

Michael J. Sepcot  
September 17, 2004

## Cryptology: Privacy or Terrorism in the Digital Age

In the age of electronic communications with data being sent around the world in a matter of seconds, people have to rely on a form of security to ensure their private information is being kept a secret. This form of security is known as cryptology, and more specifically: public key cryptology. Public key cryptology got its start in the 1970s with the Diffie-Hellman key exchange thought experiment and the subsequent creation of the RSA (Rivest-Shamir-Adleman) algorithm. The Diffie-Hellman key exchange method relies on an individual having two sets of keys, one public and the other private. The public key is used to encrypt information that the private key can decrypt. Once information is encrypted using the recipient's public key, it cannot be decrypted by anyone without knowledge of the private key; not even the sender of the message is able to decrypt the information being sent. Once the scenario had been set as to how public key encryption could come to work, it needed a method of creating the public key, using the private key and a one-way algorithm. A one-way algorithm is a mathematical function that is easy to implement to get a solution, but very difficult to reverse unless certain information (the private key) is known. The RSA algorithm is just that, a one-way mathematical function that uses the inherited difficulty of prime numbers to generate a public key. The RSA algorithm actually requires there to be two private keys, both of which are large prime numbers; and the larger the better, for the more digits in the public key, the more prime numbers one would have to examine in order to determine the private keys being used and decrypt the information. This is where the problem comes

in, the size public keys and the strength of the algorithm used to generate them. Worldwide, governments are enforcing strict laws regarding the export and use of strong encryption technology, particularly in the United States. As computers are getting faster, the time it takes to determine private keys is growing shorter and the security of the global economy is coming into jeopardy. Governments worldwide need to start relaxing cryptological laws and increase the export of strong encryption technology in order to promote the security of its citizens and its place in the global market.

The Electronic Frontiers Australia (EFA) recognizes four major applications for encryption which can be summarized into three categories: Confidentiality, Authentication, and Security (*Introduction to Cryptology*). There needs to be a means of ensuring the privacy and confidentiality of the individual. Encryption technology allows people to communicate in confidence, knowing that the only people who are able to read messages and information being transmitted are the intended recipients. On the receiving side, individuals need to be able to verify who is sending information to them. Simply adding your name to the bottom of an email does not authenticate an email for anyone who knows your name would be able to do the same. Public key encryption allows for digital signatures and time stamps encoded by private keys and decoded by public keys (the reverse of the data encryption process allows for authorship verification!). And people need a level of security built into electronic communications to protect private information, such as credit card numbers, from becoming public. Encryption technology is the solution once again with the ability to encode any form of data and keep the information out of prying eyes. With worldwide acceptance of strong encryption technology confidentiality, authentication, and security issues would be put to rest.

With the advent and spread of such computer programs as PGP (Pretty Good Privacy), which take advantage of the RSA algorithm and use public key encryption, it is becoming increasingly difficult for law enforcement agencies to decrypt messages being sent around the world to and from terrorist organizations and drug dealers alike. For this reason, governments are wary about relaxing cryptological laws concerning key length and exporting procedures. Here in the United States, our government has attempted to balance the problem with little effect. They have created a program known as Key Escrow which currently has only taken hold within government agencies. The Key Escrow program is setup to mimic the benefits of public key encryption while allowing the government a method of retrieving private keys in order to decrypt information being sent. Key Escrow requires two separate government agencies to each keep track of private keys, the keys that decrypt messages, for every person using encryption software. This would allow law enforcement agencies to petition for court orders to retrieve private keys in order for them to read information they feel might be necessary in cracking open a case. The use of two agencies provides a boundary in which no one agency holds “all the keys” and helps to eliminate the possibility of bypassing the courts to acquire the keys. From the point of view of the government, this seems like a superb program in which all sides are happy, but when closely scrutinized, we begin to see flaws in the system. Key Escrow is similar to the wire tapping system we currently have in place. Law enforcement agencies have to petition the courts in order to legally tap someone’s communications to hopefully find out critical information needed to solve a case. But, over the years and throughout the world, we have seen the wire tapping system fail. Simon Singh points out in his book *The Code Book* that “there are roughly 100,000

illegal wiretaps conducted in France each year” (307). With numbers like this, it is obvious why people are concerned about letting the government hold the keys to decrypting personal messages. Nobody would want to give a copy of their house keys to the government, why would they want to give their private decryption keys. All it would take is one greedy individual or group to gain access to all of the keys and see the information for top dollar. Secrets are bought and sold all the time between governments and corporations what is to stop the possibility of it happening in the Key Escrow program. Keeping individual private keys secret is the key to the success of public key encryption. Even if one key is found out, the entire system is not at risk; and with sufficiently large prime numbers being used as private keys, it would take hundreds or thousands of years for one key to be uncovered.

The solution is simple and consists of three parts. First, governments worldwide need to relax or eliminate their cryptological laws in order to guarantee the confidentiality, the ability to authenticate ownership, and the security of its people. Second, a global encryption protocol needs to be created for the transaction of business and transfer of information to exist equally between countries. And last, an encryption chip needs to be installed on every communications device. Only with these three steps put into practice will individuals worldwide be guaranteed the information they send out will reach the intended recipient, and only the intended recipient.

**Sources:**

*Introduction to Cryptology*. Electronic Frontiers Australia. September 17, 2004.

<<http://www.efa.org.au/Issues/Crypto/crypto1.html>>.

Singh, Simon. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. New York: Anchor Books, 1999.