Sharon Jacobs
December 7th, 2005

E-mail as Encrypted-mail?

An old Arab lived close to New York City for more than 40 years. He would have loved to plant potatoes in his garden, but he is alone, old and weak. His son is in college in Paris, so the old man sends him an e-mail. He explains the problem:
"Beloved son, I am very sad, because I can't plant potatoes in my garden. I am sure, if only you were here, you would help and dig up the garden for me. I love you, Your Father."

The following day, the old man receives a response e-mail from his son:
"Beloved Father, Please don't touch the garden. It's there that I have hidden 'the THING'. I love you, too, Ahmed."

At 4pm the US Army, The Marines, the FBI, the CIA, and the Rangers visit the house of the old man, take the whole garden apart, search every inch, but can't find anything. Disappointed they leave the house.

A day later, the old man receives another e-mail from his son.
"Beloved Father, I hope the garden is dug up by now and you can plant your potatoes. That's all I could do for you from here. I love you, Ahmed."

-Anonymous

Summary

There are almost 3,000 people dead and no one saw it coming. It is September 11th, 2001 and terrorists just crashed four planes. The once safe United States does not seem so safe anymore. In response, the long debated issue of encryption truly came to the forefront. Encryption is the action of taking a message and transferring it into a code in order to keep the message private. This protects both the sender and receiver of the message, allowing only the receiver to view the message (Brown, 2001). After the September 11th attacks, people became aware of the threat to America and in response the Patriot Act was passed to help protect the United States from further attacks. The Act provided federal officials with more allowances to track and intercept communications. The intent was to help protect the U.S. from terrorists, but some feel that the government has no right to invade their privacy.

Immediately following the terrorist attacks on the U.S., most people were happy to hear that the government was making an attempt to protect them. But as the memories of the attacks began to fade in many people's minds, so did their feelings of fear. Some people still believe that they have nothing to hide and these people want the government to do everything possible to protect its citizens. These people believe that the Patriot Act is good and that it is necessary to track and intercept any and all internet activity to find anything suspicious.

On the other hand, there are also many people who believe that their privacy is being invaded and the government exceeds their authority to look through people's personal information. These citizens feel that the government should be able to monitor terrorists without monitoring innocent civilians. Additionally, some businesses are unhappy with the Patriot Act because they say that it makes it too easy for the government to get confidential business records (Business Groups, 2005). These people disagree with the Patriot Act and either they believe it should be amended or abolished altogether.

For those who only want to amend the act, the opportunity will come soon because many provisions are set to expire on December 31st, 2005 (Patriot Act, 2005). Some of the major concerns include section 213, which is often referred to as the sneak and peek provision. This allows the police to search a house without having to inform the residents beforehand. Many believe that this goes against the Fourth Amendment, which prevents "unreasonable searches and seizures" (Patriot Act, 2005). Furthermore, there are many concerns about the treatment of immigrants and foreign

nationals. Many feel that some of the provisions created relating to these people have allowed unfair treatment to innocent people (The Patriot Act, 2005).

A related debate has emerged concerning whether or not the use of encryption should be allowed. One of the major problems with the use of encryption is the difficulty in the law enforcement (Brown, 2001). Since it is so difficult to crack encrypted data, it is hard to enforce laws. The government wanted to make it easier to crack messages, but this was obviously very controversial (Rendleman, 2001). People want to be able to protect their private information and they did not want the government to make it so that they could read encrypted messages. Encryption is beneficial for businesses that need to protect the private data being sent over the internet, but unfortunately criminals can use it too (Brown, 2001). Quoting from an editorial in the Christian Science Monitor; "There's some evidence that the perpetrators of the September 11th attacks on New York and Washington had been using email, presumable to stay in touch with each other and further develop their plot. And Osama bin Laden's network has spread its message through CDs and other digital means" (Davies, 2002). With time quickly running out, these provisions need to be looked at and decided upon very soon.

Hot Quotes

- "Unfortunately, I think we're going to be asked to give up some privacy. I think that's a terrible consequence, because it means the terrorists, in a way, will have won," says Seymour Goodman, a professor at the Georgia Institute of Technology who specializes in terrorism, information technology, and national security.
- "We don't want to allow terrorism. Yet, I don't know how we can deny terrorists the ability to encrypt and retain our ability to encrypt," says Dave Barnett, security architect at Kaiser Permanente, a health-care organization in Oakland, California.
- "The increased use of encryption by terrorists, pedophiles, drug pushers, and other criminals could jeopardize public safety," worries FBI Director Louis Freeh.

- "My message to the Congress is clear, this is not time to let our guard down, and no time to roll back good laws," says President George W. Bush.
- Dennis Pluchinsky, a senior intelligence analyst with the Diplomatic Securtiy Service in the U.S. State Department, commented that all media should be controlled so that terrorists could not get crucial information. He said that, "A skeptic would call this censorship; a patriot would call it cooperation."

Educational Importance

It is very important for you as a user of the internet to become informed on this issue. Many people are unaware of the fact that any information that they send over the internet can be intercepted. That is why when information such as credit card numbers are sent over the internet, they are encrypted to prevent hackers from stealing the information. This all happens without the user even knowing, but ordinarily your emails are not encrypted. This means that any email you send can be intercepted and read by someone other than the intended receiver.

In order to protect people from having their information intercepted, some free email services encrypt your emails before they are sent. The problem with these programs is that both the sender and receiver must have email accounts with the same service. This is one of the ways that an average person like you can protect your information. Part of the encryption debate is whether or not such programs should be allowed because it interferes with the government's ability to monitor all activity. This means it is very important for people of all ages to learn about encryption and the debate surrounding it.

My Opinion

The United States used to represent safety and security, but after the attacks on September 11th, that feeling of security seemed to fade away for many Americans. The government passed the Patriot Act in order to help protect U.S. citizens. I feel a lot safer knowing that the government is keeping an eye out for potential terrorists. Many people feel that it is an invasion of privacy, but I think it is worthwhile. I also feel that I have nothing to hide because I have done nothing wrong, so the government can go ahead and look at whatever of mine they need to. The Patriot Act was written in an attempt to protect U.S. citizens and although it may not be an ideal situation, it is necessary. The government is making an attempt to track down terrorist activity and stop them before they act.

Support for infringing rights

An August 2002 National Public Radio/Kaiser Family Foundation/Kennedy School of Government poll of 603 respondents found support for:

	Support	Oppose	Don't know
Wiretapping telephones	69%	29%	2%
Intercepting e-mail	72	23	5
Intercepting ordinary mail	57	39	4
Examining Internet activity	82	15	3
Detaining suspects for a week without charging them	58	38	3
Detaining terrorist suspects indefinitely without charging them	48	48	4
Examining telephone records	82	17	1
Examining bank records	79	20	1
Tracking credit card purchases	75	21	4

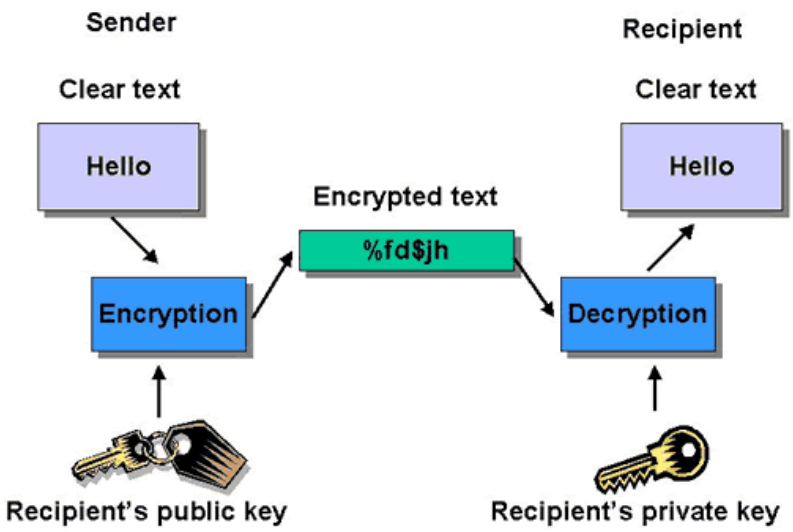
Source: National Public Radio — *The Detroit News*

As can be seen in the table to the left (Support, 2002), there are many people who support the government's infringement of rights. 72% of people responding to this poll supported the interception of email; while a mere 23% were opposed to it. At 82%, even more people supported the examination of internet activity and the same for telephone records. At this time, relatively soon after the 9/11 attacks, there was a great deal of support for many of these techniques used to find terrorists, although there was less support for detaining the suspects. Overall, there was a great deal of support in 2002, although I am afraid that some of that support has slipped as the memories of September 11th have faded in the minds of many.

Unfortunately the world is not such a safe place anymore, so sometimes we need to make sacrifices in order to protect ourselves. When we go to airports now, we all have to deal with searches. Unfortunately some people have to deal with it more often then others, but the point is to try to prevent a tragedy like September 11th from happening again. We all have to make sacrifices for the good of society. I am willing to allow the government to read my emails if that means that they will also be reading the emails of terrorists.

Encrypting Email

Two of the encrypted email services are Pretty Good Privacy (PGP) and Hushmail. They can be found at www.pgpi.org and www.hushmail.com, respectively. PGP requires that you download the program to use it. Although they are both free, Hushmail is quicker and easier to set up. Hushmail is backed up by a 2048 bit encryption. Hushmail has a new service where you do not even need to set up an account. You can simply enter your email address, the address of the receiver, and your message. Then you must enter a question and its answer that only the sender and receiver can answer. The message is sent and the receiver gets an email with a link to a Hushmail page. There they must answer the question to read the message.



This is very convenient for sending one or two encrypted emails, but if you want to send encrypted email all the time, it is very easy to set up an account. The free account has 128

megabytes of document storage. First, you can either choose your own username or have Hushmail choose a random one for you. Then you must create a password and a window opens up with directions. You have to move your mouse around in a box for about 30 seconds. This is used to create your unique encryption. Once this is complete, you are all set up and ready to go. This is a very simple setup that will allow you to send and receive encrypted emails with other Hushmail users.

Hushmail works using a public key encryption. The information gathered in the setup is used to create both a public key and a private key. The private key is made up to decrypt what the public key encrypts. Each user has a different key. When a message is to be sent, a different random key is used each time. The message is encrypted with this key. The key is then encrypted with the public key of the receiver and both are sent. Once the message is received, the key is decrypted using their private key. This key is then used to decrypt the message. This way only the receiver can decode the message.

Doe v. Gonzales

One of the provisions of the Patriot Act that has caused a lot of controversy involves the use of public internet stations in libraries. A provision allows the government to, "monitor in secret not just libraries, but all entities that keep records, including video store and book store user records." According to Attorney General Alberto Gonzales in April 2005, this provision has never in fact been implemented (Patriot Act, 2005). After the American Library Association found that in fact federal investigators were seeking more information than the Justice Department had admitted, the House voted to block this provision (Patriot Act, 2005).

The problems did not stop there. In the fall of 2005, there has been a great deal of controversy around the use of national security letters. In 1986 Congress authorized the use of national security letters to subpoena for documents (Tuohy, 2005). The Patriot Act allowed these letters to be used even more freely. When one Connecticut librarians received a letter requesting records, he refused to turn them over. He wanted a voice in the debate about the provisions of the Patriot Act (Supreme Court, 2005). The American Civil Liberties Union filed an appeal to allow the librarians to speak. The names of the librarian(s) involved in this case would not be released and the judge felt that, "nothing specific about this investigation has been put before this court that supports the conclusion that revealing Doe's identity will harm [the investigation]" (Tuohy, 2005). This case was then sent to the 2nd U.S. Circuit Court of Appeals to further argue about this gag order (Supreme Court, 2005).

In November, 2005, this case is being heard along with another similar case from the Southern District of New York (Tuohy, 2005). With time running out before December 31st when some of the Patriot Act provisions set to expire, there is quite a rush to conclude this case. The librarian(s) want a chance to speak out about the library provision. These librarians feel that the government is looking at innocent people's records without just cause. They feel that this is unfair and even unconstitutional and they want a chance to voice their opinions. However, with the gag order, they cannot even release their names, so with time running out, it is a race for a voice (Tuohy, 2005).

Keywords

- Encryption- 1: encipher
  2: encode

- Encode- 1 : to convert (as information) from one system of communication into another; especially : to convert (a message) into code

- Decode- 1 a : to convert (as a coded message) into intelligible form b : to recognize and interpret (an electronic signal)
  2 a: Decipher b: to discover the underlying meaning of

- Cryptography- 1 : secret writing
  2 : the enciphering and deciphering of messages in secret code or cipher
  3 : Cryptanalysis

- Cipher- noun: a method of transforming a text in order to conceal its meaning – compare code 3b b : a message in code
  verb: 1 : Encipher
  2 : to compute arithmetically

- ASCII- noun: a code for representing alphanumeric information

- Plaintext- noun: the intelligible form of an encrypted text or of its elements

From Miriam Webster Dictionary at www.m-w.com.

- Ceasar Cipher- also known as a Caesar shift cipher or shift cipher, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions further down the alphabet. For example, with a shift of 3, A would be replaced by D, B would become E, and so on.

- Data Encryption Systems (DES)- a cipher (a method for encrypting information) selected as an official Federal Information Processing Standard (FIPS) for the United States in 1976, and which has subsequently enjoyed widespread use internationally.

- RSA- an algorithm for public key encryption. The algorithm was described in 1977 by Ron Rivest, Adi Shamir and Len Adleman at MIT; the letters RSA are the initials of their surnames.

- Public Key Cryptography- a form of cryptography which generally allows users to communicate securely without having prior access to a shared secret key, by using a pair of cryptographic keys, designated as public key and private key, which are related mathematically.

From http://en.wikipedia.org.

Hot Articles

Bauer, Friedrich (2002). *Decrypted Secrets: Methods and Maxims of Cryptology*, Springer-Verlag Berlin Heidelberg, New York, NY.

Brown, Ken Spencer (2001). "Attacks Revive Privacy Debate (Laws On Data Encryption)." *San Francisco Business Times* Volume 16, Number 8: <http://find.galegroup.com/ips/infomark.do?&type=retrieve&tabID=T003&prodId=IPS&docId=A78873931&source=gale&srcprod=BCPM&userGroupName=mlin_s_wheaton&version=1.0> 9/15/05.

"Business Groups Want to limit Patriot Act." (2005). *The New York Times*.

Coutinho, S.C. (1999). The Mathematics of Ciphers: Number Theory and RSA Cryptography, A K Peters, Natick, MA.

Dale, Nell and Lewis, John (2004). *Computer Science Illuminated*, Jones and Barlett Publishers, Inc., Sudbury, MA. p.45-46.

Davies, Simon (2002). "A Year After 9/11: Where Are We Now?" *Communications of the ACM*, Volume 45, Number 9, p.35-39.

Herbet, Shireen J. "A Brief History on Cryptography." Articles on Cryptography. <http://cybercrimes.net/Cryptography/Articles/Hebert.html> 9/5/05.

Keyworth, G.A. (1998). "The Future of the Net: Computer Security Doesn't Hamper U.S. Security." *The Wall Street Journal*, p.1.

"The Patriot Act and Civil Liberties" (2005). *America*, Volume 193, Number 3.

PBS (2003). "Sacrifices of Security." Flashpoints USA. <http://www.pbs.org/flashpointsusa/20030715/infocus/topic_03/trans_pat_act.html> 9/5/05.

Rendleman, John (2001). "Mixed Messages -- The debate over encryption intensifies as the government looks to crack down." *InformationWeek*: <http://find.galegroup.com/ips/infomark.do?&type=retrieve&tabID=T003&prodId=IPS&docId=A78859191&source=gale&srcprod=EAIM&userGroupName=mlin_s_wheaton&version=1.0> 9/15/05.

Rogers, David (2005). "Bush Raises Heat on Congress To Extend Powers of Patriot Act." *The Wall Street Journal*, p. A4.

"Supreme Court Intervention Sought in Library Records Case." (2005). *The Hartford Courant*.

"Support for Infringing Rights." (2002). *The Detroit News*.

Tjaden, Brett (2004). *Fundamentals of Secure Computer Systems*, Franklin, Beedle, & Associates Inc., Wilsonville, Oregon.

Tuohy, Lynne (2005). "'Doe' Silent in Library Case." *The Hartford Courant*.