CHAPTER 6
Laws Concerning Cryptography

This chapter deals with the legal and political issues associated with cryptography, including government involvement, patent issues, and import and export regulations. Note that while this chapter includes legal information, it should not be used as a substitute for consulting an attorney (see below).

6.1 LEGAL DISCLAIMER

The materials should not be treated or relied upon as advice on technical and non-technical issues and the materials have not been updated to reflect recent changes in technology, the law, or any other areas. Furthermore, RSA cannot warrant that the information herein is complete or accurate and does not assume, and hereby disclaims, any liability to any person for any loss or damage caused by errors or omissions in the FAQ resulting from negligence, accident or any other cause.

6.2 GOVERNMENT INVOLVEMENT

6.2.1 What is NIST?

NIST is an acronym for the National Institute of Standards and Technology, a division of the U.S. Department of Commerce. NIST was formerly known as the National Bureau of Standards (NBS). Through its Computer Systems Laboratory it aims to promote open systems and interoperability that will spur the development of computer-based economic activity. NIST issues standards and guidelines intended to be adopted in all computer systems in the U.S., and also sponsors workshops and seminars. Official standards are published as FIPS (Federal Information Processing Standards) publications.

In 1987 Congress passed the Computer Security Act, which authorized NIST to develop standards for ensuring the security of sensitive but unclassified information in government computer systems. It encouraged NIST to work with other government agencies and private industry in evaluating proposed computer security standards.

NIST issues standards for cryptographic algorithms that U.S. government agencies are required to use. A large percentage of the private sector often adopts them as well. In January 1977, NIST declared DES (see Section 3.2) the official U.S. encryption standard and published it as FIPS 46; DES soon became a de facto standard throughout the United States. NIST is currently taking nominations for the Advanced Encryption Standard (AES), which is to replace DES (see Section 3.3). There is no definite deadline for the completion of the AES (see Question 3.3.3).

Several years ago, NIST was asked to choose a set of cryptographic standards for the U.S., this has become known as the Capstone project (see Question 6.2.3). After a few years of rather secretive deliberations, NIST, in cooperation with the NSA (see Question 6.2.2), issued proposals for various standards in cryptography. The combination of these proposals, including digital signatures (DSS, see Question 3.4.1) and data encryption (the Clipper chip, see Question 6.2.4), formed the Capstone project.

NIST has been criticized for allowing the NSA too much power in setting cryptographic standards, since the interests of the NSA sometimes conflict with that of the Commerce Department and NIST. Yet, the NSA has much more experience with cryptography, and many more qualified cryptographers and cryptanalysts than does NIST so it is perhaps unrealistic to expect NIST to forego such readily available assistance.

For more information on NIST, visit their web site at

http://www.nist.gov/ .

6.2.2 What is the NSA?

NSA is the National Security Agency, a highly secretive agency of the U.S. government created by Harry S. Truman in 1952. The NSA's very existence was kept secret for many years. For a history of the NSA, see Bamford [Bam82]. The NSA has a mandate to listen to and decode all foreign communications of interest to the security of the United States. It has also used its power in various ways to slow the spread of publicly available cryptography in order to prevent national enemies from employing encryption methods that are presumably too strong for the NSA to break.

As the premier cryptographic government agency, the NSA has huge financial and computer resources and employs a host of cryptographers. Developments in cryptography achieved at the NSA are not made public; this secrecy has led to many rumors about the NSA's ability to break popular cryptosystems like DES (see Section 3.2), as well as rumors that the NSA has secretly placed weaknesses, called "trapdoors," in government-endorsed cryptosystems. These rumors have never been proved or disproved. Also the criteria used by the NSA in selecting cryptography standards have never been made public.

Recent advances in the computer and telecommunications industries have placed NSA actions under unprecedented scrutiny, and the agency has become the target of heavy criticism for hindering U.S. industries that wish to use or sell strong cryptographic tools. The two main reasons for this increased criticism are the collapse of the Soviet Union and the development and spread of commercially available public-key cryptographic tools. Under pressure, the NSA may be forced to change its policies.

The NSA's charter limits its activities to foreign intelligence. However, the NSA is concerned with the development of commercial cryptography, since the availability of strong encryption tools through commercial channels could impede the NSA's mission of decoding international communications. In other words, the NSA is worried that strong commercial cryptography may fall into the wrong hands.

The NSA has stated that it has no objection to the use of secure cryptography by U.S. industry. It also has no objection to cryptographic tools used for authentication, as opposed to privacy. However, the NSA is widely viewed to be following policies that have the practical effect of limiting and/or weakening the cryptographic tools used by law-abiding U.S. citizens and corporations; see Barlow [Bar92] for a discussion of NSA's effect on commercial cryptography.

The NSA exerts influence over commercial cryptography in several ways. NSA serves as an advisor to the Bureau of Export Administration (BXA) at the Commerce Department, which is the front-line agency on export determination. In the past, BXA generally has not approved export of products used for encryption unless the key size is strictly limited. It did, however, approve export of any products used for authentication purposes only, no matter how large the key size, as long as the product cannot be easily converted to be used for encryption. Today the situation is different with dramatically relaxed restrictions on export regulations. The NSA has also blocked encryption methods from being published or patented, citing a national security threat; see [Lan88] for a discussion of this practice.

Additionally, the NSA serves an "advisory" role to NIST in the evaluation and selection of official U.S. government computer security standards. In this capacity, it has played a prominent and controversial role in the selection of DES and in the development of the group of standards known as the Capstone project. The NSA can also exert market pressure on U.S. companies to produce (or refrain from producing) cryptographic goods, since the NSA itself is often a large customer of these companies. Examples of NSA-supported goods include Fortezza (see Question 6.2.6), the Defense Messaging System (DMS), and MISSI, the Multilevel Information System Security Initiative.

Cryptography is in the public eye as never before and has become the subject of national public debate. The status of cryptography, and the NSA's role in it, will probably continue to change over the next few years.

6.2.3 What is Capstone?

Capstone has been the U.S. government's long-term project to develop a set of standards for publicly available cryptography, as authorized by the Computer Security Act of 1987. The primary agencies responsible for Capstone were NIST and the NSA (see Question 6.2.2). The plan called for the elements of Capstone to become official U.S. government standards, in which case both the government itself and all private companies doing business with the government would have been required to use Capstone. However, Capstone is no longer an active development initiative.

There are four major components of Capstone: a bulk data encryption algorithm, a digital signature algorithm, a key exchange protocol, and a hash function. The data encryption algorithm is called Skipjack, often referred to as Clipper (see Question 6.2.4), which was the encryption chip that included the Skipjack algorithm. The digital signature algorithm is DSA (see Section 3.4) and the hash function used is SHA-1 (see Question 3.6.5). The key exchange protocol is not published, but is generally considered to be related to Diffie-Hellman (see Question 3.6.1).

The Skipjack algorithm and the concept of a Law Enforcement Access Field (LEAFs, see Question 7.13) have been accepted as FIPS 185; DSS has been published as FIPS 186, and finally SHS has been published as FIPS 180.

All parts of Capstone were aimed at the 80-bit security level. The symmetric-keys involved were 80 bits long and other aspects of the algorithm suite were designed to withstand an "80-bit" attack, that is, an effort equivalent to 2^{80} operations.

6.2.4 What is Clipper?

Clipper chip techN ology was proposed by the U.S. Government during the mid-1990s, but is no longer being actively promoted for general use. The Clipper chip contains an encryption algorithm called Skipjack (see Question 6.2.3). Each chip contains a unique 80-bit unit key U, which is escrowed in two parts at two escrow agencies; both parts must be known in order to recover the key. Also present is a serial number and an 80-bit "family key" F; the latter is common to all Clipper chips. The chip is manufactured so that it cannot be reverse engineered; this means that the Skipjack algorithm and the keys cannot be recovered from the chip.

As specified by the Escrowed Encryption Standard, when two devices wish to communicate, they first agree on an 80-bit "session key" K. The method by which they choose this key is left up to the implementer's discretion; a public-key method such as RSA or Diffie-Hellman seems a likely choice. The message is encrypted with the key K and sent (note that the key K is not escrowed.) In addition to the encrypted message, another piece of data, called the law-enforcement access field (LEAF, see Question 7.13), is created and sent. It includes the session key K encrypted with the unit key U, then concatenated with the serial number of the sender and an authentication string, and then, finally, all encrypted with the family key. The exact details of the law-enforcement access field are classified. The receiver decrypts the law-enforcement access field, checks the authentication string, and decrypts the message with the key K.

Now suppose a law-enforcement agency wishes to "tap the line." It uses the family key to decrypt the law-enforcement access field; the agency now knows the serial number and has an encrypted version of the session key. It presents an authorization warrant to the two escrow agencies along with the serial number. The escrow agencies give the two parts of the unit key to the law-enforcement agency, which then decrypts to obtain the session key K. Now the agency can use K to decrypt the actual message. Further details on the Clipper chip operation, such as the generation of the unit key, are sketched by Denning [Den93].

Matt Blaze, AT&T, showed that it is possible to modify the LEAF in a way such that law enforcement cannot determine where the message originally came from [Bla94].

The Clipper chip proposal aroused much controversy and was the subject of much criticism. Unfortunately, two distinct issues became confused in the large volume of public comment and discussion.

First there was controversy about the whole idea of escrowed keys. It is essential for the escrow agencies to keep the key databases extremely secure, since unauthorized access to both escrow databases could allow unauthorized eavesdropping on private communications. In fact, the escrow agencies were likely to be one of the major targets for anyone trying to compromise the Clipper system. The Clipper chip factory was another likely target. Those in favor of escrowed keys saw it as a way to provide secure communications for the public at large while allowing law-enforcement agencies to monitor the communications of suspected criminals. Those opposed to escrowed keys saw it as an unnecessary and ineffective intrusion of the government into the private lives of citizens. They argued that escrowed keys infringe their rights of privacy and free speech. It will take a lot of

time and much public discussion for society to reach a consensus on what role, if any, escrowed keys should have.

The second area of controversy concerned various objections to the specific Clipper proposal, that is, objections to this particular implementation of escrowed keys, as opposed to the idea of escrowed keys in general. Common objections included: the key escrow agencies will be vulnerable to attack; there are not enough key escrow agencies (the current escrow agents are NIST and the automated systems division of the department of treasury [DB95]); the keys on the Clipper chips are not generated in a sufficiently secure fashion; there will not be sufficient competition among implementers, resulting in expensive and slow chips; software implementations are not possible; and the key size is fixed and cannot be increased if necessary.

Micali [Mic93] has proposed an alternative system that also attempts to balance the privacy concerns of law-abiding citizens with the investigative concerns of law-enforcement agencies. He called his system fair public-key cryptography. It is similar in function and purpose to the Clipper chip proposal but users can choose their own keys, which they register with the escrow agencies. Also, the system does not require secure hardware, and can be implemented completely in software. Desmedt [Des95] has also developed a secure software-based key escrow system that could be a viable alternative. There have been numerous other proposals in the cryptographic community over the last few years; Denning and Branstad give a nice survey [DB95].

6.2.5 What is the Current Status of Clipper?

Clipper has been accepted as FIPS 185 [NIS94a] by the federal government. Various forms of the Clipper chip were produced; however, it is no longer in production. The chip is still used in the AT&T TSD 3600 and in various Fortezza products (see Question 6.2.6), including PC Cards, encrypting modems, and PCI board Fortezza. All Capstone-based products have suppressed LEAF (see Question 7.13) escrow access function. There is now a CA (Certifying Authority) performing key recovery.

6.2.6 What is Fortezza?

The Fortezza Crypto Card, formerly called Tessera, is a PC card (formerly PCMCIA, Personal Computer Memory Card International Association) developed by NSA that implements the Capstone algorithms. The card provides security through verification, authentication, non-repudiation, and encryption.

Fortezza is intended for use with the Defense Messaging Service (DMS) and is export controlled. A number of vendors have announced support for the Fortezza card; NSA has also built and demonstrated a PKCS #11-based library (see Question 5.3.3) that interfaces to the card.

Currently, the NSA is working with companies, such as VLSI, to develop commercial products that implement Fortezza algorithms. VLSI is devising a "Regent" chip that adds DES and RSA algorithms. The NSA also supports commercial development of smart card chips with Fortezza algorithm capability.

6.3 PATENTS ON CRYPTOGRAPHY

6.3.1 Is RSA patented?

The patent for the RSA algorithm (U.S. Patent 4,405,829) was issued on September 20, 1983, exclusively licensed to RSA Security Inc. by the Massachusetts Institute of Technology, with an expiration date of September 20, 2000. RSA Security maintained a standard, royalty-based licensing policy that could be modified for special circumstances. In the U.S., a license has been needed to "make, use or sell" products that included the RSA algorithm. However, RSA Security has long allowed free non-commercial use of the RSA algorithm, with written permission, for academic or university research purposes.

On September 6, 2000, RSA Security made the RSA algorithm publicly available and waived its rights to enforce the RSA patent for any development activities that include the algorithm occurring after September 6, 2000. From this date forward, companies are able to develop products that incorporate their own implementation of the RSA algorithm and sell these products in the U.S.

For more information on the RSA patent, see

http://www.rsasecurity.com/developers/total-solution/faq.html .

(Question updated 9/13/2000)

6.3.2 Is DSA patented?

David Kravitz, former member of the NSA, holds a patent on DSA [Kra93]. Claus P. Schnorr has asserted that his patent [Sch91] covers certain implementations of DSA. RSA Security has also asserted coverage of certain implementations of DSA by the Schnorr patent.

6.3.3 Is DES patented?

U.S. Patent 3,962,539, which describes the Data Encryption Standard (DES), was assigned to IBM Corporation in 1976. IBM subsequently placed the patent in the public domain, offering royalty-free licenses conditional on adherence to the specifications of the standard. The patent expired in 1993.

6.3.4 Are elliptic curve cryptosystems patented?

Elliptic curve cryptosystems, as introduced in 1985 by Neal Koblitz and Victor Miller, have no general patents, though some newer elliptic curve algorithms and certain efficient implementation techniques may be covered by patents.
Here are some relevant implementation patents.

- Apple Computer holds a patent on efficient implementation of odd-characteristic elliptic curves, including elliptic curves over $GF(p)$ where p is close to a power of 2.
- Certicom holds a patent on efficient finite field multiplication in normal basis representation, which applies to elliptic curves with such a representation
- Cylink also holds a patent on multiplication in normal basis

Certicom also has two additional patents pending. The first of these covers the MQV (Menezes, Qu, and Vanstone) key agreement technique. Although this technique may be implemented as a discrete log system, a number of standards bodies are considering adoption of elliptic-curve-based variants. The second patent filing treats techniques for compressing elliptic curve point representations to achieve efficient storage in memory.

In all of these cases, it is the implementation technique that is patented, not the prime or representation, and there are alternative, compatible implementation techniques that are not covered by the patents. One example of such an alternative is a polynomial basis implementation with conversion to normal basis representation where needed. (This should not be taken as a guarantee that there are no other patents, of course, as this is not a legal opinion.) The issue of patents and representations is a motivation for supporting both representations in the IEEE P1363 and ANSI X9.62 standards efforts.

The patent issue for elliptic curve cryptosystems is the opposite of that for RSA and Diffie-Hellman, where the cryptosystems themselves have patents, but efficient implementation techniques often do not.

6.3.5 What are the important patents in cryptography?

Here is a selection of some of the important and well established patents in cryptography, including several expired patents of historical interest. The expiration date for patents used to be 17 years after issuing, but for outstandning patents as of June 8, 1995 (the day the United States ratified the GATT patent treaty), the expiration date is 17 years after the date of issue or 20 years after the date of filing, whichever is later. Today, the expiration date for U.S. patents is 20 years from filing, pursuant to the international standard.

DES

Inventors: Ehrsam et al.

U.S. Patent: 3,962,539
Filed: February 24, 1975
Issued: June 8, 1976
Assignee: IBM

This patent covered the DES cipher and was placed in the public domain by IBM. It is now expired.

Diffie-Hellman

Inventors: Hellman, Diffie, and Merkle

U.S. Patent: 4,200,770
Filed: September 6, 1977
Issued: April 29, 1980
Assignee: Stanford University

This is the first patent covering a public-key cryptosystem. It describes Diffie-Hellman key agreement, as well as a means of authentication using long-term Diffie-Hellman public keys. This patent is now expired.

Public-key cryptosystems

Inventors: Hellman and Merkle

U.S. Patent: 4,218,582
Filed: October 6, 1977
Issued: August 19, 1980
Assignee: Stanford University

The Hellman-Merkle patent covers public-key systems based on the knapsack problem and now known to be insecure. Its broader claims cover general methods of public-key encryption and digital signatures using public keys. This patent is expired.

RSA

Inventors: Rivest, Shamir, and Adelman

U.S. Patent: 4,405,829
Filed: December 14, 1977
Issued: September 20, 1983
Assignee: MIT

This patent describes the RSA public-key cryptosystem as used for both encryption and signing. It served as the basis for the founding of RSADSI.

Fiat-Shamir identification

Inventors: Shamir and Fiat

U.S. Patent: 4,748,668
Filed: July 9, 1986
Issued: May 31, 1988
Assignee: Yeda Research and Development (Israel)

This patent describes the Fiat-Shamir identification scheme.

Control vectors

Inventors: Matyas, Meyer, and Brachtl

U.S. Patent: 4,850,017
Filed: May 29, 1987
Issued: July 18, 1989
Assignee: IBM

Patent 4,850,017 is the most prominent among a number describing the use of control vectors for key management. This patent describes a method enabling a description of privileges to be bound to a cryptographic key, serving as a deterrent to the key's misuse.

GQ identification

Inventors: Guillou and Quisquater

U.S. Patent: 5,140,634
Filed: October 9, 1991
Issued: August 18, 1992
Assignee: U.S. Phillips Corporation

This patent describes the GQ identification scheme.

IDEA

Inventors: Lai and Massey

U.S. Patent: 5,214,703
Filed: January 7, 1992
Issued: May 25, 1993
Assignee: Ascom Tech AG (Switzerland)

Patent 5,214,703 covers the IDEA block cipher, an alternative to DES that employs 128-bit keys.

DSA

Inventor: Kravitz

U.S. Patent: 5,231,668
Filed: July 26, 1991
Issued: July 27, 1993
Assignee: United States of America

This patent covers the Digital Signature Algorithm (DSA), the algorithm specified in the Digital Signature Standard (DSS) of the U.S. National Institute of Standards (NIST).

Fair cryptosystems

Inventor: Micali

U.S. Patent: 5,315,658
Filed: April 19, 1993
Issued: May 24, 1994
Assignee: none

This patent covers systems in which keys are held in escrow among multiple trustees, only a specified quorum of which can reconstruct these keys.

6.4 UNITED STATES CRYPTOGRAPHY EXPORT/IMPORT LAWS

We remind the reader of the Legal Disclaimer in Section 6.1. For correct and updated information on United States cryptography export/import laws, contact the Bureau of Export Administration (BXA) (http://www.bxa.doc.gov/).

For many years, the U.S. government did not approve export of cryptographic products unless the key size was strictly limited. For this reason, cryptographic products were divided into two classes: products with "strong" cryptography and products with "weak" (that is, exportable) cryptography. Weak cryptography generally means a key size of at most 56 bits in symmetric algorithms, an RSA modulus of size at most 512 bits, and an elliptic curve key size of at most 112 bits (see Question 6.5.3). It should be noted that 56-bit DES and RC5 keys have been cracked (see Question 2.4.4), as well as a 512-bit RSA key (see Question 2.3.6).

In January 2000, the restrictions on export regulations were dramatically relaxed. Today, any cryptographic product is exportable under a license exception (that is, without a license) unless the end-users are foreign governments or embargoed destinations (Cuba, Iran, Iraq, Libya, North Korea, Serbia, Sudan, Syria, and Talisman-controlled areas of Afghanistan as of January 2000). Export to government end-users may also be approved, but under a license.

6.4.1 Can the RSA algorithm be exported from the United States?

Export of the RSA algorithm falls under the same U.S. laws as all other cryptographic products (see the beginning of Section 6.4).

Earlier, the RSA algorithm used for authentication was more easily exported than RSA used for privacy. In the former case, export was allowed regardless of key (modulus) size, although the exporter had to demonstrate that the product could not be easily converted to use the RSA algorithm for encryption. The RSA algorithm for export was generally limited to 512 bits for key management purposes, while the use of RSA for data encryption was generally prohibited.

Regardless of U.S. export policy, RSA has been available abroad in non-U.S. products for several years.

6.4.2 Can DES be exported from the United States?

For a number of years, the government rarely approved the export of DES for use outside of the financial sector or by foreign subsidiaries of U.S. companies. Some years ago, export policy was liberalized to permit unrestricted exportation of DES to companies that demonstrate plans to implement key recovery systems in a few years. Today, export of DES is decontrolled in accordance with the Wassenaar Arrangement.

Triple-DES is exportable under the regulations described in the beginning of Section 6.4.

6.4.3 Why is cryptography export-controlled?

Cryptography is export-controlled for several reasons. Strong cryptography can be used for criminal purposes or even as a weapon of war. During wartime, the ability to intercept and decipher enemy communications is crucial. For that reason, cryptographic technologies are subject to export controls.

In accordance with the Wassenaar Arrangement (see Question 6.5.3), U.S. government agencies consider strong encryption to be systems that use RSA with key sizes over 512 bits or symmetric algorithms (such as triple-DES, IDEA, or RC5) with key sizes over 56 bits. Since government encryption policy is heavily influenced by the agencies responsible for gathering domestic and international intelligence (the FBI and NSA, respectively) the government is compelled to balance the conflicting requirements of making strong cryptography available for commercial purposes while still making it possible for those agencies to break the codes, if need be. As already mentioned several times in this section, the major restrictions on export regulations were eliminated in the beginning of the year 2000.

To most cryptographers, the above level of cryptography -- 512 for RSA and 56 for symmetric algorithms -- is not considered "strong" at all. In fact, it is worth noting that RSA Laboratories has considered this level of cryptography to be commercially inadequate for several years.

Government agencies often prefer to use the terms "strategic" and "standard" to differentiate encryption systems. "Standard" refers to algorithms that have been drafted and selected as a federal standard; DES is the primary example. The government defines "strategic" as any algorithm that requires "excessive work factors" to successfully attack. Unfortunately, the government rarely publishes criteria for what it defines as "acceptable" or "excessive" work factors.

6.4.4 Are digital signature applications exportable from the United States?

Digital signature applications are one of the nine special categories of cryptography that automatically fall under the more relaxed Commerce regulations; digital signature implementations using RSA key sizes in excess of 512 bits were exportable even before the year 2000. However, there were some restrictions when developing a digital signature application using a reversible algorithm (that is, the signing operation is sort of the reverse operation for encryption), such as RSA. In this case, the application should sign a hash of the message, not the message itself. Otherwise, the message had to be transmitted with the signature appended. If the message was not transmitted with the signature, the NSA considered this quasi-encryption and the State controls would apply.

6.5 CRYPTOGRAPHY EXPORT/IMPORT LAWS IN OTHER COUNTRIES

6.5.1 What are the cryptographic policies of some countries?

This section gives a very brief description of the cryptographic policies in twelve countries. We emphasize that the laws and regulations are continuously changing, and the information given here is not necessarily complete or accurate. For example, export regulations in several countries are likely to change in the near future in accordance with the new U.S. policy. Moreover, some countries might have different policies for tangible and intangible products; intangible products are products that can be downloaded from the Internet. Please consult with export agencies or legal firms with multi-national experience in order to comply with all applicable regulations.

Australia The Australian government has been critized for its lack of coordination in establishing a policy concerning export, import, and domestic use of cryptographic products. Recent clarifications state that there are no restrictions on import and domestic use, but that export is controlled by the Department of Defense in accordance with the Wassenaar Arrangement.

Brazil While there are no restrictions of any kind today, there are proposals for a new law requiring users to register their products. Brazil is not part of the Wassenaar Arrangement.

Canada There are no restrictions on import and domestic use of encryption products in Canada today . The Canadian export policy is in accordance with the policies of countries such as United States, United Kingdom, and Australia in the sense that Canada's Communications Security Establishment (CSE) cooperates with the corresponding authorities in the mentioned countries.

China China is one of the countries with the strongest restrictions on cryptography; a license is required for export, import, or domestic use of any cryptography product. There are several restrictions on export regulations, and China is not participating in the Wassenaar Arrangement.

The European Union The European Union strongly supports the legal use of cryptography and is at the forefront of counteracting restrictions on cryptography as well as key escrow and recovery schemes. While this policy is heavily encouraged by Germany, there are a variety of more restrictive policies among the other member states.

- **France** France used to have strong restrictions on import and domestic use of encryption products, but the most substantial restrictions were abolished in early 1999. Export regulations are pursuant to the Wassenaar Arrangement and controlled by Service Central de la Securite des Systemes d'Information (SCSSI).
- **Germany** There are no restrictions on the import or use of any encryption software or hardware. Furthermore, the restrictions on export regulations were removed in June 1999.
- **Italy** While unhindered use of cryptography is supported by the Italian authorities, there have been proposals for cryptography controls. There are no import restrictions, but export is controlled in accordance with the Wassenaar Arrangement by the Ministry of Foreign Trade.
- **United Kingdom** The policy of United Kingdom is similar to that of Italy, but with even more outspoken proposals for new domestic cryptography controls. Export is controlled by the Department of Trade and Industry.

Israel Domestic use, export, and import of cryptographic products are tightly controlled in Israel. There have been proposals for slight relaxations of the regulations, but only for cryptographic products used for authentication purposes.

Japan There are no restrictions on the import or use of encryption products. Export is controlled in accordance with the Wassenaar Arrangement by the Security Export Control Division of the Ministry of International Trade and Industry.

Russia The Russian policy is similar to the policies of China and Israel with licenses required for import and domestic use of encryption products. Unlike those countries, however, Russia is a participant of the Wassenaar Arrangement. Export of cryptographic products from Russia generally requires a license.

South Africa There are no restrictions on the domestic use of cryptography, but import of cryptographic products requires a valid permit from the Armaments Control Division. Export is controlled by the Department of Defense Armaments Development and Protection. South Africa does not participate in the Wassenaar Arrangement.

In the table below, 75 countries have been divided into five categories according to their cryptographic policies as of 1999. Category 1 includes countries with a policy allowing for unrestricted use of cryptography, while category 5 consists of countries where cryptography is tightly controlled. The table and most other facts in this answer are collected from [EPIC99], which includes extensive lists of references. Countries with their names in *italics* are participants in the Wassenaar Arrangement (see Question 6.5.3).

1	*Canada*, Chile, Croatia, Cyprus, Dominica, Estonia, *Germany*, Iceland, Indonesia, *Ireland*, Kuwait, Krgystan, Latvia, Lebanon, Lithuania, Mexico, Morocco, Papua New Guinea, Philippines, Slovenia, Sri Lanka, *Switzerland*, Tanzania, Tonga, Uganda, United Arab Emirates.
2	*Argentina*, Armenia, *Australia*, *Austria*, *Belgium*, Brazil, *Bulgaria*, *Czech Republic*, *Denmark*, *Finland*, *France*, *Greece*, *Hungary*, *Italy*, *Japan*, Kenya, *South Korea*, *Luxembourg*, *Netherlands*, *New Zeeland*, *Norway*, *Poland*, *Portugal*, *Romania*, South Africa, *Sweden*, Taiwan, *Turkey*, *Ukraine*, Uruguay.
3	Hong Kong, Malaysia, *Slovakia*, *Spain*, *United Kingdom*, *United States*.
4	India, Israel, Saudi Arabia.
5	Belarus, China, Kazakhstan, Mongolia, Pakistan, *Russia*, Singapore, Tunisia, Venezuela, Vietnam.

6.5.2 Why do some countries have import restrictions on cryptography?

As indicated in the answer to Question 6.5.1, several countries including China, Israel, and Russia have import restrictions on cryptography. Some countries require vendors to obtain a license before importing cryptographic products. Many governments use such import licenses to pursue domestic policy goals. In some instances, governments require foreign vendors to provide technical information to obtain an import license. This information is then used to steer business toward local companies. Other governments have been accused of using this same information for outright industrial espionage.

6.5.3 What is the Wassenaar Arrangement?

The Wassenaar Arrangement (WA) was founded in 1996 by a group of 33 countries including United States, Russia, Japan, Australia, and the members of the European Union. Its purpose is to control exports of conventional weapons and sensitive dual-use technology, which includes cryptographic products; "dual-use" means that a product can be used for both commercial and military purposes. The Wassenaar Arrangement controls do not apply to so-called intangible products, which include downloads from the Internet.

WA is the successor of the former Coordinating Committee on Multilateral Export Controls (COCOM), which placed export restrictions to communist countries. It should be emphasized that WA is not a treaty or a law; the WA Control lists are merely guidelines and recommendations, and each participating state may adjust its export policy through new regulations. Indeed, there are substantial differences between the export regulation policies of the participating countries.

As of the latest revision in December 1999, WA controls encryption and key management products where the security is based on one or several of the following:

- A symmetric algorithm with a key size exceeding 56 bits.
- Factorization of an integer of size exceeding 512 bits.
- Computation of discrete logarithms in a multiplicative group of a field of size is excess of 512 bits.
- Computation of discrete logarithms in a group that is not part of a field, where the size of the group exceeds 112 bits.

Other products, including products based on single-DES, are decontrolled. For more information on the Wassenaar Arrangement, see `http://www.wassenaar.org/` .