# Encryption Use and Policy

December 10, 2004

## About

This paper was written for the Fall 2004 offering of Information Technology and Public Policy at the University of Washington, University of California Berkeley, and the University of California San Diego.

## Contributors


| Name | School | Email |
|---|---|---|
| Andrew Terry | UCSD | aterry@cs.ucsd.edu |
| John Naegle | UW | naeglej@cs.washington.edu |
| Josh Opos | UCSD | jopos@cs.ucsd.edu |
| Steven Huang | UCSD | sbhuang@ucsd.edu |

# Table of Contents

# 1 Introduction

Information security has played a critical role in protecting national secrets, strategies and communications for many thousands of years. Whenever a communication medium, such as paper-based message passing, radio transmissions, or digital information can be observed by an adversary, such as a foreign government, and the value of the data is high, information security has been critical to safeguarding the information. Cryptography, the process of scrambling ordinary text into a cipher text with encryption techniques and decrypting the transmitted message, is one means of achieving information security and has been in use for thousands of years.

The earliest recording of encryption use occurred 4000 years ago in Egypt where hieroglyphic inscriptions on the tombs of noblemen were written with a number of unusual symbols to obscure the meaning of the inscriptions. Julius Caesar in 50 BC and the Spartans in 5 BC developed simple substitution and transposition ciphers to send and receive secret messages. With the renaissance, the evolution of mathematics, the development of mass communications, the world wars, and the Internet era, cryptography has evolved rapidly and been used extensively to protect sensitive data.

In most applications of cryptography, the transmitted cipher text is readily available. In the early 20th century, encrypted messages were often sent over radio making it possible for any listener to intercept the encoded text. Similarly, any knowledgeable listener can intercept Internet traffic and capture an encoded message. In almost every instance, cryptography is required because of unsecured communications channels that can be passively or actively attacked by an enemy. In addition there is little security through algorithmic obscurity. History has shown that maintaining the secrecy of an encryption algorithm is very difficult. The modern cryptographic and security communities now assume that an adversary is given cipher texts and the encryption schemes used to produce them, with only the encoding or decoding keys remaining private knowledge.

This paper discusses cryptography technology, the history of encryption use and points out key events that led to the current state of cryptography and information security in the digital age. It shows the progression of adversarial attacks and what lengths adversaries will go in order to decipher messages. It discusses United States Governmental encryption policies, how they have evolved and their consequences. In addition, it will look to the future of cryptography and information security and make recommendations for future policy makers.

# 2 Technology

Encryption is the transformation of data into a form unreadable by anyone without a secret decryption key. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it was not intended, including those who can see the encrypted data. Encryption may be used to make stored data private, or to allow an unsecured communications channel to serve as a private communications channel.

There are several components that make up this process, which are defined below. An encryption scheme is a primitive that specifies a mathematical algorithm, which tells the sender how to process the plaintext, thereby producing the ciphertext that is then transmitted. An encryption scheme also specifies a decryption algorithm, which tells the receiver how to retrieve the original plaintext from the transmission and may include a verification process as well. Finally, key-generation algorithms are used to produce keys that are used as seeds for the mathematical processes used to encrypt and decrypt messages.

## *2.1 Private Key Cryptography*

Private key cryptography, also known as symmetric key cryptography, is a scheme where both the sender and receiver use the same key. Since the keys are shared, symmetric key cryptography can be more vulnerable to attack if either key is compromised. However, symmetric key cryptography is often many times faster than other schemes that will be discussed below, making it suitable for large data transmissions or high throughput applications.

### 2.1.1 Symmetric Encryption

A Symmetric (shared-key) encryption scheme SE = (G; E;D) consists of three algorithms, as follows:

- The randomized key generation algorithm, G, returns a string K. We let Keys(SE) denote the set of all strings that can be generated. The members of this set are called keys.
- The encryption algorithm E takes a key K in Keys(SE) and a plaintext M to return a ciphertext C. This algorithm might be randomized or stateful.
- The deterministic decryption algorithm D takes a key K in Keys(SE) and a ciphertext C to return some M.
- We require that for any key K in Keys(SE) and any message M, if $E_K(M)$ returns a ciphertext C then $D_K(C) = M$.

Once in possession of a shared key, the encryption algorithm is run with key K and input message M to produce a encoded message, C, which is transmitted to the receiver.

The receiver, upon receiving a ciphertext C, will run the decryption algorithm with the same key used to create the ciphertext, namely compute $D_K(C)$. If C was an output of $E_K$ on input M then $D_K(C)$ will equal M, enabling the receiver to recover the ciphertext. The decryption algorithm might however, fail to decrypt and return a special symbol to indicate that it deems the ciphertext invalid.

## *2.2 Public Key Cryptography*

Public key cryptography, also called asymmetric cryptography, is an encryption scheme where the receiver has a private key that can be used to decrypt messages encoded with a shared key. Generally, the shared key is published, available to possible adversaries as well as desired communication partners. Anyone in possession of the public key can encrypt messages, but only the receiver can decrypt a ciphertext.

### 2.2.1 Asymmetric Encryption

An Asymmetric encryption scheme AE = (K; E;D) consists of three algorithms, as follows:

- The randomized key generation algorithm K returns a pair (pk; sk) of keys, the public key and matching secret key, respectively.
- The encryption algorithm E takes the public key pk and a plaintext M to return a ciphertext C. The algorithm may be randomized, but not stateful.
- The deterministic decryption algorithm D takes the secret key sk and a ciphertext C to return some M.

For any key-pair (pk; sk) generated by K and any message M, if C was returned by $E_{pk}(M)$ then $D_{sk}(C) = M$.

## *2.3 Block Ciphers*

Sections 2.1 and 2.2 give two encryption schemes, ways of applying cryptographic algorithms to encrypt and decrypt messages or data. Block ciphers are the building blocks of encryption and decryption algorithms that work on fixed size plaintext inputs. A block cipher is a family of functions: $E(K, M) \rightarrow C$ where *K* is a *k*-bit binary string, and *M* and *C* are *n*-bit binary strings. *K* is typically referred to as the key, *M* the plaintext and *C* the ciphertext. The key-length *k* and block-length *n* are parameters associated with the specific block cipher *E*. For every encryption cipher *E* there is a corresponding decryption cipher that produces *M* from *C* detonated by $E^{-1}$.

### 2.3.1 Modes of Operation

There are several ways in which to piece together block ciphers to create encryption and decryption algorithms. These different ways are called modes of operation. A few popular modes of operation are defined below, however there are a multitude of others that are used today.

#### 2.3.1.1 Substitution Cipher

The Substitution cipher does not use a block cipher due to its simplicity, however it was very popular throughout history and was fundamental in the evolution of cryptography. Each plaintext character or group of characters is simply replaced by one from a cipher alphabet. The cipher alphabet may be shifted, reversed, or scrambled, in which case it is called a "mixed alphabet" or "deranged alphabet". A simple example of a substitution cipher that shifts the input characters to the left by three positions is shown below:

```
plain text:      give me liberty or give me death
encrypted text:  dfsb jb ifyboqv lo dfsb jb abxqe
```

**Listing 1 - Substitution Cipher Example**

Substitutions preserve the frequency of characters in the input text which can lead to statistical analysis vulnerabilities. For instance, by analyzing the frequency of letters in the encoded text and observing the frequency of letters in the plain text language, it is possible to guess the substitution cipher. Thus, substitution ciphers are not useful for high-value applications on their own. However, they form an important building block and are often used in combination with other ciphers to form strong encryption algorithms.

#### 2.3.1.2 One Time Pad

The One-Time-Pad (OTP) encryption scheme can be thought of as a block cipher. OPT encryption schemes, when used correctly, are secure against any form of analysis or attack. The OTP encryption scheme SE = (K; E;D) is stateful and deterministic. The key-generation algorithm simply returns a random k-bit string K, where the key-length k is a parameter of the scheme. The

sender maintains a counter, which is initially zero. The encryption algorithm XORs the message bits with key bits, starting with the key bit indicated by the current counter value. The counter is then incremented by the length of the message. Key bits are not reused, and thus if not enough key bits are available to encrypt a message, the encryption algorithm returns a special symbol. The ciphertext returned includes the value of the counter to enable decryption.

### 2.3.1.3 Electronic Code Book

Operating in Electronic Code Book (ECB) mode yields a stateless symmetric encryption scheme SE = (K; E;D). It breaks a message M into n-bit blocks M[0]…M[m], where m=|M|/n. It feeds each of those blocks into a block cipher along with the key k to get correspondingly long n-bit ciphertexts C[0]…C[m]. The ciphertext representing the entire message M is C = C[0]…C[m]. Shown below is a conceptual diagram of how ECB mode pieces together block ciphers to create an encryption algorithm. The decryption algorithm is not shown, but is simply the inverse of the encryption algorithm in which the decryption block ciphers receive input C[0]…C[m] and key k, and return the plaintext M = M[0]…M[m].

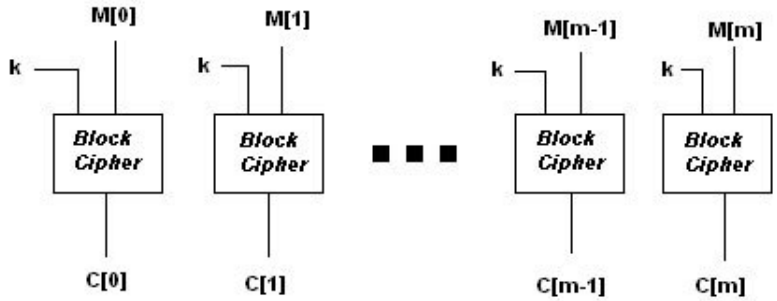


**Figure 1 – Electronic Code Book (ECB) mode encryption algorithm**

### 2.3.1.4 Cipher Block Chaining

Operating in Cipher Block Chaining (CBC) mode with counter Initialization Vector (IV) that is maintained throughout instances of use yields a stateful symmetric encryption scheme, SE = (K; E;D). Each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block is dependent on all plaintext blocks up to that point.

Shown below is a conceptual diagram of how CBC mode combines block ciphers to create encryption and decryption algorithms.

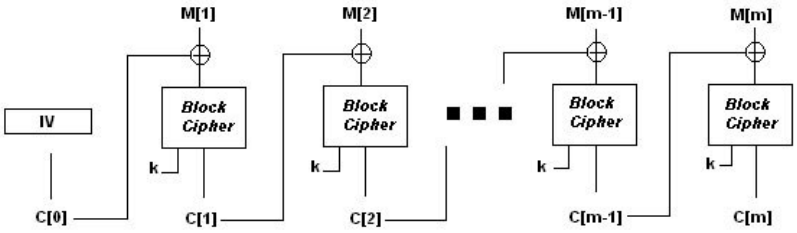


**Figure 2 - CBC Encryption Algorithm**

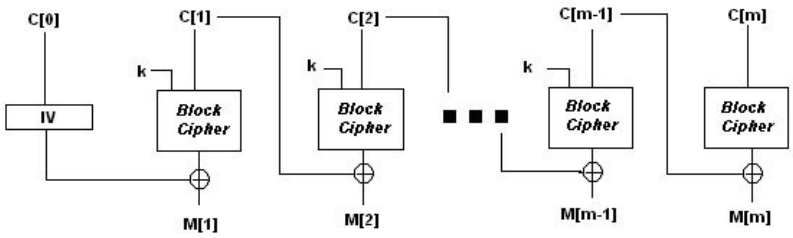


**Figure 3 - CBC Decryption Algorithm**

### 2.3.1.5 Data Encryption Standard (DES)

The Data Encryption Standard (DES) is the quintessential block cipher. Even though it is now quite old, and on the way out, no discussion of block ciphers can really omit mention of this construction. DES is a remarkably well-engineered algorithm which has had a powerful influence on cryptography. It is in very widespread use, and probably will be for some years to come in legacy applications.

DES has a key-length of k = 56 bits and a block-length of n = 64 bits. It consists of 16 rounds of what is called a "Feistel network." The basic idea behind a Feistel round is to break intermediate texts into a left and right side, which will be encrypted differently, and fed into the opposite side of the block cipher in the next round (i.e. the left output goes into the right input and vice versa). One of the reasons to use this round structure is that it is reversible even though the functions which make up the block ciphers are not. This structure is part of the reason why DES is such a strong cipher - without the correct keys and the correct Feistel network, the ciphertext is almost useless.

The only known flaw to DES is its age. The key length was used because at the time it was long enough to make exhaustive key searches and other attacks prohibitive. However, with the dramatic increase in processor speeds, this is no longer the case. Hence the key length issues are a side effect of the cipher's age. Other modes have been created to circumvent the key length problem such as Double-DES(2DES), Triple-DES(3DES), and DESX, which all use a combination of DES ciphers.

### 2.3.1.6 Advanced Encryption Standard (AES)

The AES has a block length of n = 128 bits, and a key length k that is variable: it may be 128, 192 or 256 bits. So the standard actually specifies three different block ciphers: AES128, AES192, AES256. These three block ciphers are all very similar.

AES is a very elegant algorithm which is based on finite fields and abstract algebra. A complete definition is beyond the scope of this paper, however the punch line is that AES solves the key-length and block-length problems of DES in a more efficient and elegant fashion.

## 2.3.2 RSA

The RSA system, named after its inventors Rivest, Shamir and Adelman, is the basis of the most popular public-key cryptography solutions. The RSA algorithm is based on the fact that there is no known efficient way to factor very large numbers (on the order of 100 digits and growing). Deducing an RSA key, therefore, requires an extraordinary amount of computer processing power and time.

The RSA algorithm has become the de facto standard for industrial-strength encryption, especially for data sent over the Internet. It is built into many software products, including

Netscape Navigator and Microsoft Internet Explorer. The technology is so powerful that the U.S. government has restricted exporting it to foreign countries.

## *2.4 Authentication*

Encryption concepts and primitives are not only used for data protection, but also for data authentication. In the next sections, we define two authentication schemes as they are very closely related to encryption schemes both symmetric and asymmetric. Privacy does not imply authenticity. Although the goals may appear similar, they are distinct, and one does not guarantee or imply the other.

### 2.4.1 Message Authentication

Message authentication allows one party to send a message to another party in such a way that if the message is modified en route, then the receiver will almost certainly detect that the contents have been tampered with. Message authentication is also called “data-origin authentication," since it authenticates the point-of-origin for each message. Message authentication is said to protect the “integrity" of messages, ensuring that each that is received and deemed acceptable is arriving in the same condition that it was sent out - with no bits inserted, missing, or modified.

In this case the Sender and the Receiver share a secret key, K, which they use to authenticate their transmissions. Sender S wants to send message M to receiver R in such a way that R will be sure that M came from S. They share key K. Adversary A controls the communication channel. Sender S sends an authenticated version of M, M’, which adversary A may or may not pass on. On receipt of a message M, receiver R either recovers a message that S really sent, or else R gets an indication that M has been tampered with or altered in some way

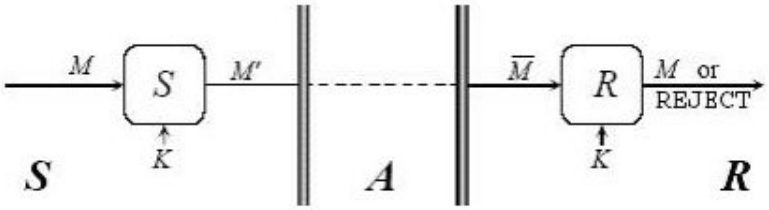


**Figure 4 - Message Authentication**

### 2.4.2 Digital Signatures

A digital signature scheme is just like a message authentication scheme except for an asymmetry in the key structure. The key sk used to generate signatures (in this setting the tags are often called signatures) is different from the key pk used to verify signatures. Furthermore pk is public, in the sense that the adversary knows it too. So while only a signer in possession of the secret key can generate signatures, anyone in possession of the corresponding public key can verify the signatures.

The key usage is the “mirror-image" of the key usage in an asymmetric encryption scheme. In a digital signature scheme, the holder of the secret key is a sender, using the secret key to tag its own messages so that the tags can be verified by others. In an asymmetric encryption scheme, the holder of the secret key is a receiver, using the secret key to decrypt ciphertexts sent to it by others.

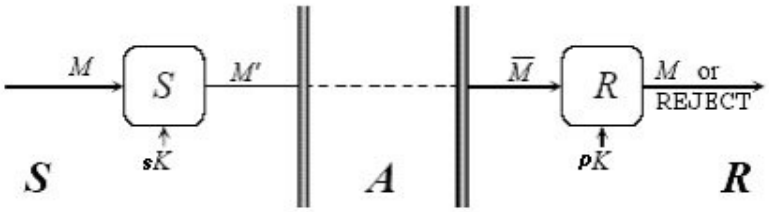


**Figure 5 - Digital Signature Scheme**

## *2.5 Attacks*

All encryption schemes have been scrutinized and gone under attack of one form or another. Although there is no concrete definition as to what a "good" encryption scheme is, it is obvious what a "bad" one is – a scheme that is vulnerable to many attacks. We discuss some different types of attacks that have proven successful on many encryption schemes in the past, as well as modern ones.

In all cases, the assumption is made that an adversary has access to the definition of the encryption scheme, and can listen to the channel on which ciphertexts are transferred. Making these assumptions may be a bit overzealous, but as demonstrated in the past, security through obscurity is not strong enough. These assumptions are the standard assumption made in creating encryption schemes, and lead to more secure and robust encryption schemes. An attack is successful if it can deduce plaintexts, or even better the key.

The attacks below are ordered from weakest to strongest. Weak attacks are attacks that do not succeed as often as stronger ones because they know less information.

### 2.5.1 Known Ciphertext Attack

A known ciphertext attack is a cryptanalytic attack in which the adversary has access to a set of ciphertexts. This is the easiest attack to mount, since it only requires the adversary to listen to an insecure communication channel. Conversely, this attack is the most difficult attack to execute successfully because the adversary lacks knowledge. Substitution ciphers, and other ciphers that repeat patterns are susceptible to these attacks because statistical analysis can aid in inferring the plaintext.

### 2.5.2 Known Plaintext Attack

The known plaintext attack is a cryptanalytic attack in which the adversary has samples of both the plaintext and its ciphertext and can use them to reveal further secret information. These types of attacks were carried out during WWII at Bletchley Park against the Germans.

### 2.5.3 Chosen Plaintext Attack

A chosen plaintext attack is any form of cryptanalysis where the adversary has the capability to capability to encrypt arbitrary plaintexts. Modern cryptography is implemented in software or hardware and is used for a diverse range of applications; in many cases, a chosen-plaintext attack is often very feasible. Any cipher that can prevent chosen-plaintext attacks is then also guaranteed to be secure against known plaintext and known ciphertext attacks

### 2.5.4 Replay Attack

A replay attack is an attack in which a valid data transmission is maliciously or fraudulently repeated, either by the originator or by an adversary who intercepted the original transmission. Although this attack does not glean any information about plaintexts or encryption keys, it is still

dangerous as it is very difficult to detect. Since the adversary does not have to manipulate the ciphertext, digital signatures and message authentication schemes are of little help. Such attacks can be carried out by intercepting valuable information such as credit card and pin numbers, and reusing them at a later time to make withdrawals.

It is extremely difficult to detect malicious replay attacks performed by the originator of a message, especially since they are supposed to be cooperative. There are however, ways to detect replay attacks performed by outside adversaries such as requiring message transmissions to contain a sequence number. This defense is simple, yet effective since each time a legitimate user transmits a message it will contain an updated sequence number that will be difficult for the adversary to reconstruct. Further, encrypting the sequence number in the ciphertext, facilitates message authentication and digital signature schemes to detect whether ciphertexts have been manipulated to update message sequence numbers.

# 3 History

As mentioned in the introduction, use of cryptography to secure information dates back many thousands of years. This section examines the historical significance of cryptography and its use in the present day.

## *3.1 Pre World War*

The earliest recording of encryption use occurred in ancient Egypt 4000 years ago where hieroglyphic inscriptions on the tombs of noblemen were written with a number of unusual symbols to obscure the meaning of the inscriptions. In 5 BC, the Spartans developed a cryptographic device called a Scytale, which was a cylinder in the possession of both the sender and receiver around which a message could be wound to perform a transposition of the letters. In 50 BC, Julius Caesar used a substitution cipher to send secret messages where each letter was replaced by a different letter a certain distance ahead or behind the actual letter in the alphabet. With evolving mathematical techniques, cryptography made great advance in the late 15$^{th}$ century. One of these advances was the poly-alphabetic cipher, developed by Italian Leon Battista Alberti in 1467, which uses multiple substitution alphabets. The most well known poly-alphabetic cipher is the Vigenère Square, created by Frenchman Blaise de Vigenère. It was long thought to be unbreakable, but was found to be vulnerable to statistical attack in the 19$^{th}$ century. Although the roots of cryptography can be traced back thousands of years, cryptography did not garner much attention until World War I.

## *3.2 World War I*

Early in World War I, many of Germany's telegraphy lines in France and Belgium, as well as across the Atlantic were severed. This forced Germany to rely on wireless communication or Swedish and American lines routed through Britain. In addition, wireless communications were often the only way to effectively communicate with vessels at sea and armies on the move. This gave Britain and her allies many opportunities to intercept German communications and affect the course of the war. However, the Germans were aware of the high likelihood of interception and encrypted their communications.

The British Admiralty's Intelligence Service formed a cryptanalysis organization known as Room 40 for their location in the Old Admiralty Building. Because of weaknesses in the algorithms and material aides such as the discovery of cipher and codebooks, the Room 40 group was successful in decrypting many troop movement and diplomatic messages.

The most notable decrypted message by Room 40 is known as the Zimmerman telegram. In January of 1917, British code-breakers William Montgomery and Nigel de Gray were given an encrypted telegram sent over Swedish lines and intercepted in Britain. Room 40 already knew the cipher and was able to decrypt enough of it to quickly realize its significance. The message was sent by the German foreign minister to Mexico declaring a start to unrestricted submarine

warfare. The message also urged Mexico to invade the US and to encourage Japan to do the same. The message ultimately prompted President Woodrow Wilson to declare war on Germany in April of 1917.

There were other uses of encryption going on during the war as well. With the known vulnerabilities of simple ciphers, armies used so called “Trench Codes” to facilitate secrete internal communications. In order to use codes, it was necessary to have codebooks to translate the meanings of the code words. Losing a codebook would render the current code useless. When this happened, it was possible to issue new codebooks to maintain security, but this was difficult in practice.

In 1918, the Germans developed a new cipher that they believed was unbreakable. The cipher was a fractioning transposition cipher called ADFGX, named for the labels of the rows and columns of the checkerboard used in constructing a message. The cipher proved to be very difficult to break. Frenchman Georges Painvin was able to decrypt some messages to gain knowledge of German activity, but the breaks were mostly a result of messages being sent with the same keys. A general solution to decrypting messages was never found during the war.

## *3.3 World War II*

Though cryptography played an important role in World War I, it played a much larger role in World War II as technologies evolved and the stakes increased.

Between the World Wars, Germany developed the Enigma machine, an encryption device thought to be unbreakable in the 1920s. Enigma was a portable machine consisting of a keyboard, a number of rotary dials and a display. Encrypting messages involved setting the rotors, entering the messages via the keyboard and observing the display. Decryption was similar in that the rotors were set and the encrypted message was entered on the keyboard. A number of different versions of Enigma machines were developed, including commercial versions.

Early in World War II, Britain started a secret project codenamed Ultra to decrypt radio traffic and Enigma messages. Ultimately, Ultra was successful in breaking Enigma encoded messages and led to significant military victories that shortened the course of the war. Ultra’s efforts were aided by several factors. In 1932 Polish cryptanalysts made fundamental breakthroughs, aided by copies of Enigma manuals sold by a disgruntled soldier, and were able to decipher “day keys” allowing decryption of a single day’s message traffic. This information made its way to Britain in 1939 and because of weaknesses in the system, such as never outputting the input character and the fact that many messages contained common greeting phrases, Ultra was able read nearly all of German Enigma traffic by 1945.

American efforts to decrypt Japanese message traffic also played a significant role in World War II. In 1943, the US intercepted Japanese messages sent using a cipher called JN-25. The code was found to be a subset of a US Army code used in the Spanish-American war of 1898. However, the Japanese did not know the code was susceptible to attack. The US Army Air Corps used intercepted messages to help in the assignation of Japanese Admiral Yamamoto Isoroku as he traveled for a tour of the South Pacific.

The JN-25 code was not Japan’s only cryptography system in use during World War II. Also of note was the Purple machine, which was an excellent form of encryption for the time, but the Japanese operators misused the device. Operational errors such as poor key choices exposed weaknesses in the scheme and led to US Signals Intelligence breaking the code. Access to these encrypted messages gave the Americans an advantage over the Japanese and many speculate that this knowledge shortened the war.

## 3.4 Cold War

Starting in the 1940s and continuing through the Cold War, the US and Britain collaborated to break Soviet encrypted messages. Codenamed the Venona project, out of hundreds of thousands of messages, thousands were able to be decrypted. The Soviets were using unbreakable one time pads, but reuse of the pads led to vulnerabilities in their system. The decryptions were a product of espionage and also the error of reusing pads. The majority of messages were KGB communications and were used to gain information about Soviet behavior. The existence and in some cases, identification of US, Canadian, British, and Australian spies was discovered. The existence and the significance of the Venona project was not made public until 1995.

## 3.5 Current Times

Up until the last 40 years, it was believed that cryptography would be more secure if the algorithms were kept secret. As history showed, keeping a cipher secret could not guarantee complete information security, and there was a shift toward publicly known standards with only secret keys. In 1976, DES encryption was adopted as the Federal Information Processing Standard (FIPS) for use by all non-military government agencies and government contractors. Although DES now has shortcomings as noted in the previous section, its standardization sparked much research and advancement of the cryptography field. The interest in the subject became more of a public concern, rather than solely a military one. Also in the late 1970's, public key cryptography, where both the sender and receiver had their own private keys and shared a known public key, was developed as an alternative to the private key cryptography that was used in the past. The most notable public key encryption scheme is called RSA. Also, there is currently a great deal of work towards advancing encryption techniques. A new topic is quantum cryptography, where it is possible to securely pass keys because the keys cannot be intercepted without being changed. It is clear that the great need for cryptography in today's society will continue to drive the field forward.

Unfortunately, a few current applications show that encryption is still not being used correctly. In the open source community, encryption and security are often overlooked or not implemented correctly. The main problem is that with so many contributors to the code, it is inevitable that someone who knows little or nothing about security will submit code. For example, many open source programs use SSL improperly, leaving them open to various types of attacks. Many programmers think that SSL APIs provide authentication by default, but they do not and thus their applications are vulnerable.

Another example of incorrect uses of cryptography is Diebold's DRE voting machine. First of all, the DRE machine uses smartcards, but fails to use any of the smartcard's cryptographic operations. Therefore, no secure authentication takes place, allowing a person to bring in a pre-programmed smartcard to perform an attack on the machine. Also, the machine uses DES encryption, which is know to be vulnerable to brute force attacks even though triple-DES and AES are known to be more secure. Unfortunately, the machine not only uses DES, it misuses it. The key value is hard coded into the source code, which obviously compromises its effectiveness. Also, DES depends on a random initialization vector to ensure security, but the vector is always initialized to zero in the Diebold machine's code. These errors show that although encryption techniques have improved, the use of outdated algorithms and misuse of encryption techniques are still common.

Today, a large number of products pass data over the Internet or have other reasons for needing encryption. Uses of encryption are clearly visible in everyday applications. ATMs are now mandated to use Triple DES encryption. RSA has become highly used to encrypt data sent over the Internet and is used in web browsers like Netscape Navigator and Microsoft Internet Explorer. E-mail uses an encryption called PGP (Pretty Good Policy) to provide cryptographic privacy and

authentication. With information transfer becoming a critical aspect of modern society, encryption has become necessary in more than just military applications. As encryption continues to affect more people in their everyday lives, it is important to learn from the misuses of encryption in the past and move forward emphasizing correct usage of secure algorithms.

# 4 Public Policy

Public policy is governmental law, rule, statute, or edict that expresses the government's goals and provides for rewards and punishments to promote their attainment [13]. This section examines US Government public policy with respect to cryptography over the last century. Export control, usage restrictions and research and development support are discussed in the following sections. The consequences of US policy are examined in section 5.

## *4.1 Export Control*

Export control is a practice, defined and enforced by governments, whereby restrictions are placed on the transfer of products and technologies to other countries. Export control policy in the United States with respect to cryptography has traditionally had two main goals: to keep strong cryptography out of the hands of potential targets of US intelligence and to support the growth of U.S. businesses in domestic and international markets. However, these goals are often in competition and the cryptographic export policy of the United States has reacted to changes in the business and national security landscapes.

For much of the 20th century, cryptography's sole use was to secure government communications and data. Public policy reflected this by striving to keep knowledge of cryptography and cryptanalysis in the exclusive domain of the United States Government. By denying enemies, perceived or real, access to communication channels secured by strong cryptography, it was easier for the National Security Agency to read foreign government communications and provide hard intelligence to policy makers.

With the large impact of cryptography and cryptanalysis in World War II, the United States government recognized the value of retaining the large technological lead it had built in this area. To these ends, the Arms Export Control Act (AECA) of 1949 gave the executive branch authority to determine what products and technical data were subject to export control, run licensing systems and to penalize violators of export policy. The AECA formed the basis for the International Traffic in Arms Regulations (ITAR) that defines the U.S. Munitions List (USML). The USML contains products and technologies, including cryptography that are intended for import and export as munitions. It is administered by the Department of State and items falling on the USML must be approved for export by the Office of Defense Trade Controls which can be time consuming and burdensome for the exporter and purchaser.

With little public or commercial demand for cryptographic systems, the export controls up to the early 1970s were effective in slowing the global spread of cryptography developed in the United States. However, with the digital evolution and globalization trends in the economy emerging in the 1960s and 1970s, commercial demand for cryptography began to grow. International banking, ATM technology, secure telephony and other industries requiring secure communications and data storage to protect global and domestic business began to exert pressure on the government to relax export controls as new opportunities emerged.

Restricting cryptography to only government use failed to recognize that public policy must incorporate business development, national security and public safety aspects. Government policy reacted to the market forces pushing for wider availability of cryptography. Beginning with the 1969 Export Administration Act (EAA), government policy began to include both national security and business interests. The EAA gave the Department of Commerce (DOC) responsibility for administering the Export Administration Regulations and maintaining the Commerce Control List (CCL) for products with both commercial and military applications. The

State Department continued to regulate cryptography through the USML, but in the 1980s began to move some control to the DOC through the CCL.

With the rise of the Internet in the 1990s, cryptography export control began to face serious practical challenges. Anti-Nuclear activist Philip Zimmerman developed Pretty Good Privacy (PGP), a strong public key cryptography system and it was posted on the Internet in 1991 as free software. PGP was soon widely available outside the US in violation of export control and a criminal investigation was brought against Zimmerman. The Internet and its global nature presented serious practical challenges to administration of export policy. "One software product with encryption capabilities taken abroad can serve as the seed for an unlimited number of reproductions that can find their way to hostile parties" [12]. In addition to the challenges presented by the Internet, regulating export of cryptography software via printed out source code mailed across borders, or knowledge carried in people's minds was, and remains, an impossibility. Many policy makers and technical advisors realized that widespread, non-governmental use of cryptography was inevitable. However, there is a significant difference between an individual and a corporation developing cryptography-enabled software for export. Corporations provide a litigation target with significant assets. Thus, while private use of cryptography was spreading, strong cryptographic products remained uncommon.

In the mid 1990s, market forces began to push the demand for more widely available strong cryptography in commercial products. With more research and publicity, cryptography became more widely available outside the United States and US businesses had to compete with foreign cryptography vendors in the global market. Through the mid 1990s, only 40-bit RC2/RC4-based products were allowed for mass export. However, cipher texts generated from 40-bit keys were easily breakable in under a week's time in 1996. Because of the difficulties required to obtain the stronger domestic version, domestic users of cryptography enabled products, such as web browsers, also tended to use the weaker product.

The United States Government made an effort to continue restrictive export control policy with the Wassenaar Arrangement in 1996. Established in 1996 it has the stated goal of contributing "to regional and international security and stability by promoting transparency and responsibility in transfers of conventional arms and sensitive dual-use goods and technologies" [18]. A total of 33 nations signed the arrangement, which was primarily aimed at preventing rogue nations and terrorists from acquiring goods with military applications. It also classified cryptography as a dual use good and placed limitations on usage and exports. However, due to public pressure from both business and private sectors, the arrangement was modified in 1998 to be less restrictive with respect to cryptography.

Market forces, along with growing electronic commerce, led to further relaxation of cryptography export policy in 2000. New export regulations published in January of 2000 made it much easier for companies and individuals in the US to export strong encryption enabled products. The four major features of the 2000 regulations were:

- "Retail" encryption products are widely exportable to all but certain "terrorist" nations though still subject to a government review and reporting requirements.
- Non-retail products are also exportable, subject to similar requirements, to most non-government users.
- Encryption products with less than 64-bit keys are freely exportable.
- Some non-proprietary source code is exportable to most countries after notice to the government. [12]

US export policy was revised again in June 2002 to allow mass-market encryption products with symmetric key lengths greater than 64-bits to be exported following a 30-day review. In addition the review processes has been streamlined to ease the export policy.

Effective December 9th, 2004, the Department of Commerce Bureau of Industry and Security (BIS) passed a final ruling that revises: the criteria for determining if a foreign made item

incorporating U.S. origin encryption is subject to the Export Administration Regulations; the notification requirements for beta test encryption software and certain “publicly available” encryption software; and the review and reporting requirements for exports and re-exports of certain encryption items under License Exception ENC that are neither “publicly available” nor eligible for “mass market” treatment. [22]

## *4.2 Usage Restrictions*

With the increasing amount of information available in digital form, the use of encryption to protect sensitive information from being accessible is becoming more widely used. One ongoing debate has been whether or not the United States government should be given access to all encrypted data so they can monitor possible illegal information. Over the years the United States government has tried, sometimes successfully and sometimes not, to pass a number of laws allowing government agencies such as the NSA, CIA, and FBI to have the ability to decrypt any message by circumventing the encryption scheme. Some of the problems with unlimited government access, which will be discussed below, are privacy rights of US citizens, limitations on advancements of cryptographic methods, and security issues with universal government keys. A summary of major government attempts to restrict and standardize encryption is included in the following sections.

### 4.2.1 The Computer Security Act

In 1987, the U.S. Congress, led by Rep. Jack Brooks, enacted a law reaffirming that the National Institute for Standards and Technology (NIST), a division of the Department of Commerce, was responsible for the security of unclassified, non-military government computer systems. Under the law, the role of the National Security Agency (NSA) was limited to providing technical assistance in the civilian security realm. Congress felt that it was inappropriate for a military intelligence agency to have control over the dissemination of unclassified information.

Since the enactment of the Computer Security Act, the NSA has sought to undercut NIST's authority. In 1989, NSA signed a Memorandum of Understanding (MOU) which purported to transfer back to NSA the authority given to NIST. The MOU created a NIST/NSA technical working group that developed the controversial Clipper Chip and Digital Signature Standard. The NSA has also worked in other ways to weaken the mandate of the CSA. In 1994, President Clinton issued Presidential Decision Directive (PDD) 29. This directive created the Security Policy Board, which has recommended that all computer security functions for the government be merged under NSA control.

### 4.2.2 The Clipper Chip

The Clipper Chip is a cryptographic device intended to protect private communications while at the same time permitting government agents to obtain the keys upon presentation of what has been vaguely characterized as "legal authorization." The keys are held by government escrow agents and would enable law enforcement to access the private communication. While Clipper would be used to encrypt voice transmissions, a similar chip known as Capstone would be used to encrypt data. The underlying cryptographic algorithm, known as Skipjack, was developed by the National Security Agency (NSA). The NSA has classified the Skipjack algorithm on national security grounds, thus precluding independent evaluation of the system's strength.

On Feb. 4, 1994, the White House announced the adoption of the Clipper Chip. After a public outcry however, the federal government eventually abandoned its plans to try to convince American businesses to build Clipper-enabled products. Even in the international arena, the U.S. government was unable to convince countries to support the use of devices such as the clipper chip.

### 4.2.3 Digital Signature Standard

The Digital Signature Standard (DSS) is a cryptographic standard promulgated by the National Institute of Standards and Technology (NIST) in 1994. It has been adopted as the federal standard for authenticating electronic documents, much as a written signature verifies the authenticity of a paper document. The DSS was the first cryptographic standard developed under the regime established by the Computer Security Act, which was intended to limit the role of the National Security Agency (NSA) in the development of civilian standards. Documents obtained by EPIC under the Freedom of Information Act have demonstrated that the DSS development process was, in fact, dominated by NSA.

### 4.2.4 Key Escrow and Key Recovery

Members of the law enforcement and intelligence communities continue to express concern about widespread use of unescrowed cryptography. At the same time, these communities have expressed increasing alarm over the vulnerability of "critical infrastructure." But there is a significant risk that widespread insertion of government-access key recovery systems into the information infrastructure will exacerbate, not alleviate, the potential for crime and information terrorism. Increasing the number of people with authorized access to the critical infrastructure and to business data will increase the likelihood of attack, whether through technical means, by exploitation of mistakes or through corruption. Furthermore, key recovery requirements, to the extent that they make encryption cumbersome or expensive, can have the effect of discouraging or delaying the deployment of cryptography in increasingly vulnerable computing and communications networks.

Key access schemes are considered by law enforcement agencies as a possible solution to cope with issues like encrypted messages. However these schemes raise a number of critical questions that would need to be carefully addressed before introducing them. The ongoing discussion of different legislative initiatives in the US is an illustrative example of the implied controversy. The most critical points are vulnerability, privacy, costs and effectiveness:

1. Inevitably, any key access scheme introduces additional ways to break into a cryptographic system. More people will know about "secret keys" and "system designs" leading to higher risks of insider abuse. These new vulnerabilities are complex and need to be understood as substantial liability and privacy questions are implied.

2. The costs associated with key access schemes can be very high. Until now, questions on costs and who would bear them have not been addressed by policy makers. Important cost factors would be the specific requirements of the schemes, e.g. response time to deliver keys, storage time for session keys, authenticate requesting government agency, secure transfer of recovered keys, internal security safeguards, etc. Furthermore, substantial and unknown costs would occur through the need for scalability of key access schemes, i.e. making it work in a multi-million user environment. Up to now, such systems have at best been developed for small scale use. The costs to make them work on a global wide scale needs to be looked at carefully.
3. Key access schemes can be easily circumvented - even if, hypothetically speaking, everyone would be forced to pass through these systems.

While key escrow has not been attempted on a wide scale in the United States, France passed a telecommunications law in 1996 requiring keys to be kept by trusted third parties who would turn them over to law enforcement when required. The technical and economic costs to implementing this program, as well as business pressures for open cryptography use caused a reversal of policy in 1998 where by trusted third parties were no longer required, keys could be 128-bits and the power to read encrypted communications was passed to the courts who were given authority and enforcement powers to force users to decrypt documents.

### 4.2.5 U.S. influence on International Policy

Even with critics pointing to all the flaws in key escrow and restrictions on encryption techniques, the United States government has continued trying to enact such policies not only in the U.S. alone, but worldwide. In 1996 the U.S. government began pressuring the Organization for Economic Cooperation (OECD), an international body consisting of 29 countries, to adopt key escrow as an international standard. The countries, however, were divided on the issue and this division shows in the eventual guidelines developed by the OECD. The guidelines attempt to accommodate for both sides by stating “The fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods”. However, they added the fact that “National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible” [23].

The European Union in particular has also taken issue with the United States' policies encouraging key escrow. Although a 1995 resolution required network operators to provide law enforcement agencies clear access to encrypted communications, the European Commission has since become more concerned with reducing controls on commercial encryption products. In a report published in October 1997, the Commission stated that "restricting the use of encryption could well prevent law-abiding companies and citizens from protecting themselves against criminal attacks," adding that key escrow systems "would not . . . totally prevent criminals from using these technologies" [23]. The report says that if such policies are necessary, they should be limited to the minimum of what is necessary.

Also in 1997, the U.S. met with 7 other top industrialized nations (G-8) and agreed that in order to counter the unlawful acts of terrorism around the world and its use in data encryption, they “invited all states to develop national policies on encryption, including key management, which may allow, consistent with these guidelines lawful government access to prevent and investigate acts of terrorism and to find a mechanism to cooperate internationally in implementing such policies.” At this point, it is clear that various countries have differing views on the topic of key escrow and there are still no internationally accepted key escrow policies.

### 4.2.6 House Resolution – HR2616

Due to both high internal and foreign opposition to a key escrow, the policy was never passed. Instead, the House of Representatives passed House Resolution – 2616 in late 1999, restricting the encryption bit lengths to 64-bit and under. The policy allows the use of any encryption algorithm or technique without the use of key escrow as long as the encryption bit length was under 64-bits.

### 4.2.7 USA PATRIOT Act (HR 3162)

Passed and signed by President Bush just 45 days after the world trade center and pentagon attacks of September 11, 2001, the USA PATRIOT Act was aimed to aid the gathering of intelligence and preventing further such attacks. Many topics that were being debated before were passed without much opposition due to the high pressure on congress and the President to take counter measures. The Patriot Act made amendments to many existing laws. The Electronic Communications Act was revised to give government access to stored email and other electronic communications. It includes the Pen Register and Trap and Trace statute. This effectively allows wire taps using a court order that does not require probable cause: there is no judicial discretion, and the court must authorize the surveillance upon government certification. A government attorney need only certify to the court that the "information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation." Therefore, the Pen Register and Trap and Trace statute lacks many of the privacy protections found in the wiretap statute.

Another law that the Patriot Act amended was the Foreign Intelligence Surveillance Act. This amendment authorizes the government to carry out electronic surveillance against any person, even American citizens, in the United States upon obtaining a judicial order based upon probable cause that the person is an agent of a foreign power. As with the Electronic Communications amendment, it does not offer many of the protections required under the federal wiretap statute.

### 4.2.8 National Intelligence Reform Bill (S 2845)

The National Intelligence Reform Bill, backed by President Bush, is currently being debated on the Senate floor. One of the bill's main concerns is the creation of a national security director. This position is of great importance given the amount of control over the $80 billion intelligence budget that the director would possess. If passed, the director would have great influence on the intelligence and encryption policies of the United States for years to come. Supporters of the bill argue for major reforms in the methods by which the U.S. gathers and handles intelligence in order to prevent large scale terrorist attacks. The national security director's powers would include setting standards and procedures for granting security clearance and recommending reforms to the President and heads of other federal agencies. In short, this bill would create a single post with the authority and influence over all other forms of intelligence gathering in the United States, including encryption policies.

## *4.3 Government Supported R&D*

Dating back to before World War I, when the British Government established the British Secret Service Bureau to gather and decode German messages, governments have had a major influence on the research and development of encryption technologies. The United States government too has a history of funding cryptographic research, such as the VERONA project, to meet the needs of the times. In large part due to the terrorist attacks of 9/11, Congress passed in 2002 the Cyber Security Research and Development Act which authorized nearly $900 million in long-term cyber security R&D at the National Science Foundation and National Institute of Standards and Technology (approximately $64 million spent in 2004 by the NSF and $15 million for the NIST). Most security experts believe the President's current budget requests continue to under fund this critical area of research at both NSF and NIST, as well as at the Department of Homeland Security.

- Information technology systems underpin key industries such as telecommunications and financial services, and also play a vital role in the smooth functioning of critical infrastructure and services, such as transportation systems, the electric power grid, and emergency response capabilities.
- Over 137,000 individual cyber attacks were reported in 2003.
- Out of a science and technology budget of over $800 million in FY 2004, the Department of Homeland Security targeted only $18 million on cybersecurity research and development.
- Despite the dangers of security flaws in these basic foundations of our economy, $22 million was cut from NIST's funding forcing a reduction in the ability to improve on the country's growing need for security research and the agency's work in helping other government agencies with their security flaws.
- Even with extra funding, there is a need for better coordination among the different agencies.

Many speculate that the government is spending more money on the problem of encryption and cyber security than is reported. The National Security Agency, part of the United States department of defense, has an annual budget of about $7 billion. The work done by the NSA however, is mostly classified, hiding it from many top research experts in the academic and commercial world. According to the agency, they had no trouble keeping track of wanted terrorist Osama Bin Laden in the 1990's. But the explosion of communications technology such as cell phones, digital communications and advanced encryption software they could no longer track down their foe.

# 5 Cryptography policy analysis

The effectiveness and results of US cryptography policy through the last century must be evaluated with respect to national security, business concerns and personal liberties. Cryptography evolved over the course of the century from being in the exclusive domain of governments for protecting state secrets to being involved in nearly every aspect the information society. While cryptography is not a stand-alone solution and any use of cryptography must be coupled with social engineering aspects, non-technical approaches cannot compensate for a weak or misguided cryptography policy. Weaknesses in cryptography methods and use can have dire consequences for business, governments, personal privacy and human lives.

## *5.1 Personal Liberties and Privacy*

Personal liberties and privacy concerns in the United States and abroad have become increasingly visible as the information and digital eras have emerged. The open nature of the Internet allows unprecedented access to information and the ability for an individual to disseminate thoughts, ideas and observations to disparate audiences. However, with this openness comes an increased vulnerability of critical personal information. In the wrong hands, personal information and communications could be used to suppress free speech, exploit or intimidate. Cryptography can secure personal information by enabling encrypted communications, data source and identity authentication and access control. However, cryptography policy, for much of the 20th century, was primarily focused on national security and failed to protect individuals in a number of ways.

A containment oriented export policy damaged personal privacy in the United States. Restrictions on the strength of encryption that could be exported led to two important trends in software products: the lowest common denominator in encryption technology was deployed in order to reach the widest possible audience and users tended to use the weaker of two products when both were available. For example, Netscape developed two different versions of its Navigator web browser in the mid 1990s: one with 40-bit encryption intended for international users and one with 128-bit encryption for domestic users. However, because of the difficulties involved for domestic users in getting the 128-bit version most used the much weaker 40-bit version. In addition, many believe that restrictive export controls led to software vendors to not only choose the lowest common denominator, but to exclude encryption from products such as operating systems in order to reach a larger market. Ultimately, encryption export policy failed to keep up with the changing market forces and placed weak encryption in the hands of consumers jeopardizing personal privacy. Export policies changed, but not before weak products were in the hands of consumers and much of the infrastructure of the Internet and ecommerce was in place.

## *5.2 National Security*

Cryptography policy and national security have a long and intertwined history and because of the secret nature of intelligence gathering and counter intelligence it is difficult to fully assess the impact that cryptography policy has had upon national security. Prior to the information age, cryptography policy with respect to national security was straightforward: policies that supported developing more advanced encryption and cryptanalysis techniques while denying them to the rest of the world enhanced national security. National security and information gathering are threatened by cryptography in a two separate ways: [12]:

- Strong cryptography can prevent any given message from being understood.
- Any form of cryptography, strong or weak, if practiced on a widespread basis, increases the cost of signals analysis by increasing the amount of work that must be done to find interesting messages.

When considering the ways that cryptography threatens national security, the polices of containment pursued by the government in the mid to late 20th century were well suited for

denying cryptography to foreign entities and were effective until the emergence of the digital and information ages.

With the emergence of the information and digital ages, analyzing cryptography policy is less straightforward. Policy that protects American cryptography techniques and abilities from spreading may in the long run, negatively impact the information gathering and protection abilities of our national security agencies. Foreign entities and governments had a growing interest in applying cryptography in information security that led to growth of foreign cryptography products and research. Foreign development of new cryptographic algorithms and the training of new cryptanalysts is detrimental to the United States in that there are more people able to correctly apply cryptography to enable information security and the cost of U.S. information protection and analysis are increased.

As mentioned in section 4.1, the United States' policy of cryptography containment ultimately failed under technological and market pressures, with the exception of a few cases. However, for many years it was successful in giving signal intelligence an advantage in analysis and decryption of electronic communications that resulted in many political and military successes. Recently important Al-Qaeda files were recovered as a direct result of export restrictions. The files were encrypted using a weak 40-bit encryption scheme that is inferior to the 128-bit versions available in the US. By delaying wide spread use of strong cryptography for as long as possible and by limiting market knowledge of cryptography, many non-government organizations that are targets of signal intelligence are still using weak cryptographic products.

## *5.3 Law Enforcement*

Law enforcement agencies have two main roles: crime prevention and prosecution. Information gathering is critical to both these aspects. FBI director Louis Freeh argued in 1995 that: "unless the issue of encryption is resolved soon, criminal conversations over the telephone and other communications devices will become indecipherable by law enforcement. This, as much as any issue, jeopardizes the public safety and national security of this country. Drug cartels, terrorists, and kidnappers will use telephones and other communications media with impunity knowing that their conversations are immune from our most valued investigative technique." Depending on the role, cryptography can be either aid or a hinder law enforcement agencies. Cryptography can aid crime prevention by securing personal information and corporate trade secrets. However, cryptography, when employed by criminals can have significant impact on prevention and prosecution. National cryptography policy has had both successes and failures with respect to law enforcement as information has moved to the digital age.

Restrictive export policies, as mentioned in previous sections, besides delaying widespread use of strong cryptography also limited use of cryptography in the domestic market. From a law enforcement point of view, restrictive export policy denied criminals easy access to cryptography which simplifies and reduces the cost of intelligence gathering. As the National Research Council's 1996 study stated: "As a general rule, criminals are most likely to use what is available to the general public, and the encryption available to and usable by the public has to date been minimal". On the other hand, because domestic users were also denied strong cryptography software, their vulnerability to Internet-based criminals was increased. Many criminals do have, and will use cryptography to secure their communications and data.

White collar criminals and drug traffickers stand out from many ordinary criminals that are oriented towards physical crimes in several ways: they are well funded, have many resources at their disposals, are often better educated and often keep detailed records of their activities. Wealthy and sophisticated criminals are more likely to have access to and use cryptography. Escrowed encryption and restrictive export controls were two ways in which cryptographic policy addressed the need to keep cryptography out of the hands of criminals, or at least allow law enforcement back door access to encrypted messages and data. However, the implementation failure of both these policies, export policy in failing to stop the spread of strong encryption, and

escrowed encryption in failing to become widely adopted, hinders law enforcement's efforts to prevent and prosecute crimes.

## 5.4 Business

For many years, business desires and the goals of public cryptographic policy were in direct contention. Government policy aimed to limit the spread of cryptography technology and place severe limitations on cryptographic use, both domestically and internationally. However, for many years, there was little or no market for cryptography enabled products and the impact on businesses were negligible.

As computers moved from research and government settings to commercial applications, the demand for cryptography grew from the value and vulnerabilities of electronic information. Adding additional pressures for public policy reform came from the increasing important role played by international markets and the increasing value of information transacted in electronic form. Public policy has become more favorable towards business applications of cryptography by loosening export restrictions, publishing encryption standards, and supporting research and development efforts. However, because public policy changed as an evolutionary process rather then from market analysis and predicting technological directions, United States businesses suffered.

Cryptography export policy directly impacted businesses' ability to capture international market share. Export policy drove vendors to a lowest common denominator technology that would pass export review and sell in the domestic market. In addition, because of the limited options for foreign businesses in purchasing cryptography, the number of international cryptography vendors grew under strict export control. These two factors hampered US businesses' ability to garner market share in the important international market by reducing the relative quality of US products and increasing the cost of entry. Had cryptographic policy been more supportive of cryptography consumers and vendors in the international market as the Internet and e-commerce emerged as major components of the domestic and international economies, US businesses would have been in a better position to grow and expand into overseas markets.

## 5.5 Research

There is an ongoing need to continue open-world research funding into both cryptography and cryptanalysis. Most governments focus their cryptographic research in the military-sector. While this is understandable, those efforts often have limited, or no, publications in the open literature. Since the university engineering community must work from the open literature, it is important that open-world research continues in the future.

However, current university research funding trends are not representative of this ongoing need. Research funding in the computer science field is sub par. About $55 billion of the nations $2,319 billion budget goes towards basic research, and of that $55 billion, approximately 4% goes towards IT research[17]. Further, within the available IT research funds, cryptography research suffers even further because of its supposed implications on national security.

Although government must balance the goals of innovation and national security, they are not mutually exclusive. Increasing cryptography research funding will lead to improved technologies, stronger encryption schemes, and maybe most importantly, ways to allow use of those improved technologies domestically while being able to control or disable their use in the rest of the world.

# 6 Conclusions

The current state of technology is such that it is impossible to keep strong encryption schemes out of the hands of our adversaries. The Internet facilitates rapid access to information, making it difficult for monitoring agencies to stop protected information and data from spreading. Because there is virtually no cost for making digital copies of information, one program or paper released onto the net can serve as the seed for an infinite number of perfect copies. The realities of the Internet have forced government policies to change because of technical limitations and increasing demand for information security

Government policies that restrict cryptography use, development and export are outdated and impractical. Strong cryptography is available to nearly any corporation or citizen and policies that relied on, or promoted limited use of cryptography are bound to be marked by more failures than successes. However, cryptography is not a stand-alone solution. There are many ways to access private information – restricted information will always be attacked at its weakest perceived point – including installation of key loggers, disgruntled employees, poor password policies, weak network security, poor choice of cryptographic keys, weak key escrow systems and so forth.

Government policy should therefore focus on strengthening cryptography usage, implementation, and awareness and promote good practices that address weaknesses in information security. Strong cryptography is available to our enemies and they are using it. Government policy should take steps to ensure that our privacy, national security and business interests are advanced and strengthened. Non-cryptography aspects are now the weakest link in information security and must be aggressively strengthened on the domestic front.

In order to strengthen usage patterns domestically, government should publish standards for the many technological and social aspects of cryptography and information security. It should educate the implementers and users of cryptography-enabled products and promote widespread use of cryptography. Further, it is important for government to increase funding into cryptographic research. Doing so will facilitate stronger encryption schemes that are developed in the United States, and are better understood by Americans. If current funding trends continue, not only will the progression of American cryptographic techniques be slowed tremendously, but it will allow other countries and entities to move forward more quickly, and Americans will be responsible for the majority of encryption misuse.

# 7 References

[1] Mihir Bellare, *Introduction to Modern Cryptography*, http://www.cse.ucsd.edu/users/mihir/cse107/classnotes.html.

[2] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, *Handbook of Appied Cryptography*, http://www.cacr.math.uwaterloo.ca/hac/ Fifth Printing, August 2001.

[3] David Kahn, *The Codebreakers : The Comprehensive History of Secret Communication from Ancient Times to the Internet*, May 1996.

[4] *Wikipedia, the free encyclopedia*, http://en.wikipedia.org/wiki/

[5] Farlex, *The Free Dictionary*, http://encyclopedia.thefreedictionary.com/

[6] Patrick Beesly, *Room 40: British Naval Intelligence, 1914-1918*, 1982.

[7] *WorldHistory.com*, http://www.worldhistory.com

[8] Global Internet Liberty Campaign, *Cryptography and liberty – An International Survey of Encryption Policy*, February 1998.

[9] Electronic Privacy Information Center (EPIC), *Cryptography Policy*, http://www.epic.org/crypto/, October 2001.

[10] T. Kohno *et al.*, *Analysis of an Electronic Voting System*, *IEEE Symposium on Security and Privacy* (May 2004)

[11] J. Vega, *Open Source Security: Still a Myth*, ONLamp.com (9/16/2004)

[12] National Research Council, Computer Science and Telecommunications Board, *Cryptography's Role In Securing the Information Society*, 1996.

[13] http://www.wwnorton.com/college/polisci/lowi/glossp.htm
[14] https://web.lexis-nexis.com/universe /academic
[15] https://web.lexis-nexis.com/congcomp/
[16] http://library2.cqpress.com/cqresearcher

[17] Ed Lazowska, *The IT Innovation Ecosystem*, Autumn 2004.
http://www.cs.washington.edu/education/courses/csep590tu/04au/lectures/slides/class2b.pdf

[18] http://www.usun-vienna.usia.co.at/wassenaar/

[19] http://www.rsasecurity.com/rsalabs/node.asp?id=2335

[20] http://www.worldhistory.com/wiki/E/Export-of-cryptography.htm

[21] http://www.praxagora.com/andyo/ar/crypto_reversal.html

[22] Federal Register, Vol. 69, No. 263 http://www.access.gpo.gov/su_docs/aces/fr-cont.html, December 2004.

[23] Electronic Privacy Information Center (EPIC), *Cryptography & Liberty 1999: An International Survey of Encryption Policy*, June, 1999.