

## Cryptology: Privacy or Terrorism in the Digital Age

### 1. What is the problem itself?

In the age of the Internet with instantaneous communication and purchases being made every second of every day, there needs to be some form of security in place to prevent private information from falling into the wrong hands. There are various programs and algorithms that have been developed to encrypt data to keep information private, but these steps forward have fallen under attack from law enforcement agencies as being tools for terrorists and drug dealers to keep their plans from being uncovered. Here arises a problem; how to protect the transactions and communications of innocent civilians, while uncovering the plots of criminals.

### 2. What are the problem's effects?

(1) Encryption prevents law enforcement agencies from finding out about criminal intentions.

(2) Lack of encryption would destroy online trading and purchasing.

### 3. What are the problem's causes?

The encryption standard, RSA, is based on one-way mathematical functions and prime numbers. One-way mathematical functions are named in such that they are easy to compute, but difficult to reverse. This is enhanced when large prime numbers are added to the equation. In this case, three keys are needed: two large private keys, and one large public key. The private keys are used to compute the public key. Since there exists no fast and easy way to factor prime numbers, large prime numbers are used as the private keys. Because of the nature of the RSA algorithm, any information encrypted with the algorithm becomes impractical to attempt to decipher. Any average citizen can therefore protect themselves from their data being stolen over communication lines, but criminals can also keep their secrets well hidden.

### 4. What, if anything, is being done to solve the problem – and does this create further problems?

The government has taken on the job of finding a middle ground solution to the privacy concern. Their idea, Key Escrow, would follow in the RSA footsteps, but would keep a copy of one of the private keys in a government agency and the other key in a separate agency. Their thoughts were that law enforcement agencies can petition the key holding agencies to obtain the keys and there for decipher the information needed. This process is similar to the petitioning of the courts to obtain permission to perform wire taps on suspected criminals.

Opposition to this method has arisen from privacy groups such as the Electron Freedom Foundation (EFF). Their argument parallels the keeping of private keys to allowing the government to keep a copy of your house key. Allowing the government to keep a copy of your house key would allow them access to your house if they suspected you of wrong doing, but also carries the possibility of a bad cop taking your key and

entering your house any time they please. Giving the government copies of private keys would allow them access to all the information they want, reason or not.

5. What kind of thing is needed to solve the problem?

There needs to exist the guarantee of privacy over normal everyday communications methods, while allowing law enforcement agencies the ability to read the information if there exists evidence that the information being transmitted is of criminal intent; or one of the sides needs to give in for the better good for the whole.

6. What are the possible solutions?

(1) Government's Key Escrow is placed into effect in all new technology. The location of the data must be well secure and accessible via court order only.

(2) Encryption technology grows without government intervention. Enhance the security for people and corporations to conduct business in a secure environment.

(3) A middle ground is found that satisfies both parties.

7. Which solution is the best?

The middle ground is found. Since this option is not in the foreseeable future, encryption technology should be allowed to grow without interference.

8. How should the solution be implemented?

Overtake all laws pertaining to limiting encryption technologies.

9. What is the background to the problem?

RSA algorithm

Prime numbers

Key Escrow

Cryptology