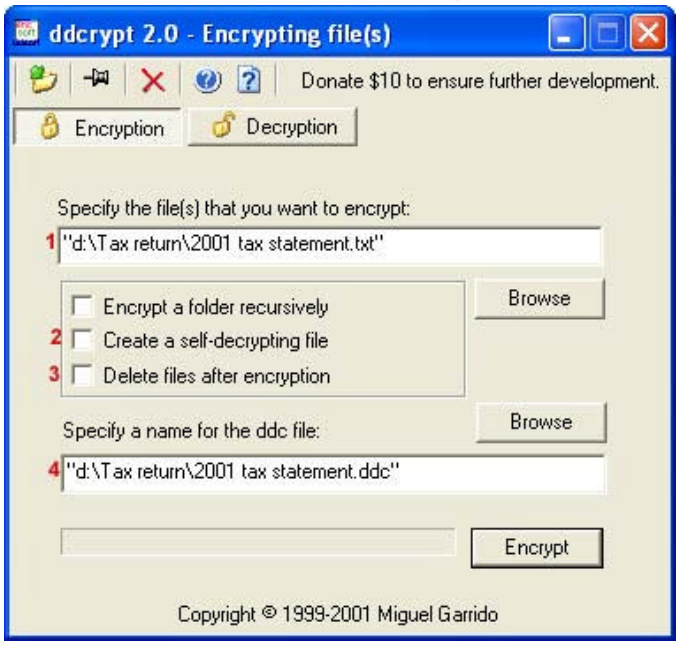

Figure 2

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 2 demonstrates the encryption menu from ddcrypt. Next to the number 1 is the file you intend to encrypt. To the right of the 2 you can see the option to create a self decrypting file. Next to the 3 is the option to delete the original file. Finally, next to the 4 is where you type the destination path and name of the file. By default, it uses the same path and name as the original file. However, it does change the extension to ".ddc". If you leave the extension as ".ddc" then you can decrypt the file by simply double clicking on it.



Figure 3

Figure 3 shows the decryption menu that appears when trying to decrypt an encrypted file with ddcrypt 2.0. If you do not enter a destination path it will save the decrypted version in the same location as the encrypted version. After selecting decrypt, you will be prompted to enter the decryption password.

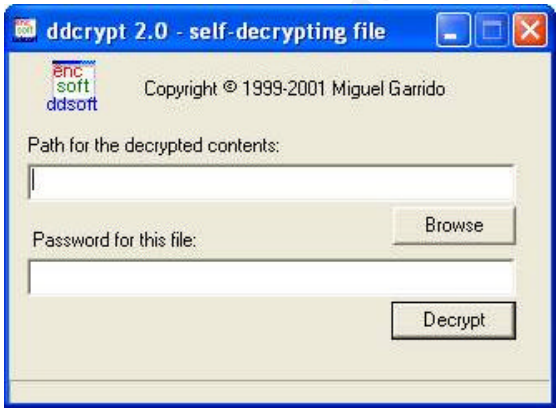

Figure 4

Figure 4 is a window that appears when running a self-decrypting ddcrypt 2.0 file. You will prompted for a destination path and password.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix B:
DriveCrypt is an on-the-fly drive encryption program available from SecurStar from URL: http://www.securstar.de/about.html
The following screen shots show windows used to configure a virtual drive.

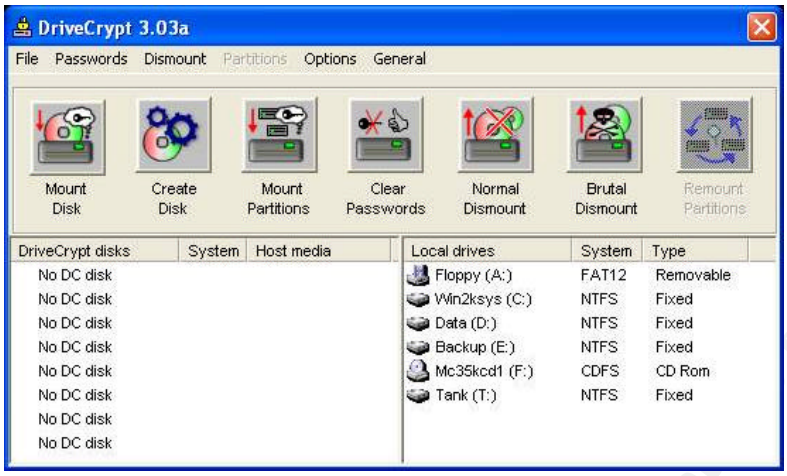

Figure 5

Figure 5 is the main DriveCrypt window.



Figure 6

Figure 6 is the first window displayed for selecting a new container. You can see that this program enables you to use steganography; you can hide the container files within 16 bit wav files.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

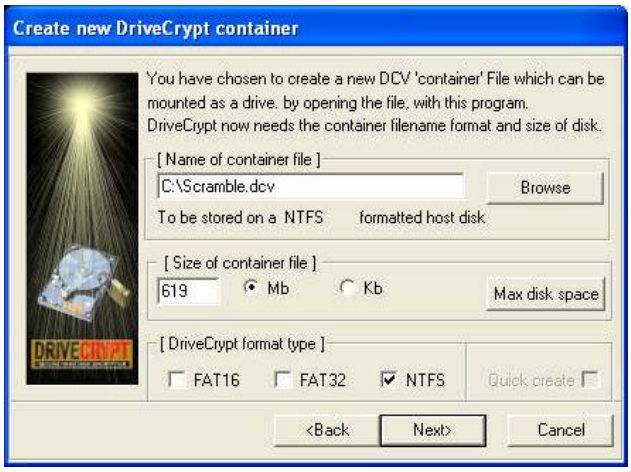

Figure 7

Figure 7 shows the next window in the process of creating a virtual drive. You must enter the destination location of the container, the size of the container, and the file system type. In this example, you can see that the size of the container file is 619 Mb. Once the virtual drive has been created, that will be the amount of storage space you will have. Also because the container is under 650 Mb, it can be backed up to a recordable compact disk.

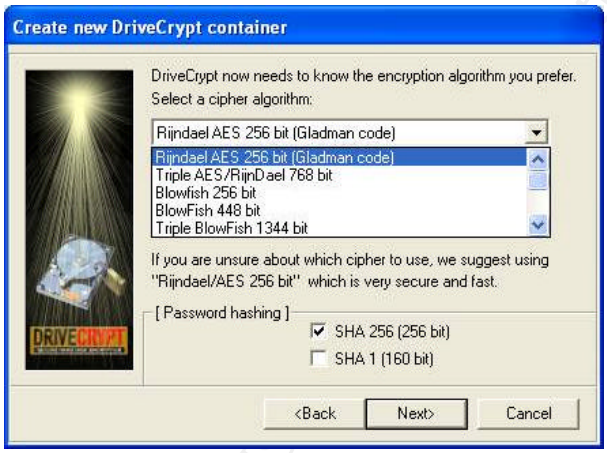

Figure 8

Figure 8 shows the next step, you must select an algorithm. Some encryption programs will let choose what algorithm you want to use. As you can see, this program has a large variety of algorithms to choose from.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



Figure 9

Figure 9 is the last screen in the process of creating the container file.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.