# Global Information Assurance Certification Paper

Name: Diego Zalles

Assignment: GSEC

Title: Data protection - Obtain Maximum protection without experience

September 10, 2003

Table of Contents

## 1. Introduction

What things should we cover when protecting the information? Generally when we think of protect our information, we only think in our documents. However, the protection of data involves many other factors. Some factors are: the protection of private information that can be stored for example, in the record of Internet that is available to the eye of any person that has access to our PC. Another factor to avoid is the shipment of our personal data by some programs, without our consent, to their power stations, providing them our private information. Lastly, another factor that very few people know, involves the elimination of our confidential files by special programs; because if we simply eliminate them with the recycle trash, these files won't really be destroyed and will be able to consent them with some programs that allow to recover the information, this can mean that private data stay available to third persons.

Knowing what the protection of information really involves, it is also necessary to know some concepts about the protection forms. This will allow to understand the grade of security that one can obtain, although we have not known until now, how the data can be protected.

As we have said the Encryption and the Steganography are among the concepts that we will revise. These are methods of data protection that work in the last layer of what we know as “defense in deep". By means of their use through some programs, we can increase the security of our information transfer and their protection in disk.

Although in Internet we can find an enormous quantity of programs of encryption and steganography, we will analyze the Steganos Security Suit, because it is a program that has a big number of the factors that involves the protection of information and that also has a system of extremely simple handling.

The use of this program will only be with the purpose of demonstrating the easy way that it turns to protect our information, even if we don't have any knowledge. However, we can reach similar levels of security with other programs as: the Invisible Secrets, S - Tools, Blowfish97, etc.. Many of these programs, like Blowfish97, are freeware; this will allow us in brief minutes to get them of internet and to be able to increase substantially our security.

## 2. Encryption

When analyzing the necessary concepts to understand as assuring the information, we find the Encryption. This consists on modifying the understandable content of our information to a content without logical meaning or with a different meaning to the one we want.

Along the history, many forms have existed of carrying out the encryption (encoding) of the information and these techniques have been used broadly all over the world for diverse causes. The encryption form in its beginnings was developed manually and it could be carried out by different forms among which are: substitutions for rotation,

arbitrary rotations and exchanges. However, existed the problem that these systems were very vulnerable to be decoded. (If you want to know more about the old forms of encryption visit http://www.htmlweb.net/seguridad/cripto/cripto_2.html ).

The following step for the encoding of messages was to use keys. This consisted on choosing a word or any sentence and with this, a womb was developed that would have as columns the number of letters of the key (word or sentence) and the lines of the womb were formed according to the text that were encrypting. In this way, the first line of the womb was occupied by the key that we have defined and starting from the second line the text to encrypt was taking its place, going down to the following line every time that you ended up occupying the last column of the line. After this the form of the womb got changed. A way to make it was to change the order of the columns that we have in the womb, for example, ordering it alphabetically according to the word that we had in the first line. Then you replaced the lines of the womb putting them as columns and at last you proceeded to read the womb with their new order.

If we wanted to decrypt the text, the only thing we had to do was to carry out the process in an inverse way and it was ready.

By means of this encryption form the term “encoding key” arises, which refers to the word that we are using to code the information. Besides that the term “longitude of the key” arises and comes to be the long of the word that we are using to encode.

Currently the encryption systems are based on the system of keys that we have explained previously together with mathematical processes that allow to carry out the encoding in a quicker and surer way. We know these processes with the name of “encryption algorithms”.

Finally, another important thing when carrying out the encryption, is to know that when we speak of the “plane text", we refer to the original state of the information and when we speak of “cipher text", we refer to our text after carrying out the encoding process.

### 2.1. Types of Encryption

There are two encryption types: The symmetrical encryption and the asymmetric one. For the handling of the software that we will analyze we will focus ourselves in the symmetrical encryption.

The symmetrical encryption uses a key (secret word) to carry out the encoding and the same key to decode, that is to say, at the encryption moment, the person chooses a password. His information gets encrypt with that password and when he wants to decrypt, he uses the same password that defined in the encryption to obtain his plane text.

## 2.2. Algorithms of Encryption

As we have already explained previously the encryption algorithms are the processes that by a system of keys and mathematical calculations, allow us to carry out the encoding of the information.

Every day are more the algorithms that we can find and the security that they offer depends overall of the size of the encryption key that they offer.

The key of the encryption algorithms depends in its complexity and security of the bits number that it supports. It is as well as a key of 4 bits hardly supports 15 possible combinations to carry out, being this a very vulnerable way to identification intents by means of the brute force, that is to say, attempting all the possible combinations. Then, a key of 16 bits, allows 65535 combinations, there we see how the security increases notably and in this way, while the longitude of the key is bigger, bigger number of combinations it will exist and minor will be the possibility that the password will be broken.

Something that we don't have to forget, is that while longer is our password, surer will be the encryption. If we encrypt a document with such a simple password as the number “1357” even if the encryption algorithm that we are using has a key of 60 bits, our password can be easily broken and our information can be overdraft.

Now we will explain some of the most insurance and better known algorithms; among those are the AES and the Blowfish that are used in the Steganos Security Suit.

*2.2.1. Algorithm DES (Data Encryption Standard).* This algorithm was created originally by the IBM and it was adopted then in 1977 by the government of USA as standard of encryption for all the sensitive but not classified information (SBU). This algorithm calculates blocks of 64 bits by means of substitution and exchange using a key of 64 bits of which 8 are of parity.
Their main characteristics are that this algorithm is the more used in the world, easy to use and quick. However, this algorithm at the moment doesn't offer a lot of security due to its small key width and has been substituted for algorithms with more key size.

*2.2.2. Algorithm Triple DES.* This algorithm is replacing the algorithm that we saw before. In fact, Triple DES is the same DES but applied three times; this allows to achieve a key more difficult of deciphering, with a width that reaches up to 128 bits where 112 are the key and 16 are of parity.

Due to the strength that offers, this algorithm is used by banks to carry out transfers and also Visa and Master Card are incorporating it to their ATMs, with the purpose of avoiding the robbery of pin numbers.

*2.2.3. AES (Advanced Encryption Standard).* Algorithm developed by the Belgian scientists Vincent Rijmen and Joan Daemen. This algorithm, also well-known as Rijndael, was selected in October of the 2000 by the NIST (National Institute of

Standard and Technology) as the best standard of encryption. The Rijndael works with keys of 128, 192 bits and it even accepts longitudes until 256 bits and its encryption block that uses is of 128 bits. According to the NIST, to conquer this algorithm using a key of 128 bits, it would be necessary 149 trillions of years besides having to make it with an appropriate equipment.

For the security that offers, it is expected that this algorithm is quickly adopted for a wide variety of uses. Besides that as we have already mentioned, the program that we will analyze uses this algorithm for its encryption process.

*2.2.4. BlowFish.* This algorithm was developed by the company Counterpane Internet Security. Some of the characteristics that this algorithm has are: that it is compact, simple and sure. Its key is of 448 bits and the operations that it uses for the encryption are adding, the exclusive OR, and search the chart of partitions in operations of 32-bits. At the moment, Blowfish is one of the surest algorithms that exist and it is used in a big variety of packages like the PGPfone and the Nautilus.

## 3. Steganography

Steganography is the art of hiding the information. The word steganography derives of the Greek “steganos and graphy” that it means in its entirety, hidden writing. If we compare the steganography with the encryption, the difference resides in that the encryption is based in changing the content of the information for another content without importance for the reader, on the other hand, the steganography hides the information of the people view. In this way, with the encryption, any person can identify where is the coded information giving possibility to attempt decode the real information hidden, while with the steganography, they won't even be able to know that an information exists.

The same as the encryption, the steganography has being used in different ways through the history. An example is the use that was given during the Second World War, where the "micro point" was used to send secret messages that were photographed and reduced to the size of a point and were stuck instead of the point of the letter “i” in any message. In this way the message could travel without lifting any suspicion.

Currently in computation, the steganography is managed hiding the useful information in other messages that can be images or sounds, Steganos Security Suit, allows to carry out in both.

The form in which the information hides inside some image or sound is using the method (LSB) or the Less Significant Bit.

### 3.1. Steganography in Images

For the computer, an image is a womb of numbers that represent intensities of colours in several points; this is what we call “pixels". For example, the most common images that we have are of 640 X 480 pixels and 256 colours. The digital images are generally

stored in a quality of 24 bits, that is to say, 16.777.216 colours which is ideal to hide information. These images use 3 bytes for each pixel to represent a colour. The basic colours that represent these 3 bytes are: the red, green and blue. Now, if we take these bytes in decimal value, we have that each byte could go from a value 0 to 255 and as we combine these values among the 3 bytes we will obtain a colour tone. In this way, if we see a yellow pixel in the screen, it will be formed by a value 255 in the red byte, a value 255 in the blue byte and a value 0 in the green byte. On the other hand a pixel that we see orange will be formed by the values 255, 128, 0 in the bytes.

Each byte is formed by 8 bits, that is to say, in binary a byte would be for example the number:

10011000

Where the bit of the right end would come to be the (LSB) or the Less Significant Bit, that is the one that we will replace with the steganography for a bit of the information that we want to hide. For example, if our information to hide is the bit (1) what we have to do is to change the byte that we had 1001100**0** for the 1001100**1** where the Less Significant Bit that was zero has been replaced for one.

But why we replace the bit of the right end? We replace this bit because when we alter it the colour that we had is not much affected, on the other hand if we alter a bit that is more to the left the change that will suffer the colour would be much more notorious for our eyes.

Let see an example of this. Let say that we have a pixel that will be the navy blue colour that will be formed by the binary bytes:

00000000 01000101 10101010

Now suppose that we want to hide in this image the information that represents the bit (101) or number 5, then, using the steganography in this image we will change the less significant bit, what will give us as a result that the image now will be formed by the bytes:

00000000 01000100 10101011

In this way, if we compare the original colour that we had for the one that now we have we will notice that a perceptible change doesn't exist for our view.

Initial Colour

Colour with hidden information

On the other hand if we wanted to hide the bit (110) or number 6 and instead of using the method (LSB) or the less significant bit we changed the fourth bit of each byte we would have as a result the bytes:

0000**1**000 0100**1**101 1010**0**010

Here we can clearly notice the difference of colour that take place.

Initial Colour

Colour changing the fourth bit

This is the reason why the steganography carries out the change of the last bit of the right.

In this case and only for learning reasons we have supposed that the whole colour was a pixel, however in the real life the graph would be formed by many pixels where a lot of more information would enter.

Basically this is the form in which the "Steganos Security Suit" and many other programs carries out the insert of information in images and the type of files in which it allows to insert are: bmp and dib.

### 3.2. Steganography in Sound

The steganography in sound uses the same method that in the images, that is to say, replace the less significant bit in the original sound for the bit that corresponds to the information to hide. Steganos Security Suit also allows to carry out the insert of information in sounds and uses for this the format wav.

So much the information hidden in images as the information hidden in sounds, are very difficult to perceive for people, because when it is about images, only happens a very small imperceptible colour variations for the human eye, and when it is about sounds, the change in the sound is very insignificant for the human hearing.

## 4. The Synergy of the Encryption and the Steganography

We already saw the security that offers the encryption and we also saw the great security that offers the steganography. Now, as we know how strong are these two tools for separate, imagine the security that they can offer together. That is why we talk of the synergy of the encryption and the steganography, because if we occupy these tools individually, it is possible that somebody can obtain the information that we were trying

to hide. However, if we use the two together to protect, for example a document, we will be able to increase the level of security of our data making it almost impossible to decode.

The form how we achieve this synergy is, first encrypting the data to make it incomprehensible and then occupying the steganography to hide these data of the human view. The program that we will begin to analyze “Steganos Security Suit", always uses the steganography in combination with the encryption.

**5. Politics for the Protection of Information**

Knowing which techniques we can use to protect our information, it is time to see some politics that can help us to improve and at the same time to facilitate the installation of a security system.

One way that facilitates us the election of what to protect and allows us to take a better control of the information, is the establishment of specific politics regarding the protection that will be given to the data according to their grade of confidentiality.

For this we can use the classification created by the Department of Defense (DoD) from U.S.A., that differs the information according to the grade of sensibility that this has, this classification can be useful to identify the level of importance that our information possess and later on to adopt different protection measures for each grade of sensibility.

The classification is the following:

- Top Secret.- At this level corresponds the most critical information.
- Secret.- Very important Information and of high sensibility.
- Confidential.-Important Information and only consented by few people.
- Sensitive but Not Classified.- This information is stopped for the public but it can be consented by governmental agents, its also called “Only for official use”.
- Unclassified.- This information is open to the knowledge of every one but its better to have it in reserve.

In this way, after including our information in one of the categories, we could define for example, the use of sure units, encryption and steganography for the information that enters in the Top Secret or Secret classification; then for the information classified as Confidential or SBU (Sensitive but Not Classified), we can apply encryption and lastly the unclassified information can be managed with freedom.

Another politic could be, to define the form of shipment of electronic mail of high sensibility. For example, the use of PGP or other programs that assure us high security of our information when it is circulating in internet.

Another politic that we can adopt, is to use a password’s generating program for the definition of our secret word. Although, this is something that we can make it manually

without necessity of a program, we generally define as passwords words that are very common, simple or short; this causes that our password will be very vulnerable and easy to identify. On the other hand, the advantage of using the programs that generate passwords is that they allow us to create passwords of a certain size of bits, so that we can define and know the security that this will offer us. They also generate passwords choosing the characters in a random way and the result is a concatenation of letters without sense that are a password of high security.

## 6. Steganos Security Suit

To begin the steganos analysis, first we will see their installation process. After acquiring the product, we should proceed to install it in our computer. The form is simple, the only thing that it is necessary to carry out, is to follow the “wizard” that the program offers, where the only options to choose are: the selection of the language and the unit where we want to install.

After carrying out the installation and when beginning the program, it leaves us a window that allows the access to all the tools that we have available. The configuration and help options are in the inferior part of the screen. In the configuration, the program allows to change some options of the different tools that provides us; in the help option, the program offers all the information of the company, technical attendance and functions that it has.

Let us pass to see the diverse tools that the program offers us, tools that are very easy to use and that allow to protect us in many fronts, for example: in the transfer of information through the electronic mail, in the storage of the information in our hard disk, in the handling of data in portable storage units as cd rooms and in the elimination of private information that can be stored in our computer. In this way, as the same program informs, steganos allows us to protect our data, so much of simple curious, as of spies in our own office and even of computer pirates.

### 6.1. Tools that offers

Steganos Security Suit version 5, offers seven tools to maintain sure our information. What we can find is:

*6.1.1. Safe Steganos.* This is an innovative system that works like a virtual unit that can be hide of the people view and when you proceed to hide the data that are inside this unit the data is encrypted allowing to maintain our information invisible to people and also coded. Every time that we open or close the "safe", the program decodes or codes the data respectively in real time in a very speedy way, being able to carry out the encoding of 1.2 gigabytes in only one second.

The program gives us the option of create 4 “safes”, which have a capacity of 1.2 gigabytes each one. The way to create the safes is simply entering to the tool "safe", choosing the option "create" and then we only chose the name that the unit will have, the letter that will correspond to that unit and the password that we will define to open

that unit. In this way after creating our secure unit, we will be able to consent to it entering to the program Steganos Security Suit, choosing the tool "safe", and pressing in the option "open". There we introduce our password we accept and then we only select the option "show" which will allow us to see our secure unit in the list of units of the windows explorer, this occurs when we enter to My PC. Starting from that moment the secure unit is managed like any other partition of the system, allowing us to create folders, to keep documents, to open documents, etc… Then, in the moment that we decide to protect the information that is contained in the "safe", the only option to carry out is to enter to the Steganos Security Suit, choose the tool "safe" and there we press "close" in the "safe" that we want to protect. At that moment our information will be encrypted and will get lost of the list of units in the windows explorer.

Some points that are necessary to take care and that the program recommends are that before closing the secure units we have to close all the files that we have opened because if we want to close a unit with open files, the unit won't close. Another important thing is that we should not install programs in the secure units, because the application can be damaged if we execute the programs when the secure unit is closed.

*6.1.2. Steganos Portable Safe.* It allows to transport information in a sure way creating mobile safes in CD, DVDs, or other storage supports, in this way the contained information travels encoded. This information can be consented only by us from any computer with the access password without being necessary to have installed the Steganos program. This interesting protection system, allows us to transport big quantities of sensitive information in a sure way eliminating the problem that would bring us the loss of the storage support.
The way to create a “portable safe” involves, first to choose the support type where the information will stay, then we have to define the folder for the files of the safe portable package, that are the files that will be recorded in the elected support. Next comes the definition of the password which let us be able to open the portable secure unit. Then a letter is chosen for the momentary partition that will carry out the preliminary packed of the files. In this way, a new unit is created, where is introduced everything that you want to copy, and lastly we only have to begin the recording program and to copy to the storage support the files of the package.

*6.1.3. Mail encoding.* The shipment of sensitive information by electronic mail is one of the most vulnerable things referring to security.

Steganos and many other programs offer a codifier of electronic mail. The way that Steganos works, is that when we enter to the tool “Mail Code", a window is open with 3 options and a space to write the mail. One of the options that presents, is “add file". This option let us attach the file that we want to send. The other option is to "save coded"; this allows us to save what we have written and the attached files in a encrypted form so we can send them later by e - mail. To have this done, the program asks us to choose a password that will be the key that will be used to decode the file. The last option that presents is “Send coded”; this option allows to encrypt the attached files and the written text sending the electronic mail immediately. For this last option it is necessary to have the appropriate configuration in the application of the electronic mail.

*6.1.4. Files administrator.* This tool presents several options, first it allows us to encrypt or hide a file or allows to open a file encrypted or hidden to reveal its content. When choosing the option "new" it is only necessary to look for the document or file to encode and to load it with the option "add file" or “add folder", depending on what we want to do and then choose the option “keep and close". When choosing “keep and close” the program asks us if we want to code or to hide, when choosing “encode” the program will only carried out the encryption of the file. However, when we choose ”hide” it will use the steganography and the encryption together. If we put “encode” we will have to choose a file name with that the encoded file will stay and also will be necessary to choose a password with which the file will be decoded, after carrying out this, the program creates a file with the extension ".sef " that will be our encrypted data.

If we choose the option “hide” (which is the recommended) the program will ask us choose a file porter, this will be the image or the sound where the information to hide will be camouflaged. There are 3 forms of defining a file porter.

1) Let the program find the files porters that are in our hard disk. In this way we define in what partition to look, what type of files can look (sound, image or both) and then it will give us a list with all the files that were found so we can define the one that will serve us as porter.

2) Create a new file payee. To use this system, if we want to create an image like file payee, we will need to have a scanner compatible with TWAIN and if we want to create a sound like file payee, we will only need to have a microphone installed. In this way if we want to hide information in images and we have a scanner, we choose the entrance device and we press “scan”, later we define a password and our file payee will be already created. If we want to hide information in sounds and we have a microphone, we only have to record something in the sounds recorder that we open when we press create a file of sound, then we define a password and we will already have our information hidden and coded.

3) The last way is simply selecting a sound file or existent image. In this way we search for a image or sound manually in our units, we select it, we define a password and it is ready.

It is necessary to notice that when we hide our information the files payees don't change for anything, that is to say, if it was a sound, we can press on it and listen what we always listened, The same with an image, if we open it, we will see the image that we always had before the image becomes a file payee. In this way, it is almost impossible that other people can find the place where the information that we hide is. On the other hand, when we only encode the information, a file is created with an extension ".sef" this file will have the information encrypted. Now, if we change the extension of this file for "txt" or if we open it with the Microsoft Word, the text that will come out will be incomprehensible and a text that says "Steganos Encrypted File" will also come out. This allows to a "third people" understand that they are trying with coded information and in this way they will try to give with the information that we hide.

*6.1.5. Password Manager.* This tool is good for store all our passwords in one place, maintaining them encrypted and allowing us to create a different password for each service that we use avoiding the problem of forgetting them or writing them in some place that is vulnerable. This system allows us to give a high complexity to our passwords, protecting ourselves better of the attacks. In this way, we only have to remind the entrance password to the “Password manager” and from this place we will manage all our other passwords.

Although, this system is good when we speak of creating passwords that take advantage of all the width of encryption key and maintain them in a sure way without the danger of forgetting them, the security that offers is relative because if somebody gets the access to our computer and it is able to decipher the password of our “Password manager”, all the passwords that we manage will be overdraft causing us an enormous problem. Although, the use of programs administrators of passwords is not very recommended, the utility that these can have, as in the case of the Steganos, it is the option that brings us to create a random password with a define complexity, allowing us to know the security that will offer.

The way to create our random password is entering to the "Password manager", choosing the option "add" and in the screen that opens up we choose "create password". When we choose this option, it will leave us another screen that allows to notice the characteristics that will include our password. These characteristics are: number of characters that will have, the use of numbers, special characters, lowercase, and uppercase letter. While more options are selected and bigger is the number of characters that we use, the number of bits that will have the resulting password will increase, allowing us to create a password until of 630 bits.

After choosing the options that the password will have, the program shows a window that indicates us to move the mouse, when carrying out this action, the aleatory characters will be generated and will form our password. Once generated, this window will close and our password will be created with the complexity that we have chosen.

An interesting characteristic of the program, is that when we define the options that our password will include, the program tell us how sure it will be, for example: with a password of 630 bits the program tells us that the password offers maximum security and it can not be decoded by secret services, with a password of 126 bits will says that it can not be decoded by professional pirates that use a big group of computers. With a password of 63 bits will says that it can not be decoded neither by experts in programming, and lastly with a password under 9 bits Steganos says that it doesn't offer any special protection.

*6.1.6. Internet Trace Destructor.* This tool allows to eliminate all the information that is generated when we use the computer even when we are connected or not to the internet.

Among the things that allows us to eliminate are: The list of documents used recently, the list of the files searched recently, the list of applications used recently, the content of

the recycle trash, cookies and record of internet explorer, temporary files of internet, cookies, record and cache of netscape 6.

There are two ways to carry out the elimination of this information: "Complete overwriting" that only makes a faster erase of the information overwriting once. And "Repeated overwriting" that makes a slower erase but surer overwriting several times, avoiding that the data can be recovered with special programs. For this last elimination form Steganos Security Suit uses the standard of the Department of Defense of U.S.A. (DoD 5220.22 - M, NISPOM 8 - 306).

Also for Windows XP Steganos offers an option called "Anonimity XP", this option allows to avoid the flow of some personal information that we have and that is correspondent to Microsoft.

Among the things that can be disabled are: The transfer of data from the windows media player, the send of registration errors, the function of control of updates and some other things.

*6.1.7. Shredder.* This last tool allows us to delete information in a sure way so that can not be recovered with special programs.

The way to manage it, is entering to the "Steganos Destructor", adding the file or folder that we want to delete and choosing the option "eliminate". The "Steganos Destructor" also allows to carry out the erase in the two ways that we comment previously, that is to say the "complete overwriting" and the "repeated overwriting".

As we see, the program let us use a big quantity of very useful tools and in a very simple way but with a very high level of security thanks to the algorithms that it uses for the encoding of the data.

### 6.2. Algorithms used by Steganos

The program in its version 5.06 uses two algorithms that at the moment are the algorithms that offers the maximum security and that can guarantee a practically total protection before any event.

The first algorithm and the more used by Steganos is the AES. As we have explained previously it is the new standard of code of data adopted by the NIST that offers a key of encryption of 128 bits. This algorithm is used by Steganos in their "safe", in the encryption of the electronic mail, in the encoding of files and in the password administrator.

The other algorithm used by Steganos is the Blowfish, an algorithm that can reach a key of encryption of 448 bits and that it is used with the steganography in the process of hiding the information in images as well as hiding the information in sound files.

## 7. Conclusions

After seeing tools so useful as the encryption and the steganography that allow us to establish a quite strong protection, it is important that we look for a program that takes a big advantage of these tools. Like we saw, the way of finding a good program will be analyzing the tools that offers and mainly the encryption algorithms that occupies in the use of these tools. This will tell us the level of security that we will be able to expect from this program and in this way to see if it is useful for our necessities.

Another thing that we should not forget is the determination of the politics that we will use when managing sensitive information and that will allow us to transfer our information among authorized people without the danger that it falls in the hands of unauthorized people.

At last, we don't have to forget that the analysis that we have made is to achieve a bigger protection of the data when other people have the possibility to consent to these. However, it is also important that we establish a wider system of protection that embraces the security of the machine or the machines in the net, in internet and physically. This type of security can be obtained by means of the installation of firewalls, IDS, physical security (protection against people and disasters) and other systems that will be able to diminish the vulnerabilities and to offer us a surer atmosphere of work as much in our home as in our office.

## 8. References


[1] Sánchez Arriazu Jorge. “Descripción del Algoritmo DES”. Diciembre 1999

[2] Wolf Gunnar. ”Llaves secretas o simétricas”. 15 diciembre 2000.
URL: http://www.gwolf.cx/seguridad/pki/node3.html (8 Jul 2003)

[3] Hally John. “Steganography: What’s the real risk?” GSEC Practical Requirements v.1.2f URL: http://www.sans.org/rr/catindex.php?cat_id=54 (24 Jun 2003)

[4] Ardita Julio, Caratti Mariana, Do Cabo Roberto, Giusto Mariel, Isar Guido, Pagouapé Matías, Schellhase Livio, Stavrinakis Florencia. Investigación en informática “Steganografía”. Universidad John F. Kennedy. Buenos Aires Argentina 1998.

[5] Moreno Luciano. “Criptografía”
URL: http://www.htmlweb.net/seguridad/cripto/cripto_2.html (7 July 2003).

[6] Moreno Luciano “Criptografía”. DES and Triple DES
URL: http://www.htmlweb.net/seguridad/cripto/cripto_7.html (7 july 2003).

[7] José de Jesús Angel Angel. “Sobre la longitud de las llaves de acceso a un sistema”.
URL: http://www.htmlweb.net/seguridad/varios/longitud_claves.html (7 july 2003).

[8] Silman Joshua. “Steganography and Steganalisis: An Overview”. Gsec 1.2f. Agosto 2001 URL: http://www.sans.org/rr/catindex.php?cat_id=54 (24 june 2003).

[9] No author. 2.1 SANS Security Essentials IV : Secure communications SANS Institute (2003).

[10] Trosky`s. “Algoritmos basados en llave”.
URL: http://www.geocities.com/troskysinc/algo.html (2 July 2003).

[11] GBM (General Business Machines). “Triple DES Nuevo Estándar de Encriptación”.
URL: http://www.gbm.net/bluetech/Edicion17.5/tripledes (27 June 2003).

[12] EuroLogic Data Protection Systems. “Algoritmos Simétricos”. Barcelona 2003
URL: http://www.eurologic.es/cifrado/simetric.htm#des (2 July 2003).

[13] Neil F. Johnson. “Steganography”
URL: http://www.jjtc.com/stegdoc/sec202.html (8 July 2003).

[14] Steganos GmbH. URL: http://www.steganos.com/es/sss/info.htm (20 June 2003).

[15] Microsoft TechNet. “Comercio Electrónico”. Microsoft Corporation 1999.
URL: http://www.reduy.com/computacion/ms-com-electronico/technet-4.htm (15 July 2003).

Last Updated: May 29th, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| SANS San Francisco Summer 2017 | San Francisco, CA | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| Security Operations Center Summit & Training | Washington, DC | Jun 05, 2017 - Jun 12, 2017 | Live Event |
| SANS Houston 2017 | Houston, TX | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| Community SANS Ottawa SEC401 | Ottawa, ON | Jun 05, 2017 - Jun 10, 2017 | Community SANS |
| Community SANS Portland SEC401 | Portland, OR | Jun 12, 2017 - Jun 17, 2017 | Community SANS |
| SANS Secure Europe 2017 | Amsterdam, Netherlands | Jun 12, 2017 - Jun 20, 2017 | Live Event |
| SANS Rocky Mountain 2017 | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Charlotte 2017 | Charlotte, NC | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | vLive |
| SANS Minneapolis 2017 | Minneapolis, MN | Jun 19, 2017 - Jun 24, 2017 | Live Event |
| SANS Columbia, MD 2017 | Columbia, MD | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS Cyber Defence Canberra 2017 | Canberra, Australia | Jun 26, 2017 - Jul 08, 2017 | Live Event |
| SANS Paris 2017 | Paris, France | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS London July 2017 | London, United Kingdom | Jul 03, 2017 - Jul 08, 2017 | Live Event |
| Cyber Defence Japan 2017 | Tokyo, Japan | Jul 05, 2017 - Jul 15, 2017 | Live Event |
| SANS Cyber Defence Singapore 2017 | Singapore, Singapore | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Minneapolis SEC401 | Minneapolis, MN | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| SANS Los Angeles - Long Beach 2017 | Long Beach, CA | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Phoenix SEC401 | Phoenix, AZ | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| SANS Munich Summer 2017 | Munich, Germany | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Mentor Session - SEC401 | Macon, GA | Jul 12, 2017 - Aug 23, 2017 | Mentor |
| Mentor Session - SEC401 | Ventura, CA | Jul 12, 2017 - Sep 13, 2017 | Mentor |
| Community SANS Atlanta SEC401 | Atlanta, GA | Jul 17, 2017 - Jul 22, 2017 | Community SANS |
| Community SANS Colorado Springs SEC401 | Colorado Springs, CO | Jul 17, 2017 - Jul 22, 2017 | Community SANS |
| SANSFIRE 2017 | Washington, DC | Jul 22, 2017 - Jul 29, 2017 | Live Event |
| SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style | Washington, DC | Jul 24, 2017 - Jul 29, 2017 | vLive |
| Community SANS Charleston SEC401 | Charleston, SC | Jul 24, 2017 - Jul 29, 2017 | Community SANS |
| Community SANS Fort Lauderdale SEC401 | Fort Lauderdale, FL | Jul 31, 2017 - Aug 05, 2017 | Community SANS |
| SANS San Antonio 2017 | San Antonio, TX | Aug 06, 2017 - Aug 11, 2017 | Live Event |
| SANS Prague 2017 | Prague, Czech Republic | Aug 07, 2017 - Aug 12, 2017 | Live Event |
| SANS Boston 2017 | Boston, MA | Aug 07, 2017 - Aug 12, 2017 | Live Event |