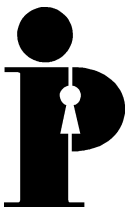
Information
and Privacy
Commissioner/
Ontario

E-mail Encryption Made Simple



Ann Cavoukian, Ph.D.
Commissioner
August 1999

The IPC gratefully acknowledges of the work of Mike Gurski for his contributions to this paper.

The IPC would like to give a special note of thanks to Jim Heath, of Viacorp, an Australia-based communications firm, for giving freely of his time and expertise in reviewing this paper. Mr. Heath has provided guidance to both the private and public sectors on e-mail security.

This publication is also available on the IPC website.

Cette publication est également disponible en français.

Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

Table of Contents

E-mail Encryption Made Simple[1]

Introduction

Does it really matter who reads your e-mails? If the answer is no, then e-mail encryption could be a potentially cumbersome luxury. However, if you e-mail sensitive, personal, or business information, then encryption is likely a necessity.

Unless you have been a meditating hermit for the last few years, the media has bombarded you with the woes of sending unencrypted e-mail.[2] Still, 99% of all e-mail traffic travels over the Internet unsecured.[3]

An unencrypted e-mail can bounce from Toronto to Brussels to New York. It can go anywhere for that matter. It all depends on the state of Internet "traffic" that day. An e-mail message can pass through numerous different computer systems en route to its final destination. Meanwhile, on some computers through which that e-mail is relayed, there may be 'sniffers' or other malicious software tools. They are waiting to copy, alter or tamper with that e-mail in some way. Some are looking for key words or names. Other sniffers are watching for credit card numbers or login passwords.

Those people who use some form of encryption system relax comfortably at their keyboards. Nonetheless, they feel a cold chill each time someone reports a new security hole. Some holes are found in the encryption tools. More often though, the application that uses the encryption tool has bugs. Internet browser applications are prone to this due to their large size and complexity. While the cryptographic component might remain secure, back door bugs to the application can nullify the value of the e-mail encryption.

Users of Netscape Communicator and MS Internet Explorer have felt a few cold chills since both browsers were e-mail encryption enabled. Communicator 4.0 had a bug that allowed Web sites access to information from the hard disks of visitors. More recently, Explorer 5 had flaws that allowed Web hackers to access files on a person's system.[4]

---

[1] Einstein is reputed to have said, 'Make things as simple as possible, but not simpler than possible.' This paper follows Einstein's adage.

[2] www.wired.com/news/news/technology/story/20481.html

[3] E-mail Privacy, Dave Kosiur, Help Channel ZDnet.

[4] www2.pcworld.com/news/daily/data/0697/970618170431.html and www2.pcworld.com/heres_how/article/0,1400,10579,00.html

The Information Privacy Commission (IPC) does not endorse the products or services associated with sites listed in this paper, nor does it guarantee the information provided by the sites.

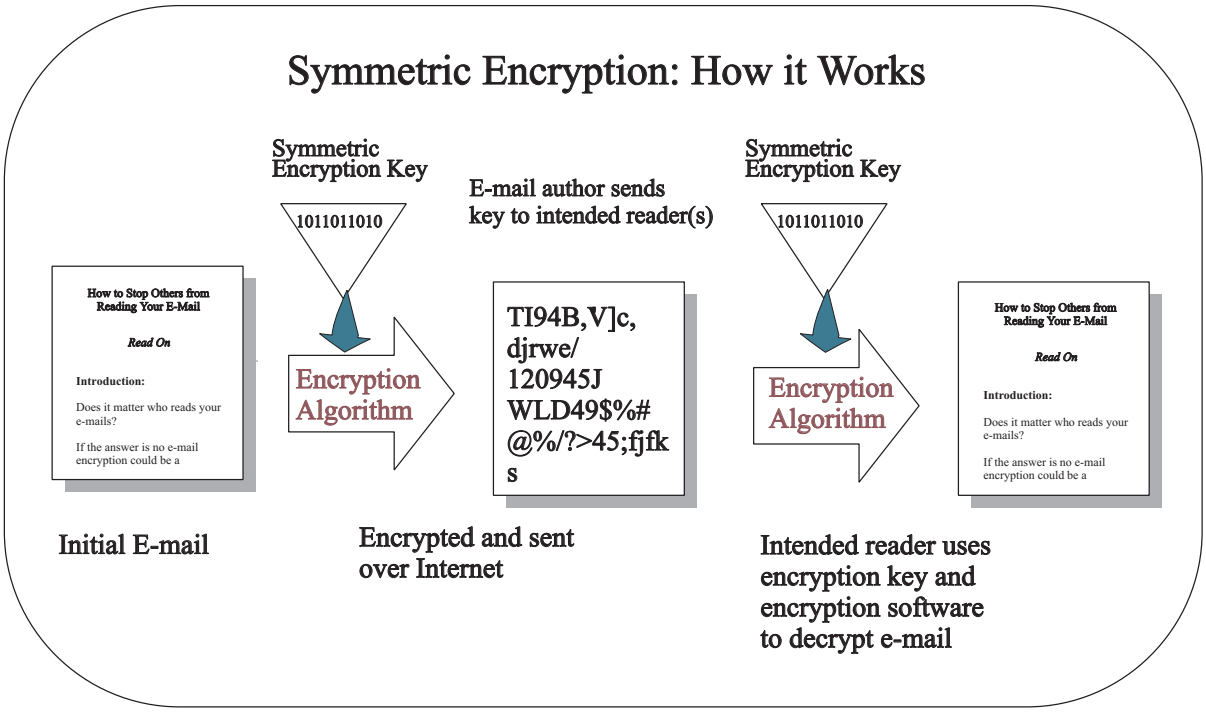
What is E-mail Encryption and how does it work?

It seems that every day, a new e-mail encryption product hits the market. Each claims to have the strongest encryption algorithms and guarantees attack-proof security. Before an individual or organization decides to purchase or use a product, undertaking some fact-finding and analysis is necessary. This paper is not a substitute for that fact-finding but will point toward some next steps.

There are more than 800 encryption programs currently available. Programs range in 'quality.' Some are secure (those that third parties have tested and could not break). Others are weak (those that can be broken in a few seconds by 'someone in the business'). Finally, there are the dangerous products (the untested).

Symmetric-key Encryption

At the heart of symmetric encryption programs are cryptographic keys. The key is nothing more than a binary number of 1's and 0's (e.g., 11001010110101000111001). The author creates a 'passphrase.' The encryption program in turn creates the key based on the passphrase. The 'key' will be used to both encrypt and decrypt the e-mail in a 'symmetric key cryptography program.' That means the intended receiver (and no one else) needs to receive a copy of the passphrase by other secure means. The encryption program uses that key to scramble or encrypt the e-mail's contents. The number of symmetric encryption programs is legion. A few include: PKZIP, BLOWFISH, DES, and IDEA.



Of course, if the author never changes the key for all ensuing e-mails, there could be problems. The author could make those problems worse if the passphrase is little more than a word or string of words. A few seconds with a dictionary-based hacking tool will crack that system. That is why authorities urge authors to create long, complex passphrases with upper and lowercase numbers, letters and keyboard characters. Nevertheless, how does the author of the e-mail get that passphrase to the intended audience securely?

Asymmetric Encryption

In 1976, Whitfield Diffie teamed with Stanford professor Martin Hellman. Together they devised what experts greeted as the most important development in cryptography in modern times. They produced a system that allowed people to communicate with total privacy. A year later, a group at MIT used the Diffie-Helman theory and launched RSA (named after Ron **R**ivest, Adi **S**hamir, and Leonard **A**dleman). RSA brought asymmetric cryptography to the public. (The British Intelligence community had invented it years before but had not shared it publicly.)[5]

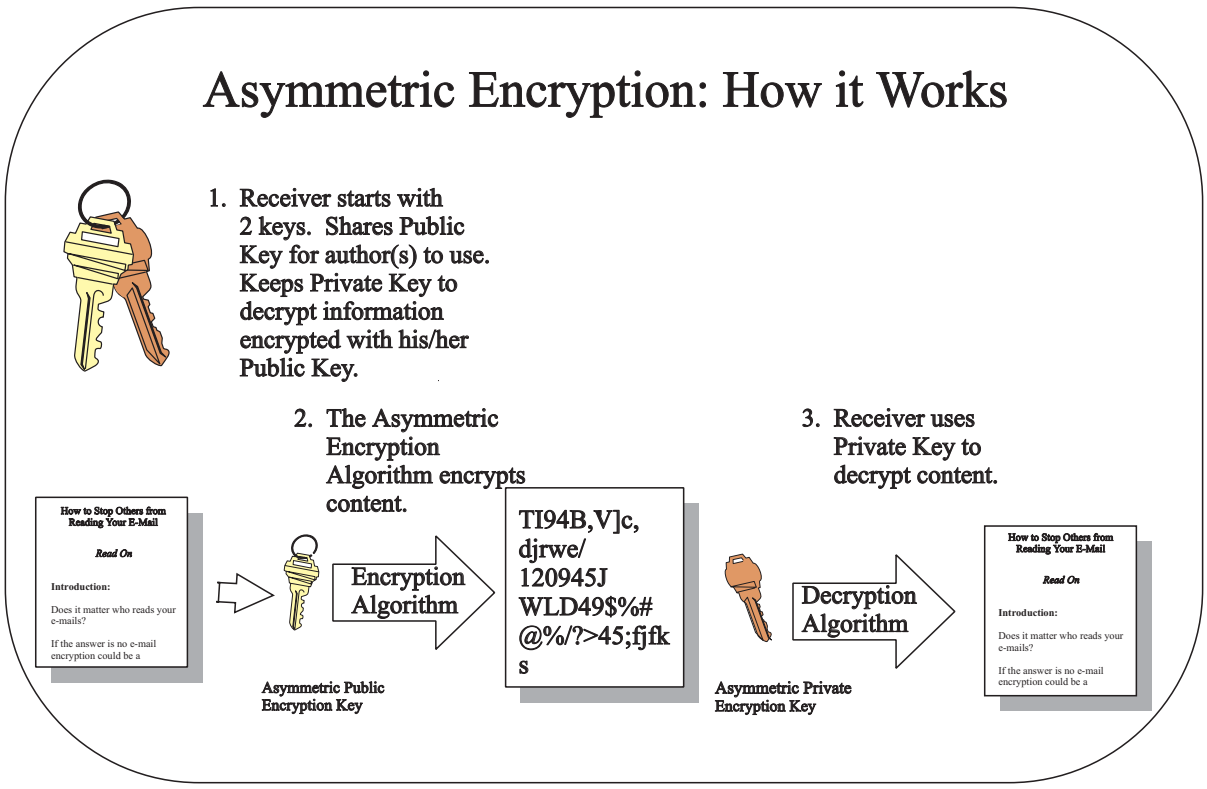
RSA software can generate a pair of keys that could be used to either encrypt or decrypt a message. Each key is a large integer. The two integers are mathematically related in a special way. Either key can be used by the encryption software to encrypt a message. The other key is used later to decrypt the message.

The reader can share one key, called the public key, with intended authors. The reader's private key remains just that: private. Once an author receives the reader's public key, the author can use the public key to encrypt information. The author can then send the encrypted e-mail. The reader can then decrypt the author's e-mail with his/her own private key. In other words, the author encrypts information using the intended reader's public key. The reader then decrypts the information using his/her private key. This concept always makes people blink at first. (See diagram on next page.)

Asymmetric encryption overcomes the problem of having to share the same key whereas symmetric key encryption requires it.[6] Asymmetric encryption made a breakthrough. However, it is a labour-intensive encryption process for computers. Using it to encrypt and decrypt all of a person's e-mail traffic would bring the average PC into submission.

[5] www.wired.com/wired/archive/7.04/crypto.html

[6] www.viacorp.com/crypto.html and www.rsa.com/rsalabs/faq/index.html



Common practice in most encryption applications today is to use asymmetric encryption to 'wrap' or encrypt only a symmetric key. The key is chosen at random, and the program generates a new one for each message. Remember that the symmetric key is used to encrypt the e-mail. The intended reader of the author's encrypted e-mail can then decrypt the symmetric key using the reader's own private key. Now, the symmetric key decrypts the e-mail. Thankfully, the encryption program does all this in the background so you do not need to remember 300-digit prime numbers or work with long binary sequences.

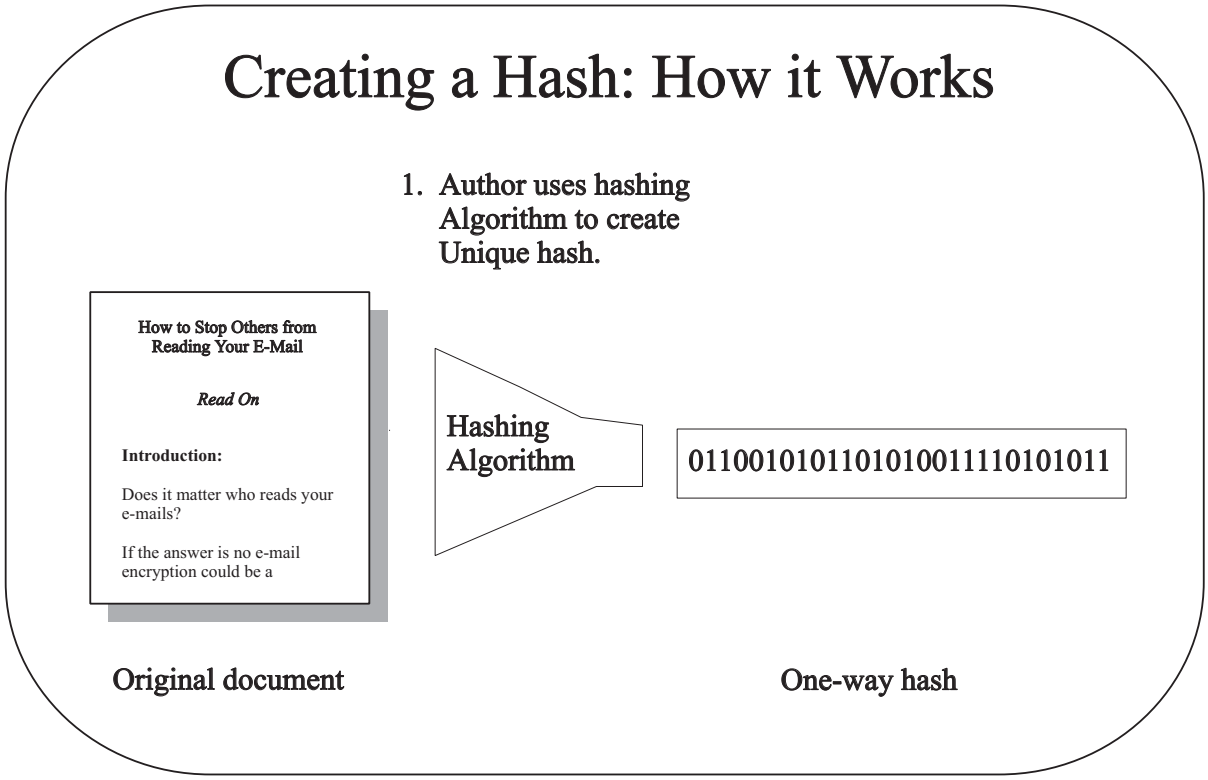
Digital Signatures

Most e-mail encryption tools have another element. On top of the encryption algorithms, they add a digital signature. The digital signature assures the e-mail's reader that no one tampered with the message and that it did in fact come from the author.

To do this, a digital signature combines two pieces of information: a hash and the author's private key. First, let's talk about the 'hash.' The software creates the 'hash' which is a sequence of numbers (ones and zeros) unique to the author's message. The software does this by first scrambling the message. Think of it like making scrambled eggs and hash browns, mixed up together in the frying pan. Then the software crunches the scrambled mess down, digitally that is. Now think of scrunching the scrambled eggs and hash brown potatoes into a small egg cup. That's the hash: the stuff that made it into the small egg cup.

The encryption software can only create one possible hash from an original message. However, there could be other messages that end up creating the same hash. Still, finding those other messages is virtually impossible. Though improbable, a person could find a different message that creates the same hash. That other message would most likely be gibberish.

This hash cannot be reverse engineered (that is why they call it a one-way hash). The digital hash is just like the scrunched up hash in the egg cup. There is no way to go backwards. The hash cannot go back to the eggs in their shells and the unpeeled potato. So no one can use the digital hash to find out what the message is, nor can it be used to create a different message resulting in the same hash. The common length of the hash is 128 bits.

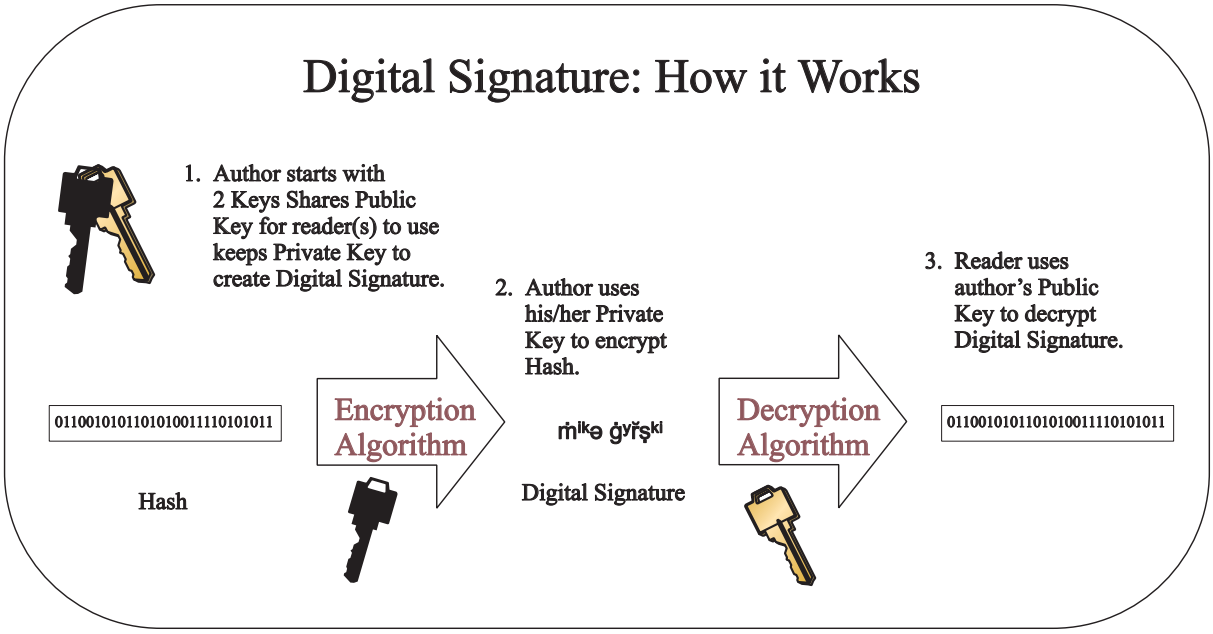


The second step is to encrypt the hash. The author encrypts the hash using his/her private key. Voilà: a digital signature. The reader can decrypt the encrypted hash using the author's public key. The intended reader's encryption software checks to see if the author's message creates the same hash. That ensures that no one has altered the message.

The digital signatures work the opposite way to ordinary messages. The author encrypts the outgoing hash with his private key. Then the author sends out his/her public key to allow readers to verify the hash is right. The reader would also know that only the author could have initially encrypted and sent the e-mail. Only the author has the private key that will make that system work. The weak link is in the complexity of the keys that a user creates. A safe bet is to have keys with a minimum of 230 digits.

Increasingly, e-mail encryption is becoming part of a suite of services that are transparent to the user. These products target private and public sector organizations rather than individual users. To use these systems, 'users don't need to know anything about security.' Most importantly, they need not remember those 230 digit keys.

However, an organization's decision-makers do need to know a few things. For a start, they need to remember that encrypted traffic cannot be scanned for viruses at the firewall or the anti-virus application level. That applies to encrypted e-mail that is entering or leaving the organization. One option is to stop the encrypted e-mail at the firewall and decrypt it there. Another is to decrypt at the server or individual PC and scan there for potential viruses.[7]



Types of E-mail Encryption Products

Most e-mail encryption products include all of the above features. However, they fall into two main standards or protocols. The two defacto ad hoc standards are: S/MIME V.3 and Open PGP. S/MIME V.3 stands for Secure Multipurpose Internet Mail Extension, Version 3. Open PGP stands for Open Pretty Good Privacy. In the tradition of competing ad hoc standards, they are incompatible. This incompatibility will most likely continue. S/MIME V.3 recently became an approved standard by the Internet Engineering Task Force (IETF). The IETF is currently working on also creating an Open PGP standard before the millennium.[8] Having two incompatible standards is not a problem for a company

[7] www8.zdnet.com:80/pcweek/stories/news/0,4153,1015432,00.html

[8] www.imc.org/smime-pgpmime.html

that decides to use one protocol to communicate internally. But it does create a challenge for communicating securely with a host of external organizations or individuals that have opted to use incompatible products.[9]

Apart from choosing which protocol to use, the consumer has to choose a product. That is where it gets complicated. The following is just a small sample of the various products available:[10]

1. Web-based encryption services give the user an e-mail account on a Web site and provide encryption software at that Web site. The Web site acts as a traffic controller for the user's e-mail:

    - www.ZipLip.com
    - www.Hushmail.com

    Using Web-based systems is easy. Simply follow their instruction list. Be aware that some Web-based e-mail encryption systems require both the author and reader to register to the Web site to encrypt and decrypt e-mail.

2. PC-based applications install on a user's PC or network:

    - www.jawstech.com
    - www.pgpi.com
    - www.cypost.com
    - www.ancort.ru/
    - abi.hypermart.net
    - www.invisimail.com
    - www.cybergs.com/~issonline/
    - www.symantec.com

    Application-based tools vary in degrees of usability and strength. A good bet is to look for ones computer magazines have tested and given the coveted 'editors' choice' stickers. Most of the current products have made encrypting e-mail a one or two click process once the program has been set up. This is a major improvement from just a year ago. These PC-based products are independent of the Internet Service Provider used and can be installed with a few mouse clicks.

---

[9] For a more in-depth review of the two protocols, please see an article by Dave Kosiur, on the zdnet Help Channel, April 28, 1999, entitled "E-mail Privacy": www.zdnet.com/zdhelp/. Finding this article is not straightforward. Once at the URL, type 'email' into the search window and choose 'Internet' in the 'Categories' window. In the related info, click on E-mail Privacy (How to).

[10] Note: the Information and Privacy Commission does not endorse any of the products listed, nor any other products. This list is for reference only.

3. Public key infrastructures incorporate end-to-end security for organizations:

   - www.entrust.com
   - www.verisign.com

   These solutions add a host of other services to basic e-mail encryption ranging from securing Web sites to managing authentication. This includes handling all the digital certificates (i.e., where a third party guarantees your identity) needed by an organization to move information securely. These products are virtually transparent to the user.

4. Hybrid applications have e-mail encryption plus other features such as anonymizers/ pseudonymizers to break the connection between the user and any electronic flotsam that he or she leaves behind on the Internet:

   - www.zeroknowledge.com
   - www.proxymate.com

   The promising software "Freedom" by Zero Knowledge was at the beta stage of development as of August 1999, and, according to the company, it:

   - manages all of your digital identities, watches all outbound traffic for personal information, automatically encrypts and routes traffic through their Freedom network, transparently decrypts all incoming traffic, manages cookies, and filters spam.

   Proxymate's services do not include e-mail encryption but provide aliases. The service is easy to install and use. This proxy-based service gives users anonymity while surfing the net. Once registered (the software has an automatic setup option), the only added steps involve entering a username and password when you start up your Web browser. Proxymate provides aliases to Web sites asking for a user's name and e-mail address. Essentially a privacy screen, the service is transparent to the user.

5. Encryption tools in Netscape Communicator and Internet Explorer involve purchasing a digital certificate (60-day-free-trial period) from a third party such as Verisign. Vendors have simplified and fully integrated the process for installation and use in the browsers. However, expect to pay $10–$20/year for your digital ID. Corporate rates are available as well.

Next Steps

Once the user or organization has done some fact finding and is in the market for an e-mail encryption product, keep the following things in mind.

1. Has the encryption code been tested?

This assumes that the code is available for testing. Untested code is dangerous, as Netscape can attest to with Communicator 4. Netscape has published its Communicator 5 code for testing. Yet, not all companies do this. Third parties tied to academic cryptography bodies do the best testing. The Centre for Applied Cryptography at University of Waterloo, (www.cacr.math.uwaterloo.ca) is a fine Ontario example. In the words of Robert Morris Sr., former senior scientist at the American National Security Agency, "Never underestimate the time, expense, and effort someone will expend to break a code."

2. Is it a mature encryption software?

Mature in this context means the software has been in use for at least three years, undergone testing and review and continues to be used. In 1997, PC Magazine reviewed several e-mail encryption systems. Two years later, some of these products and their companies are impossible to find, or perhaps worse, might no longer exist.

3. Does it meet the needs of your organization or personal preferences?

The user needs to assess whether the product can support the traffic of e-mails generated. He or she needs to decide whether the product provides the required protection needed.

On the other hand, if the e-mail content is of limited value to others, use a product like Pkzip. Pkzip is a commonly used utility to zip or compress files through symmetric encryption. A complex password might be sufficient. Just change the password often and avoid file names that are too descriptive of the content, because that's another possible clue for snoopers.

4. What is the learning curve and ease of use of the product?

This often comes down to the number of key strokes it takes to encrypt and decrypt e-mail. It also comes down to the steps and time needed to acquire digital certificates (a way to avoid the need to remember and manage multiple passwords.)[11]

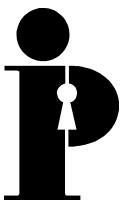
[11] www.netscape.com/security/basics/getpercert.html

Conclusion

E-mail encryption is a powerful tool in helping to protect an individual's privacy. This paper has attempted to map out the basic concepts. The Information and Privacy Commissioner encourages readers to put this new knowledge into practice and to actively investigate using e-mail encryption software.

Since this paper only provides a brief overview of the topic, we suggest that readers follow the links cited to gain an even better understanding of e-mail encryption. It is always useful to start with a list of your requirements. Such a list can be used to assess any potential products. If possible, test some products yourself. Soon, using encryption software will become second nature.

If you don't protect your privacy with tools like e-mail encryption, you may well lose it. And that could result in anything from a minor annoyance, to a gut-wrenching feeling of violation, to the loss of significant amounts of money. So guard your privacy well; the tools are out there for you to do so.



Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca