CHAPTER 25

Politics

25.1 NATIONAL SECURITY AGENCY (NSA)

The NSA is the National Security Agency (once called "No Such Agency" or "Never Say Anything," but they've been more open recently), the official security body of the U.S. government. President Harry Truman created the agency in 1952 under the Department of Defense, and for many years its very existence was kept secret. The NSA is concerned with signals intelligence; its mandate is to listen in on and decode all foreign communications of interest to the security of the United States.

The following paragraphs are excerpted from NSA's original charter, signed by President Truman in 1952, and classified for many years thereafter [1535]:

> The COMINT mission of the National Security Agency (NSA) shall be to provide an effective, unified organization and control of the communications intelligence activities of the United States conducted against foreign governments, to provide for integrated operational policies and procedures pertaining thereto. As used in this directive, the terms "communications intelligence" or "COMINT" shall be construed to mean all procedures and methods used in the interception of communications other than foreign press and propaganda broadcasts and the obtaining of information from such communications by other than intended recipients, but shall exclude censorship and the production and dissemination of finished intelligence.
>
> The special nature of COMINT actives requires that they be treated in all respects as being outside the framework of other or general intelligence activities. Orders, directives, policies, or recommendations of any authority of the Executive Branch relating to the collection, production, security, handling, dissemination, or utilization of intelligence, and/or classified material, shall not be applicable to COMINT actives, unless specifically so stated and issued by competent department or agency authority represented on the Board. Other National Security

> Council Intelligence Directives to the Director of Central Intelligence and related implementing directives issued by the Director of Central Intelligence shall be construed as non-applicable to COMINT activities, unless the National Security Council has made its directive specifically applicable to COMINT.

NSA conducts research in cryptology, both in designing secure algorithms to protect U.S. communications and in designing cryptanalytic techniques to listen in on non-U.S. communications. The NSA is known to be the largest employer of mathematicians in the world; it is also the largest purchaser of computer hardware in the world. The NSA probably possesses cryptographic expertise many years ahead of the public state of the art (in algorithms, but probably not in protocols) and can undoubtedly break many of the systems used in practice. But, for reasons of national security, almost all information about the NSA—even its budget—is classified. (Its budget is rumored to be $13 billion per year—including military funding of NSA projects and personnel—and it is rumored to employ 16,000 people.)

The NSA uses its power to restrict the public availability of cryptography, so as to prevent national enemies from employing encryption methods too strong for the NSA to break. James Massey discusses this struggle between academic and military research in cryptography [1007]:

> If one regards cryptology as the prerogative of government, one accepts that most cryptologic research will be conducted behind closed doors. Without doubt, the number of workers engaged today in such secret research in cryptology far exceeds that of those engaged in open research in cryptology. For only about 10 years has there in fact been widespread open research in cryptology. There have been, and will continue to be, conflicts between these two research communities. Open research is a common quest for knowledge that depends for its vitality on the open exchange of ideas via conference presentations and publications in scholarly journals. But can a government agency, charged with responsibilities of breaking the ciphers of other nations, countenance the publication of a cipher that it cannot break? Can a researcher in good conscience publish such a cipher that might undermine the effectiveness of his own government's code-breakers? One might argue that publication of a provably secure cipher would force all governments to behave like Stimson's "gentlemen," but one must be aware that open research in cryptography is fraught with political and ethical considerations of a severity more than in most scientific fields. The wonder is not that some conflicts have occurred between government agencies and open researchers in cryptology, but rather that these conflicts (at least those of which we are aware) have been so few and so mild.

James Bamford wrote a fascinating book about the NSA: *The Puzzle Palace* [79], recently updated by Bamford and Wayne Madsen [80].

The Commercial COMSEC Endorsement Program (CCEP)

The Commercial COMSEC Endorsement Program (CCEP), codenamed Overtake, is a 1984 NSA initiative to facilitate the development of computer and communications products with embedded cryptography [85,1165]. The military had always paid

for this kind of thing for themselves, and it was very expensive. The NSA figured that if companies could sell equipment to both the military and to corporate users, even overseas, costs would go down and everyone would benefit. They would no longer endorse equipment as complying with Federal Standard 1027, and then CCEP would provide government-endorsed cryptographic equipment [419].

NSA developed a series of cryptographic modules for different purposes. Different algorithms would be used in the modules for different applications, and manufacturers would be able to pull one module out and plug in another depending on the customer. There were modules for military use (Type I), modules for "unclassified but sensitive" government use (Type II), modules for corporate use (Type III), and modules for export (Type IV). Table 25.1 summarizes the different modules, applications, and names.

This program is still around, but never became popular outside the government. All the modules were tamperproof, all the algorithms were classified, and you had to get your keys from NSA. Corporations never really bought into the idea of using classified algorithms dictated by the government. You'd think the NSA would have learned from this lesson and not even bothered with Clipper, Skipjack, and escrowed encryption chips.

25.2 National Computer Security Center (NCSC)

The National Computer Security Center, a branch of the NSA, is responsible for the government's trusted computer program. Currently, the center evaluates commercial security products (both hardware and software), sponsors and publishes research, develops technical guidelines, and generally provides advice, support, and training.

The NCSC publishes the infamous "Orange Book" [465]. Its actual title is the *Department of Defense Trusted Computer System Evaluation Criteria*, but that's a mouthful to say and the book has an orange cover. The Orange Book attempts to define security requirements, gives computer manufacturers an objective way to measure the security of their systems, and guides them as to what to build into their secure products. It focuses on computer security and doesn't really say a lot about cryptography.

The Orange Book defines four broad divisions of security protection. It also defines classes of protection within some of those divisions. They are summarized in Table 25.2.

Table 25.1
CCEP Modules

Application	Type I	Type II
Voice/low-speed data	Winster	Edgeshot
Computer	Tepache	Bulletproof
High-speed data	Foresee	Brushstroke
Next Generation	Countersign I	Countersign II

Sometimes manufacturers say things like "we have C2 security." This is what they're talking about. For more information on this, read [1365]. The computer security model used in these criteria is called the Bell-LaPadula model [100,101,102,103].

The NCSC has published a whole series of books on computer security, sometimes called the Rainbow Books (all the covers have different colors). For example, *Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria* [1146], sometimes called the "Red Book," interprets the Orange Book for networks and network equipment. The *Trusted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria* [1147]—I can't even begin to describe the color of that cover—does the same for databases. There are now over 30 of these books, some with hideously colored covers.

For a complete set of the Rainbow Books, write Director, National Security Agency, INFOSEC Awareness, Attention: C81, 9800 Savage Road, Fort George G. Meade, MD 20755-6000; (410) 766-8729. Don't tell them I sent you.

25.3 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

The NIST is the National Institute of Standards and Technology, a division of the U.S. Department of Commerce. Formerly the NBS (National Bureau of Standards), it changed its name in 1988. Through its Computer Systems Laboratory (CSL), NIST promotes open standards and interoperability that it hopes will spur the economic development of computer-based industries. To this end, NIST issues standards and guidelines that it hopes will be adopted by all computer systems in the United States. Official standards are published as FIPS (Federal Information Processing Standards) publications.

If you want copies of any FIPS (or any other NIST publication), contact National Technical Information Service (NTIS), U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22161; (703) 487-4650; or visit gopher://csrc.ncsl.nist.gov.

When Congress passed the Computer Security Act of 1987, NIST was mandated to define standards for ensuring the security of sensitive but unclassified informa-

Table 25.2
Orange Book Classifications

D: Minimal Security
C: Discretionary Protection
C1: Discretionary Security Protection
C2: Controlled Access Protection
B: Mandatory Protection
B1: Labeled Security Protection
B2: Structured Protection
B3: Security Domains
A: Verified Protection
A1: Verified Design

tion in government computer systems. (Classified information and Warner Amendment data are under the jurisdiction of the NSA.) The Act authorizes NIST to work with other government agencies and private industry in evaluating proposed technology standards.

NIST issues standards for cryptographic functions. U.S. government agencies are required to use them for sensitive but unclassified information. Often the private sector adopts these standards as well. NIST issued DES, DSS, SHS, and EES.

All these algorithms were developed with some help from the NSA, ranging from analyzing DES to designing DSS, SHS, and the Skipjack algorithm in EES. Some people have criticized NIST for allowing the NSA to have too much control over these standards, since the NSA's interests may not coincide with those of NIST. It is unclear how much actual influence NSA has on the design and development of the algorithms. Given NIST's limited staff, budget, and resources, NSA's involvement is probably considerable. NSA has significant resources to contribute, including a computer facility second-to-none.

The official "Memorandum of Understanding" (MOU) between the two agencies reads:

> MEMORANDUM OF UNDERSTANDING BETWEEN THE DIRECTOR OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY AND THE DIRECTOR OF THE NATIONAL SECURITY AGENCY CONCERNING THE IMPLEMENTATION OF PUBLIC LAW 100-235
>
> Recognizing that:
>
> A. Under Section 2 of the Computer Security Act of 1987 (Public Law 100-235), (the Act), the National Institute of Standards and Technology (NIST) has the responsibility within the Federal Government for:
>
> 1. Developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems as defined in the Act; and,
>
> 2. Drawing on the computer system technical security guidelines of the National Security Agency (NSA) in this regard where appropriate.
>
> B. Under Section 3 of the Act, the NIST is to coordinate closely with other agencies and offices, including the NSA, to assure:
>
> 1. Maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and,
>
> 2. To the maximum extent feasible, that standards developed by the NIST under the Act are consistent and compatible with standards and procedures developed for the protection of classified information in Federal computer systems.
>
> C. Under the Act, the Secretary of Commerce has the responsibility, which he has delegated to the Director of NIST, for appointing the members of the Computer System Security and Privacy Advisory Board, at least one of whom shall be from the NSA.
>
> Therefore, in furtherance of the purposes of this MOU, the Director of the NIST and the Director of the NSA hereby agree as follows:

I. The NIST will:

1. Appoint to the Computer Security and Privacy Advisory Board at least one representative nominated by the Director of the NSA.

2. Draw upon computer system technical security guidelines developed by the NSA to the extent that the NIST determines that such guidelines are consistent with the requirements for protecting sensitive information in Federal computer systems.

3. Recognize the NSA-certified rating of evaluated trusted systems under the Trusted Computer Security Evaluation Criteria Program without requiring additional evaluation.

4. Develop telecommunications security standards for protecting sensitive unclassified computer data, drawing upon the expertise and products of the National Security Agency, to the greatest extent possible, in meeting these responsibilities in a timely and cost-effective manner.

5. Avoid duplication where possible in entering into mutually agreeable arrangements with the NSA for the NSA support.

6. Request the NSA's assistance on all matters related to cryptographic algorithms and cryptographic techniques including but not limited to research, development evaluation, or endorsement.

II. The NSA will:

1. Provide the NIST with technical guidelines in trusted technology, telecommunications security, and personal identification that may be used in cost-effective systems for protecting sensitive computer data.

2. Conduct or initiate research and development programs in trusted technology, telecommunications security, cryptographic techniques and personal identification methods.

3. Be responsive to the NIST's requests for assistance in respect to all matters related to cryptographic algorithms and cryptographic techniques including but not limited to research, development, evaluation, or endorsement.

4. Establish the standards and endorse products for application to secure systems covered in 10 USC Section 2315 (the Warner Amendment).

5. Upon request by Federal agencies, their contractors and other government-sponsored entities, conduct assessments of the hostile intelligence threat to federal information systems, and provide technical assistance and recommend endorsed products for application to secure systems against that threat.

III. The NIST and the NSA shall:

1. Jointly review agency plans for the security and privacy of computer systems submitted to NIST and NSA pursuant to section 6(b) of the Act.

2. Exchange technical standards and guidelines as necessary to achieve the purposes of the Act.

3. Work together to achieve the purposes of this memorandum with the greatest efficiency possible, avoiding unnecessary duplication of effort.

4. Maintain an on-going open dialogue to ensure that each organization remains abreast of emerging technologies and issues affecting automated information system security in computer-based systems.

5. Establish a Technical Working Group to review and analyze issues of mutual interest pertinent to protection of systems that process sensitive or other unclassified information. The Group shall be composed of six federal employees, three each selected by NIST and NSA and to be augmented as necessary by representatives of other agencies. Issues may be referred to the group by either the NSA Deputy Director for Information Security or the NIST Deputy Director or may be generated and addressed by the group upon approval by the NSA DDI or NIST Deputy Director. Within days of the referral of an issue to the Group by either the NSA Deputy Director for Information Security or the NIST Deputy Director, the Group will respond with a progress report and plan for further analysis, if any.

6. Exchange work plans on an annual basis on all research and development projects pertinent to protection of systems that process sensitive or other unclassified information, including trusted technology, for protecting the integrity and availability of data, telecommunications security and personal identification methods. Project updates will be exchanged quarterly, and project reviews will be provided by either party upon request of the other party.

7. Ensure the Technical Working Group reviews prior to public disclosure all matters regarding technical systems security techniques to be developed for use in protecting sensitive information in federal computer systems to ensure they are consistent with the national security of the United States. If NIST and NSA are unable to resolve such an issue within 60 days, either agency may elect to raise the issue to the Secretary of Defense and the Secretary of Commerce. It is recognized that such an issue may be referred to the President through the NSC for resolution. No action shall be taken on such an issue until it is resolved.

8. Specify additional operational agreements in annexes to this MOU as they are agreed to by NSA and NIST.

IV. Either party may elect to terminate this MOU upon six months' written notice. This MOU is effective upon approval of both signatories.

/signed/

RAYMOND G. KAMMER

Acting Director, National Institute of Standards and Technology, 24 March 1989

W. O. STUDEMAN

Vice Admiral, U.S. Navy; Director, National Security Agency, 23 March 1989

25.4 RSA Data Security, Inc.

RSA Data Security, Inc. (RSADSI) was founded in 1982 to develop, license, and market the RSA patent. It has some commercial products, including a standalone e-mail security package, and various cryptographic libraries (available in either source or object form). RSADSI also markets the RC2 and RC4 symmetric algorithms (see Section 11.8). RSA Laboratories, a research lab associated with RSADSI, performs basic cryptographic research and provides consulting services.

Anyone interested in either their patents or products should contact Director of Sales, RSA Data Security, Inc., 100 Marine Parkway, Redwood City, CA 94065; (415) 595-8782; fax: (415) 595-1873.

25.5 PUBLIC KEY PARTNERS

The five patents in Table 25.3 are held by Public Key Partners (PKP) of Sunnyvale, California, a partnership between RSADSI and Caro-Kahn, Inc.—the parent company of Cylink. (RSADSI gets 65 percent of the profits and Caro-Kahn gets 35 percent.) PKP claims that these patents, and 4,218,582 in particular, apply to *all uses* of public-key cryptography.

In [574], PKP wrote:

> These patents [4,200,770, 4,218,582, 4,405,829, and 4,424,414] cover all known methods of practicing the art of Public Key, including the variations collectively known as ElGamal.
>
> Due to the broad acceptance of RSA digital signatures throughout the international community, Public Key Partners strongly endorses its incorporation in a digital signature standard. We assure all interested parties that Public Key Partners will comply with all of the policies of ANSI and the IEEE concerning the availability of licenses to practice this art. Specifically, in support of any RSA signature standard which may be adopted, Public Key Partners hereby gives its assurance that licenses to practice RSA signatures will be available under reasonable terms and conditions on a nondiscriminatory basis.

Whether this is true depends on who you talk to. PKP's licenses have mostly been secret, so there is no way to check if the licenses are standard. Although they claim to have never denied a license to anyone, at least two companies claim to have been denied a license. PKP guards its patents closely, threatening anyone who tries to use public-key cryptography without a license. In part, this is a reaction to U.S. patent law. If you hold a patent and fail to prosecute an infringement, you can lose your patent. There has been much talk about whether the patents are legal, but so far it has all been talk. All legal challenges to PKP's patents have been settled before judgment.

Table 25.3
Public Key Partners' Patents

Patent #	Date	Inventors	Patent Covers
4,200,770	4/29/80	Hellman, Diffie, Merkle	Diffie-Hellman Key Exchange
4,218,582	8/19/80	Hellman, Merkle	Merkle-Hellman Knapsacks
4,405,829	9/20/83	Rivest, Shamir, Adleman	RSA
4,424,414	3/3/84	Hellman, Pohlig	Pohlig-Hellman
4,995,082	2/19/91	Schnorr	Schnorr Signatures

I am not going to dispense legal advice in this book. Maybe the RSA patent will not hold up in court. Maybe the patents do not apply to the entirety of public-key cryptography. (Honestly, I can't see how they cover ElGamal or elliptic curve cryptosystems.) Perhaps someone will eventually win a suit against PKP or RSADSI. But keep in mind that corporations with large legal departments like IBM, Microsoft, Lotus, Apple, Novell, Digital, National Semiconductor, AT&T, and Sun have all licensed RSA for use in their products rather than fight them in court. And Boeing, Shell Oil, DuPont, Raytheon, and Citicorp have all licensed RSA for their own internal use.

In one case, PKP brought suit against TRW Corporation for using the ElGamal algorithm without a license. TRW claimed they did not need a license. PKP and TRW reached a settlement in June 1992. The details of the settlement are unknown, but they included an agreement by TRW to license the patents. This does not bode well. TRW can afford good lawyers; I can only assume that if they thought they could win the suit without spending an unreasonable amount of money, they would have fought.

Meanwhile, PKP is having its own internal problems. In June 1994 Caro-Kahn sued RSADSI alleging, among other things, that the RSA patent is invalid and unenforceable [401]. Both partners are trying to have the partnership dissolved. Are the patents valid or not? Will users have to get a license from Caro-Kahn to use the RSA algorithm? Who will own the Schnorr patent? The matter will probably be sorted out by the time this book sees publication.

Patents are good for only 17 years, and cannot be renewed. On April 29, 1997, Diffie-Hellman key exchange (and the ElGamal algorithm) will enter the public domain. On September 20, 2000, RSA will enter the public domain. Mark your calendars.

25.6 International Association for Cryptologic Research (IACR)

The International Association for Cryptologic Research is the worldwide cryptographic research organization. Its stated purpose is to advance the theory and practice of cryptology and related fields. Membership is open to any person. The association sponsors two annual conferences, Crypto (held in Santa Barbara in August) and Eurocrypt (held in Europe in May), and publishes quarterly *The Journal of Cryptology* and the *IACR Newsletter*.

The address of the IACR Business Office changes whenever the president does. The current address is: IACR Business Office, Aarhus Science Park, Gustav Wieds Vej 10, DK-8000 Aarhus C, Denmark.

25.7 RACE Integrity Primitives Evaluation (RIPE)

The Research and Development in Advanced Communication Technologies in Europe (RACE) program was launched by the European Community to support pre-

competitive and pre-normative work in communications standards and technologies to support Integrated Broadband Communication (IBC). As part of that effort, RACE established the RACE Integrity Primitives Evaluation (RIPE) to put together a portfolio of techniques to meet the anticipated security requirements of IBC.

Six leading European cryptography research groups made up the RIPE consortium: Center for Mathematics and Computer Science, Amsterdam; Siemens AG; Philips Crypto BV; Royal PTT Nederland NV, PTT Research; Katholieke Universiteit Leuven; and Aarhus Universitet. After calls for algorithms in 1989 and 1991 [1564], 32 submissions from around the world, and a 350 man-month evaluation project, the consortium published *RIPE Integrity Primitives* [1305,1332]. The report included an introduction and some basic integrity concepts, and these primitives: MDC-4 (see Section 18.11), RIPE-MD (see Section 18.8), RIPE-MAC (see Section 18.14), IBC-HASH, SKID (see Section 3.2), RSA, COMSET (see Section 16.1), and RSA key generation.

25.8 CONDITIONAL ACCESS FOR EUROPE (CAFE)

Conditional Access for Europe (CAFE) is a project in the European Community's ESPRIT program [204,205]. Work began in December 1992 and is scheduled to be finished by the end of 1995. The consortium involved consists of groups for social and market studies (Cardware, Institut für Sozialforschung), software and hardware manufacturers (DigiCash, Gemplus, Ingenico, Siemens), and cryptographers (CWI Amsterdam, PTT Research Netherlands, SPET, Sintef Delab Trondheim, Universities of Århus, Hildesheim and Leuven).

The goal is to develop systems for conditional access, particularly digital payment systems. Payment systems must give legal certainty to everybody at all times and require as little trust as possible—this certainty should not depend on the tamper-resistance of any devices.

The basic device for CAFE is an electronic wallet: a small computer that looks something like a pocket calculator. It has a battery, keyboard, screen, and an infrared channel for communicating with other wallets. Every user owns and uses his own wallet, which administers his rights and guarantees his security.

A device with a keyboard and screen has an advantage over a smart card; it can operate independent of a terminal. A user can directly enter his password and the amount of the payment. The user does not have to give his wallet up to complete a transaction, unlike the current situation with credit cards.

Additional features are:

- Offline transactions. The purpose of the system is to replace small cash transactions; an online system would be too cumbersome.
- Loss tolerance. If a user loses his wallet, or if it breaks or is stolen, he can recover his money.
- Support for different currencies.

— An open architecture and open system. A user should be able to pay for arbitrary services, such as shopping, telephone, and public transport, by a range of service providers. The system should be interoperable between any number of electronic money issuers, and between different wallet types and manufacturers.
— Low cost.

At this writing there is a software version of the system, and the consortium is hard at work on a hardware prototype.

25.9 ISO/IEC 9979

In the mid-80s, the ISO tried to standardize DES, which by then was already a FIPS and an ANSI standard. After some political wrangling, the ISO decided not to standardize cryptographic algorithms, but instead to register algorithms. Only encryption algorithms can be registered; hash functions and signature schemes cannot. Any national body can submit an algorithm for registration.

Currently only three algorithms have been submitted (see Table 25.4). A submission includes information about applications, parameters, implementations, modes, and test vectors. A detailed description is optional; it is possible to submit secret algorithms for registration.

The fact that an algorithm is registered does not imply anything about its quality, nor is registration an approval of the algorithm by the ISO/IEC. Registration merely indicates that a single national body wants to register the algorithm, based on whatever criteria that body uses.

I am not impressed with this idea. Registration obstructs the standardization process. Rather than agreeing on a few algorithms, the ISO is allowing any algorithm to be registered. With so little control over what is registered, stating that an algorithm is "ISO/IEC 9979 Registered" sounds a whole lot better than it is. In any case, the registry is maintained by the National Computer Centre Ltd., Oxford Road, Manchester, M1 7ED, United Kingdom.

Table 25.4
ISO/IEC 9979
Registered Algorithms

Name	Registration Number
B-CRYPT	0001
IDEA	0002
LUC	0003

25.10 PROFESSIONAL, CIVIL LIBERTIES, AND INDUSTRY GROUPS

Electronic Privacy Information Center (EPIC)

EPIC was established in 1994 to focus public attention on emerging privacy issues relating to the National Information Infrastructure, such as the Clipper chip, the Digital Telephony proposal, national identity numbers and systems, medical records privacy, and the sale of consumer data. EPIC conducts litigation, sponsors conferences, produces reports, publishes the *EPIC Alert*, and leads campaigns on privacy issues. Anyone interested in joining should contact Electronic Privacy Information Center, 666 Pennsylvania Avenue SE, Suite 301, Washington, D.C. 20003; (202) 544-9240; fax: (202) 547-5482; Internet: info@epic.org.

Electronic Frontier Foundation (EFF)

The EFF is dedicated to protecting civil rights in cyberspace. With respect to cryptographic policy in the United States, they believe that information and access to cryptography are fundamental rights, and therefore should be free of government restriction. They organized the Digital Privacy and Security Working Group, a coalition of 50 organizations. The group opposed the Digital Telephony bill and the Clipper initiative. The EFF is also helping in a lawsuit against cryptography export controls [143]. Anyone interested in joining the EFF should contact Electronic Frontier Foundation, 1001 G Street NW, Suite 950E, Washington, D.C. 20001; (202) 347-5400; fax: (202) 393-5509; Internet: eff@eff.org.

Association for Computing Machinery (ACM)

The ACM is an international computer industry organization. In 1994 the U.S. ACM Public Policy Committee produced an excellent report on U.S. cryptography policy [935]. This should be required reading for anyone interested in the politics of cryptography. It is available via anonymous ftp from info.acm.org in /reports/acm_crypto/acm_crypto_study.ps.

Institute of Electrical and Electronics Engineers (IEEE)

The IEEE is another professional organization. The U.S. office investigates and makes recommendations on privacy-related issues including encryption policy, identity numbers, and privacy protections on the Internet.

Software Publishers Association (SPA)

The SPA is a trade association of over 1000 personal computer software companies. They have lobbied for relaxation of export controls on cryptography, and maintain a list of commercially available foreign cryptography products.

25.11 SCI.CRYPT

Sci.crypt is the Usenet newsgroup for cryptology. It is read by an estimated 100,000 people worldwide. Most of the posts are nonsense, bickering, or both; some are

political, and most of the rest are requests for information or basic questions. Occasionally nuggets of new and useful information are posted to this newsgroup. If you follow sci.crypt regularly, you will learn how to use something called a kill file.

Another Usenet newsgroup is sci.crypt.research, a moderated newsgroup devoted to discussions about cryptology research. There are fewer posts and they are more interesting.

25.12 CYPHERPUNKS

The Cypherpunks are an informal group of people interested in teaching and learning about cryptography. They also experiment with cryptography and try to put it into use. In their opinion, all the cryptographic research in the world doesn't do society any good unless it gets used.

In "A Cypherpunk's Manifesto," Eric Hughes writes [744]:

> We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.
>
> Cypherpunks write code. We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it. We publish our code so that our fellow Cypherpunks may practice and play with it. Our code is free for all to use, worldwide. We don't care much if you don't approve of the software we write. We know that software can't be destroyed and that widely dispersed systems can't be shut down.

People interested in joining the cypherpunks mailing list on the Internet should send mail to majordomo@toad.com. The mailing list is archived at ftp.csua.berkeley.edu in /pub/cypherpunks.

25.13 PATENTS

Software patents are an issue much larger than the scope of this book. Whether they're good or bad, they exist. Algorithms, cryptographic algorithms included, can be patented in the United States. IBM owned the DES patents [514]. IDEA is patented. Almost every public-key algorithm is patented. NIST even has a patent for the DSA. Some cryptography patents have been blocked by intervention from the NSA, under the authority of the Invention Secrecy Act of 1940 and the National Security Act of 1947. This means that instead of a patent, the inventor gets a secrecy order and is prohibited from discussing his invention with anybody.

The NSA has special dispensation when it comes to patents. They can apply for a patent and then block its issuance. It's a secrecy order again, but here the NSA is both the inventor and the issuer of the order. When, at some later date, the secrecy order is removed, the Patent Office issues the patent good for the standard 17 years. This rather clearly protects the invention while keeping it secret. If someone else

invents the same thing, the NSA has already filed for the patent. If no one else invents it, then it remains secret.

Not only does this fly directly in the face of the patent process, which is supposed to disclose as well as protect inventions, it allows the NSA to keep a patent for more than 17 years. The 17-year clock starts ticking after the patent is issued, not when it is filed. How this will change, now that the United States has ratified the GATT treaty, is unclear.

25.14 U.S. EXPORT RULES

According to the U.S. government, cryptography can be a munition. This means it is covered under the same rules as a TOW missile or an M1 Abrams tank. If you sell cryptography overseas without the proper export license, then you are an international arms smuggler. Unless you think time in a federal penitentiary would look good on your résumé, pay attention to the rules.

With the advent of the Cold War in 1949, all of the NATO countries (except Iceland), and later Australia, Japan, and Spain, formed CoCom, the Coordinating Committee for Multilateral Export Controls. This is an unofficial nontreaty organization, chartered to coordinate national restrictions on the export of sensitive military technologies to the Soviet Union, other Warsaw Pact countries, and the People's Republic of China. Examples of controlled technologies are computers, milling machinery, and cryptography. The goal here was to slow technology transfer into those countries, and thereby keep their militaries inferior.

Since the end of the Cold War, the CoCom countries realized that many of their controls were obsolete. They are supposedly in the process of defining something called the "New Forum," another multinational organization designed to stop the flow of military technologies to countries the members don't particularly like.

In any case, U.S. export policy on strategic goods is defined by the Export Administration Act, the Arms Export Control Act, the Atomic Energy Act, and the Nuclear Non-Proliferation Act. The controls established by all this legislation are implemented through a number of statutes, none of them coordinated with each other. Over a dozen agencies including the military services administer controls; often their regulatory programs overlap and contradict.

Controlled technologies appear on several lists. Cryptography has traditionally been classified as a munition and appears on the U.S. Munitions List (USML), the International Munitions List (IML), the Commerce Control List (CCL), and the International Industrial List (IIL). The Department of State is responsible for the USML; it is published as part of the International Traffic in Arms Regulations (ITAR) [466,467].

Two U.S. government agencies control export of cryptography. One is the Bureau of Export Administration (BXA) in the Department of Commerce, authorized by the Export Administration Regulations (EAR). The other is the Office of Defense Trade Controls (DTC) in the State Department, authorized by the ITAR. As a rule of thumb, the Commerce Department's BXA has far less stringent requirements, but

State Department's DTC (which takes technical and national security advice from the NSA, and always seems to follow that advice) sees all cryptography exports first and can refuse to transfer jurisdiction to BXA.

The ITAR regulates this stuff. (Before 1990 the Office of Defense Trade Controls was called the Office of Munitions Controls; presumably this public relations effort is designed to help us forget that we're dealing with guns and bombs.) Historically, the DTC has been reluctant to grant export licenses for encryption products stronger than a certain level—not that they have ever been public about exactly what that level is.

The following sections are excerpted from the ITAR [466,467]:

§ 120.10 Technical data.

Technical data means, for purposes of this subchapter:

(1) Information, other than software as defined in 120.10(d), which is required for the design, development, production, processing, manufacture, assembly, operation, repair, maintenance or modification of defense articles. This includes, for example, information in the form of blueprints, drawings, photographs, plans, instructions and documentation;

(2) Classified information relating to defense articles and defense services;

(3) Information covered by an invention secrecy order;

(4) Software as defined in Sec. 121.8(f) directly related to defense articles;

(5) This definition does not include information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges and universities in the public domain as defined in § 120.11. It also does not include basic marketing information on function or purpose or general system descriptions of defense articles.

§ 120.11 Public domain.

Public domain means information which is published and which is generally accessible or available to the public:

(1) Through sales at newsstands and bookstores;

(2) Through subscriptions which are available without restriction to any individual who desires to obtain or purchase the published information;

(3) Through second class mailing privileges granted by the U.S. Government;

(4) At libraries open to the public or from which the public can obtain documents;

(5) Through patents available at any patent office;

(6) Through unlimited distribution at a conference, meeting, seminar, trade show or exhibition, generally accessible to the public, in the United States;

(7) Through public release (i.e., unlimited distribution) in any form (e.g., not necessarily in published form) after approval by the cognizant U.S. government department or agency (see also § 125.4(b)(13)).

(8) Through fundamental research in science and engineering at accredited institutions of higher learning in the U.S., where the resulting information is ordinarily published and shared broadly in the scientific community. Fundamental research is defined to mean basic and applied research in science and engineering where the

resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research the results of which are restricted for proprietary reasons or specific U.S. Government access and dissemination controls. University research will not be considered fundamental research if:

(i) The University or its researchers accept other restrictions on publication of scientific and technical information resulting from the project or activity, or

(ii) The research is funded by the U.S. Government and specific access and dissemination controls protecting information resulting from the research are applicable.

§ 120.17 Export.

Export means:

(1) Sending or taking defense articles out of the United States in any manner, except by mere travel outside of the United States by a person whose personal knowledge includes technical data; or

(2) Transferring registration, control or ownership to a foreign person of any aircraft, vessel, or satellite covered by the U.S. Munitions List, whether in the United States or abroad; or

(3) Disclosing (including oral or visual disclosure) or transferring in the United States any defense articles to an embassy, any agency or subdivision of a foreign government (e.g., diplomatic missions); or

(4) Disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad; or

(5) Performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the United States or abroad.

(6) A launch vehicle or payload shall not, by the launching of such vehicle, be considered export for the purposes of this subchapter. However, for certain limited purposes (see § 126.1 of this subchapter), the controls of this subchapter apply to sales and other transfers of defense articles or defense services.

Part 121—The United States Munitions List

§ 121.1 General. The United States Munitions List

Category XIII—Auxiliary Military Equipment

(1) Cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems, except cryptographic equipment and software as follows:

(i) Restricted to decryption functions specifically designed to allow the execution of copy protected software, provided the decryption functions are not user-accessible.

(ii) Specifically designed, developed or modified for use in machines for banking or money transactions, and restricted to use only in such transactions. Machines for banking or money transactions include automatic teller machines, self-service statement printers, point of sale terminals or equipment for the encryption of interbanking transactions.

(iii) Employing only analog techniques to provide the cryptographic processing that ensures information security in the following applications. . . .

(iv) Personalized smart cards using cryptography restricted for use only in equipment or systems exempted from the controls of the USML.

(v) Limited to access control, such as automatic teller machines, self-service statement printers or point of sale terminals, which protects passwords or personal identification numbers (PIN) or similar data to prevent unauthorized access to facilities but does not allow for encryption or files or text, except as directly related to the password of PIN protection.

(vi) Limited to data authentication which calculates a Message Authentication Code (MAC) or similar result to ensure no alteration of text has taken place, or authenticate users, but does not allow for encryption of data, text or other media other than that needed for the authentication.

(vii) Restricted for fixed data compression or coding techniques.

(viii) Limited to receiving for radio broadcast, pay television or similar restricted audience television of the consumer type, without digital encryption and where digital decryption is limited to video, audio or management functions.

(ix) Software designed or modified to protect against malicious computer damage, (e.g., viruses).

(2) Cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software which have the capability of generating spreading or hopping codes for spread spectrum systems or equipment.

(3) Cryptographic systems, equipment, assemblies, modules, integrated circuits, components or software.

§ 125.2 Exports of unclassified technical data.

(a) General. A license (DSP-5) is required for the export of unclassified technical data unless the export is exempt from the licensing requirements of this subchapter. In the case of a plant visit, details of the proposed discussions must be transmitted to the Office of Defense Trade Controls for an appraisal of the technical data. Seven copies of the technical data or the details of the discussions must be provided.

(b) Patents. A license issued by the Office of Defense Trade Controls is required for the export of technical data whenever the data exceeds that which is used to support a domestic filing of a patent application or to support a foreign filing of a patent application whenever no domestic application has been filed. Requests for the filing of patent applications in a foreign country, and requests for the filing of amendments, modifications or supplements to such patents, should follow the regulations of the U.S. Patent and Trademark Office in accordance with 37 CFR part 5. The export of technical data to support the filing and processing of patent applications in foreign countries is subject to regulations issued by the U.S. Patent and Trademark Office pursuant to 35 U.S.C. 184.

(c) Disclosures. Unless otherwise expressly exempted in this subchapter, a license is required for the oral, visual or documentary disclosure of technical data

> by U.S. persons to foreign persons. A license is required regardless of the manner in which the technical data is transmitted (e.g., in person, by telephone, correspondence, electronic means, etc.). A license is required for such disclosures by U.S. persons in connection with visits to foreign diplomatic missions and consular offices.

And so on. There's a lot more information in this document. If you're going to try to export cryptography, I suggest you get a copy of the entire thing and a lawyer who speaks the language.

In reality, the NSA has control over the export of cryptographic products. If you want a Commodity Jurisdiction (CJ), you must submit your product to the NSA for approval and submit the CJ application to the State Department. After State Department approval, the matter moves under the jurisdiction of the Commerce Department, which has never cared much about the export of cryptography. However, the State Department will never grant a CJ without NSA approval.

In 1977 an NSA employee named Joseph A. Meyer wrote a letter—unauthorized, according to the official story of the incident—to the IEEE, warning them that the scheduled presentation of the original RSA paper would violate the ITAR. From *The Puzzle Palace:*

> He had a point. The ITAR did cover any "unclassified information that can be used, or adapted for use, in the design, production, manufacture, repair, overhaul, processing, engineering, development, operation, maintenance, or reconstruction" of the listed materials, as well as "any technology which advances the state-of-the-art or establishes a new art in an area of significant military applicability in the United States." And export did include transferring the information both by writing and by either oral or visual means, including briefings and symposia in which foreign nationals are present.
>
> But followed literally, the vague, overly broad regulations would seem to require that anyone planning to write or speak out publicly on a topic touching the Munitions List must first get approval from the State Department—a chilling prospect clearly at odds with the First Amendment and one as yet untested by the Supreme Court.

In the end NSA disavowed Meyer's actions and the RSA paper was presented as planned. No actions were taken against any of the inventors, although their work arguably enhanced foreign cryptography capabilities more than anything released since.

The following statement by NSA discusses the export of cryptography [363]:

> Cryptographic technology is deemed vital to national security interests. This includes economic, military, and foreign policy interests.
>
> We do not agree with the implications from the House Judiciary Committee hearing of 7 May 1992 and recent news articles that allege that U.S. export laws prevent U.S. firms' manufacture and use of top encryption equipment. We are unaware of any case where a U.S. firm has been prevented from manufacturing and using encryption equipment within this country or for use by the U.S. firm or

its subsidiaries in locations outside the U.S. because of U.S. export restrictions. In fact, NSA has always supported the use of encryption by U.S. businesses operating domestically and overseas to protect sensitive information.

For export to foreign countries, NSA as a component of the Department of Defense (along with the Department of State and the Department of Commerce) reviews export licenses for information security technologies controlled by the Export Administration Regulations or the International Traffic in Arms Regulations. Similar export control systems are in effect in all the Coordinating Committee for Multilateral Export Controls (CoCom) countries as well as many non-CoCom countries as these technologies are universally considered as sensitive. Such technologies are not banned from export and are reviewed on a case-by-case basis. As part of the export review process, licenses may be required for these systems and are reviewed to determine the effect such export could have on national security interests-including economic, military, and political security interests. Export licenses are approved or denied based upon the type of equipment involved, the proposed end use and the end user.

Our analysis indicates that the U.S. leads the world in the manufacture and export of information security technologies. Of those cryptologic products referred to NSA by the Department of State for export licenses, we consistently approve over 90%. Export licenses for information security products under the jurisdiction of the Department of Commerce are processed and approved without referral to NSA or DoD. This includes products using such techniques as the DSS and RSA which provide authentication and access control to computers or networks. In fact, in the past NSA has played a major role in successfully advocating the relaxation of export controls on RSA and related technologies for authentication purposes. Such techniques are extremely valuable against the hacker problem and unauthorized use of resources.

It is the stated policy of the NSA not to restrict the export of authentication products, only encryption products. If you want to export an authentication-only product, approval may merely be a matter of showing that your product cannot easily be used for encryption. Furthermore, the bureaucratic procedures are much simpler for authentication products than for encryption products. An authentication product needs State Department approval only once for a CJ; an encryption product may require approval for every product revision or even every sale.

Without a CJ, you must request export approval every time you wish to export the product. The State Department does not approve the export of products with strong encryption, even those using DES. Isolated exceptions include export to U.S. subsidiaries for the purposes of communicating to the U.S., exports for some banking applications, and export to appropriate U.S. military users. The Software Publishers Association (SPA) has been negotiating with the government to ease export license restrictions. A 1992 agreement between them and the State Department eased the export license rules for two algorithms, RC2 and RC4, as long as the key size is 40 bits or less. Refer to Section 7.1 for more information.

In 1993, Rep. Maria Cantwell (D-WA) introduced a bill at the behest of the software industry to relax export controls on encryption software. Sen. Patty Murray

(D-WA) introduced a companion bill in the Senate. The Cantwell Bill was appended to the general export control legislation going through Congress, but was deleted by the House Intelligence Committee after a massive lobbying effort by the NSA. Whatever the NSA did, it was impressive; the committee voted unanimously to delete the wording. I can't remember the last time a bunch of legislators voted unanimously to do anything.

In 1995 Dan Bernstein, with the help of the EFF, sued the U.S. government, seeking to bar the government from restricting publication of cryptographic documents and software [143]. The suit claimed that the export control laws are unconstitutional, an "impermissible prior restraint on speech, in violation of the First Amendment." Specifically, the lawsuit charges that the current export control process:

- Allows bureaucrats to restrict publication without ever going to court.
- Provides too few procedural safeguards for First Amendment rights.
- Requires publishers to register with the government, creating in effect a "licensed press."
- Disallows general publication by requiring recipients to be individually identified.
- Is sufficiently vague that ordinary people cannot know what conduct is allowed and what conduct is prohibited.
- Is overbroad because it prohibits conduct that is clearly protected (such as speaking to foreigners within the United States).
- Is applied too broadly, by prohibiting export of software that contains no cryptography, on the theory that cryptography could be added to it later.
- Egregiously violates the First Amendment by prohibiting private speech on cryptography because the government wishes its own opinions on cryptography to guide the public instead.
- Exceeds the authority granted by Congress in the export control laws in many ways, as well as exceeding the authority granted by the Constitution.

Everyone anticipates that the case will take several years to settle, and no one has any idea how it will come out.

Meanwhile, the Computer Security and Privacy Advisory Board, an official advisory board to NIST, voted in March 1992 to recommend a national policy review of cryptographic issues, including export policy. They said that export policy is decided solely by agencies concerned with national security, without input from agencies concerned with encouraging commerce. Those agencies concerned with national security are doing everything possible to make sure this doesn't change, but eventually it has to.

25.15 FOREIGN IMPORT AND EXPORT OF CRYPTOGRAPHY

Other countries have their own import and export rules [311]. This summary is incomplete and probably out of date. Countries could have rules and ignore them, or could have no rules but restrict import, export, and use anyway.

- Australia requires an import certificate for cryptography only upon request from the exporting country.
- Canada has no import controls, and export controls are similar to those of the United States. The exportation of items from Canada may be subject to restriction if they are included on the Export Control List pursuant to the Export and Import Permits Act. Canada follows the CoCom regulations in the regulation of cryptographic technology. Encryption devices are outlined in category five, part two of Canada's export regulations. These provisions are similar to U.S. category five in the Export Administration Regulations.
- China has a licensing scheme for importing commodities; exporters must file an application with the Ministry of Foreign Trade. Based on China's List of Prohibited and Restricted Imports and Exports enacted in 1987, China restricts the import and export of voice-encoding devices.
- France has no special rules for the import of cryptography, but they have rules regarding the sale and use of cryptography in their country. All products must be certified: Either they must meet a published specification, or the company proprietary specification must be provided to the government. The government may also ask for two units for their own use. Companies must have a license to sell cryptography within France; the license specifies the target market. Users must have a license to buy and use cryptography; the license includes a statement to the effect that users must be prepared to give up their keys to the government up to four months after use. This restriction may be waived in some cases: for banks, large companies, and so on. And there is no use license requirement for cryptography exportable from the U.S.
- Germany follows the CoCom guidelines, requiring a license to export cryptography. They specifically maintain control of public-domain and mass-market cryptography software.
- Israel has import restrictions, but no one seems to know what they are.
- Belgium, Italy, Japan, Netherlands, and the United Kingdom follow the CoCom guidelines on cryptography, requiring a license for export.
- Brazil, India, Mexico, Russia, Saudi Arabia, Spain, South Africa, Sweden, and Switzerland have no import or export controls on cryptography.

25.16 LEGAL ISSUES

Are digital signatures real signatures? Will they stand up in court? Some preliminary legal research has resulted in the opinion that digital signatures would meet the requirements of legally binding signatures for most purposes, including commercial use as defined in the Uniform Commercial Code (UCC). A GAO (General Accounting Office) decision, made at the request of NIST, opines that digital signatures will meet the legal standards of handwritten signatures [362].

The Utah Digital Signature Act went into effect on May 1, 1995, providing a legal framework for the use of digital signatures in the judicial system. California has a bill pending, while Oregon and Washington are still writing theirs. Texas and Florida are right behind. By this book's publication, more states will have followed suit.

The American Bar Association (ED1 and Information Technology Division of the Science and Technology Section) produced a model act for states to use for their own legislation. The act attempts to incorporate digital signatures into the existing legal infrastructure for signatures: the Uniform Commercial Code, the United States Federal Reserve regulations, common law of contracts and signatures, the United Nations Convention on Contracts for the International Sale of Goods, and the United Nations Convention on International Bills of Exchange and International Promissory Committees. Included in the act are responsibilities and obligations of certification authorities, issues of liability, and limits and policies.

In the United States, laws about signatures, contracts, and commercial transactions are state laws, so this model act is designed for states. The eventual goal is a federal act, but if this all begins at the state level there is less chance of the NSA mucking up the works.

Even so, the validity of digital signatures has not been challenged in court; their legal status is still undefined. In order for digital signatures to carry the same authority as handwritten signatures, they must first be used to sign a legally binding document, and then be challenged in court by one party. The court would then consider the security of the signature scheme and issue a ruling. Over time, as this happened repeatedly, a body of precedent rulings would emerge regarding which digital signature methods and what key sizes are required for a digital signature to be legally binding. This is likely to take years.

Until then, if two people wish to use digital signatures for contracts (or purchase requests, or work orders, or whatever), it is recommended that they sign a paper contract in which they agree in the future to be bound by any documents digitally signed by them [1099]. This document would specify algorithm, key size, and any other parameters; it should also delineate how disputes would be resolved.