

Problem/Solution – Topic: Cryptology

Issue 1: Privacy

Privacy has been a big concern since the dawn of recorded time. Military figures and governments wanted to keep their plans and secrets well guarded. Today, that same focus exists on the military and government side, but has also spread to the corporate world and down to the individual. The growing concern over privacy is not without cause. It has been estimated that there are over 100,000 unauthorized telephone taps made by law enforcement agencies each year. These numbers have alerted free speech organizations such as the EFF, Electronic Freedom Foundation, to petition against bills that would allow the government any more snooping power.

The continued development and improvement of public use cryptology software has made a strong stand to protect the average citizen's right for privacy. The development of the RSA algorithm and quick spread use of PGP, Pretty Good Privacy, in the home and corporate world since their introduction in the 1970s has improved the odds for personal and professional privacy, but the government would prefer to see otherwise.

Issue 2: Law Enforcement

There has been a big push in government for the reduction of cryptology since the outcome of September 11th. Law enforcement agencies see terrorism and drug dealers as the prime market for encryption based technology – not the average citizen. 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 due to the increase in use of privacy software and public key encryption.

The Key Escrow program, in which the government would not only allow, but promote the use of public key encryption technologies, has been the latest attempt from the government to solve their dilemma. Key Escrow would require two separate government agencies to each keep track of one of the two private keys, the keys that decrypt messages, for every person using encryption software in the country. While this would follow the same set up as the phone tapping system, which requires a court order to legally tap a phone, it has not become a standard outside the government. Most people would not be comfortable with giving a copy of their house key over to the government in case there is a problem, and that is effectively what Key Escrow is asking, if there is reasonable evidence to suggest wrong doing, then the government can step in and verify it by reading messages. But the misuse of wire taps indicates that there is a good probability of misuse of private keys and as such, the efforts of government supported encryption have so far failed.

Issue 3: Public Trade

From E-Trade to E-Bay, and every business in between, online shopping and day trading have become a norm in the United States. With current legislation, it has become standard practice for companies to build in encryption technology into their web stores and web browsers making for an individual's online shopping experience a happy one knowing that their private information is kept away from peeping eyes. However, this is not the case world wide. Some countries have more restrictive encryption laws and demand that public keys, keys that encrypt data, be limited to a length that can be broken by law enforcement. By limiting such keys, public trade becomes riskier. Keys that should take thousands of years to break if left alone would now become breakable in a

reasonable amount of time (few hours to a few days). While this might help out with law enforcement, it also helps out the criminals who steal credit card numbers and personal data. These restrictive encryption laws need to be overturned in order for all countries to benefit from the online trade market.