3

Cryptography and Public Policy

The Legacy of World War I

Histories of cryptography usually begin by observing that cryptography is of ancient lineage, having been used by Caesar and recommended as one of the feminine arts in the Kama Sutra. As we saw in the last chapter, there is a remarkable degree of continuity in the basics of cryptographic technology over the past several centuries, and new ideas often turn out to have old roots.[1] Be this as it may, the field we know today is a creature of the twentieth century.

World War I was the first war to be fought in the era of radio. In the early years of the century, the military (particularly navies) saw the potential of the new medium of communication and adopted it wholesale. Before the advent of radio, Britain's First Sea Lord sent an admiral off with a fleet and expected to hear news in weeks or months. With radio, ships at sea were brought under much closer control by shore-based headquarters. Radio also had the advantage of being able to carry human voice, which undersea cable systems of the time could not do. Radio, however, had a serious disadvantage: anyone could listen in. Sometimes an unintended listener even got better reception than the intended recipient.

The Mechanization of Cryptography

The solution to the ubiquity of radio reception was, of course, to use cryptography. Messages were enciphered before being transmitted, and were deciphered upon reception. Radio was much more vulnerable to interception than any communication channel that had been in use before, with the result that a much larger fraction of the messages required encryption. The methods in use, codes and some hand cipher systems,

had grown up over centuries of written communication in which they were usually reserved for the most sensitive traffic. In consequence, there was a crushing burden on the cipher clerks, and often a glut of traffic waiting to be deciphered.

In the years immediately after the war, inventors turned their attention to the problem of mechanizing encryption and embarked on the path that has led us to the automatic cryptography of today. As described in the previous chapter, the technique was a form of multiple-Vigenère cipher in which letters were looked up in tables by electric currents passing through wires rather than by cipher clerks.

Rotor machines arose simultaneously on both sides of the Atlantic. The inventions of Edward Hebern of Oakland, California emerged as the backbone of US cryptography in World War II. Those of Arthur Scherbius and Arvid Gerhard Damm played a similar role in Europe and gave rise to the most widely used of all rotor principles: that of the German Enigma machine (Kahn 1967, pp. 420–422).

At the time of World War I, cryptography was more an esoteric than a secret field. It was not widely understood, and codebreakers kept their intrusions into opponents' codes secret. Yet the whole culture of military secrecy, rampant today, was in its infancy, and military secrets did not belong to governments in the way they do now. Works on cryptography reasonably representative of the state of the art were published and enjoyed a status similar to that of other technical treatises. Indeed, during the war, William Frederick Friedman, the intellectual founder of the organization that eventually grew to become the National Security Agency, published groundbreaking new cryptographic discoveries as technical reports of the private Riverbank Laboratories.

The inventors of the rotor machine all took out patents, intending to sell their machines commercially. In the United States and in Europe the granting of a patent is a very public process and the publication of patents is regulated by treaty. Both earlier and later laws made it possible for the US government to declare a patent application secret and delay the granting indefinitely, but in 1919 this was not the case.

The issuing of the patents turned out to be one of the last public things about rotor machines. The commercial market for cryptographic equipment proved not to be as good as the inventors expected, and Hebern

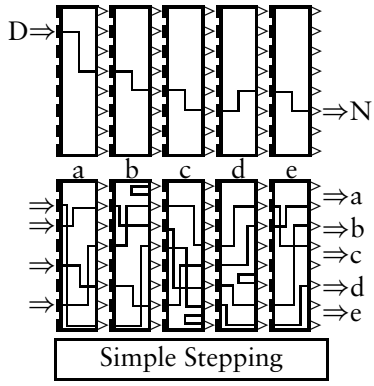

Figure 3.1
Simplified Sigaba.

tried to sell his invention to the government. As designed, Hebern's machine was not secure, and it was broken by Friedman in 1921 (Deavours and Kruh 1985, pp. 46–47). Although attacks on the machine Friedman broke can be found in the contemporary public literature, Friedman's 1925 paper on the subject is still secret.

The government bought only sample quantities of Hebern's device. The weaknesses Friedman discovered were correctable, but the Army did not share its design changes with Hebern. It developed and employed his invention without compensating him, under cover of cryptography's growing secrecy. Only in the 1950s did Hebern's heirs succeed, through a lawsuit, in recovering some of what Hebern was owed (Kahn 1967, p. 420). In the United States, development of cryptographic systems became a secret enterprise of small groups in the Army and the Navy.

Hebern's simple three-wheel machine and regular pattern of wheel movement led to Sigaba, the most secure rotor machine of World War II. In the mid 1930s Friedman designed a rotor machine, designated M-134a, whose five wheels moved under the control of a paper tape. In retrospect this can be seen to be merely an overly complicated way of achieving a one-time cryptosystem, but at the time the additional complexity must have seemed an advantage. Unfortunately, the M-134a had the same problem that goes with any one-time system: it needed lots of keying material. A young cryptanalyst named Frank Rowlett was given the task of producing matching pairs of key tapes—a task made tedious

by the fact that any error in the tapes would produce not only an error in the plain text but also a disastrous loss of synchronization between the sending and receiving machines. Rowlett conceived of using one rotor machine to manufacture the pattern of rotor motions for the other, an idea that was to remain officially secret for 60 years.

The Growth of US Signals Intelligence

After World War I, the United States maintained and developed its capacity for signals intelligence (SIGINT), something unprecedented in peacetime. Equally important, the responsibility for signals intelligence was merged with the responsibility for developing codes to protect US military communications.[2] Both intelligence and security prospered under this arrangement. By making good use of signals intelligence during arms negotiations with Japan in 1921, the US pushed the Japanese all the way to their planned best offer (Kahn 1967, pp. 357–359; Yardley 1931).

The role secrecy plays in intelligence is quite different from the role it plays in security. Cryptography relies on the secrecy of cryptographic keys, just as safes rely on the secrecy of their combinations. It may also profit from the secrecy of cryptographic systems. It could hardly be easier to break a cryptosystem whose workings are not known than to break one whose workings are known. On the other hand, such secrecy has costs that usually outweigh its benefits. The workings of ordinary pin-tumbler door locks and those of the combination locks that guard bank vaults are familiar to locksmiths and burglars alike, yet both are widespread and successful security devices. It is essentially impossible, on the other hand, to practice intelligence without secrecy. If you reveal the fact that you are spying on people or, worse yet, precisely how you are doing it, it is almost certain that, if those people care at all about security, they will change their communication practices in order to make your task more difficult.

A celebrated example of this occurred in Britain in 1927. The Security Service (MI5) raided the London office of the All-Russian Cooperative Society, whose trade activities were a key element of Soviet spying on British industry. Parliament imprudently demanded to know what had led MI5 to such an action and publicly extracted the fact that Britain had been reading Soviet messages for years. In the words of R. V. Jones,

Britain's head of scientific intelligence during World War II, that incident showed the Soviets the weakness of "their diplomatic codes, which were changed a fortnight later and were not since readable, at least up to the time that I left MI6 in 1946" (Corson et al. 1985, pp. 286 and 440).

The integration of communications intelligence (a field in which it is advantageous to keep even the basic techniques secret) and communication security (a field whose need for secrecy is far narrower) is the apparent cause of the general increase in the secrecy of cryptography that occurred from the 1920s through the 1960s.

World War II

World War II was a triumph for America's codemakers and codebreakers. On the defensive side, American high-grade cryptosystems, Sigaba in particular, survived the war, apparently unread by our opponents. On the offensive side, communications intelligence contributed decisively to victory in both the Atlantic and the Pacific. The United States routinely read high-level Japanese traffic in both military and diplomatic systems, and collaborated extensively with Great Britain in reading German communications.

Cryptography and signals intelligence during World War II have been written about extensively, but a little-known project undertaken during the same period presaged much of what has happened since: the development of the first secure telephone.

Voice scramblers of various sorts had been in existence since the early years of the twentieth century, but none of these systems was in any real sense secure. Scrambling systems were adequate to thwart casual listeners; however, most of them were vulnerable to being unraveled by talented ears—particularly after the development of recording, which permitted the signal to be listened to more than once. The existing scramblers were inadequate to protect high-level traffic, and the US military started development on Sigsaly, the first digital secure telephone.

Sigsaly was in some ways like and in some ways preposterously unlike a contemporary secure phone. Sigsaly was a digital telephone. It used a vocoder developed at Bell Laboratories to convert the speaker's voice into a 2400-bit-per-second stream.[3] The digitized voice was then encrypted

with one-time keys stored on phonograph records. The records were shattered after each use to ensure that they could not be reused. Although modern secure phones do not normally use one-time keys, there is nothing bizarre about the practice. Especially remarkable were Sigsaly's size (30 equipment racks, each 7 feet tall) and cost (so high that only two people in the world could afford such installations: Franklin Roosevelt and Winston Churchill—later a few more were installed in high-level military headquarters).

The successes of the American signals intelligence establishment during the war set the stage for further expansion and consolidation.

The Cold War

The late 1940s brought the explosion in technology that has dominated the lives of the Baby Boom generation. Some technologies, most conspicuously atomic energy and radar, were developed as consequences of World War II. Others, including television, had been put on hold by the war and now profited from the overall growth of the electronics industry that the war had produced. In the world of cryptography, it was a great period of conversion from mechanical and electro-mechanical cryptosystems to purely electronic cryptosystems.

Inappropriate as Sigsaly was for any normal military or civilian communication requirement, it showed the possibility of genuinely secure voice communication. However, there were many hurdles to jump. The highest of these was the problem of digitizing the voice. Decades would pass before secure voice equipment at the low data rates of Sigsaly would be widely available. In the meantime, it was necessary to simplify the problem by sending voice at between 6000 and 50,000 bits per second. This created a new cryptographic problem.

Sigsaly had achieved 2400-bit-per-second encryption by using a one-time system to protect its signal. Like all one-time systems, it suffered from inflexibility of key management. This was of little concern when the supply of instruments numbered two, but it would be a limiting factor in wider deployment. What was required was a cryptographic machine capable of operating at voice speeds. Unfortunately, rotor machines, which

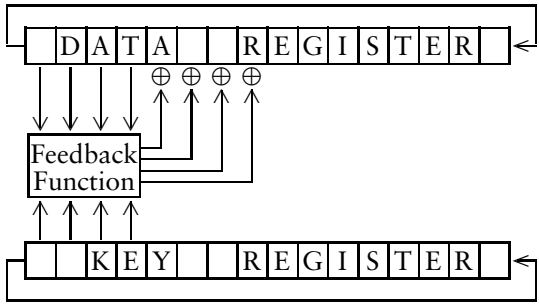

Figure 3.2
Nonlinear shift register.

operated at 10 characters per second, could not come close to keeping up with Sigsaly's 2400 bits (240 characters) per second.[4] The result was the development of shift-register cryptography, which accounts for most of the encrypted bits transmitted today.

During and before World War II, intelligence in general and communications intelligence in particular was attached to military commands. After the war, there was a move to improve the quality of US intelligence by centralizing authority and coordinating the activities of various groups. The year 1947 saw passage of the Central Intelligence Act, which created the Central Intelligence Agency and the position of Director of Central Intelligence (who, at least in principle, coordinated the efforts of the whole US intelligence community). The centralization of signals intelligence took longer and was far less public, but in 1952, after some 5 years of study and reorganization, President Harry Truman signed a secret presidential order creating the National Security Agency. From its creation the new organization sought to capture control of all cryptographic and cryptanalytic work within the United States. Overall, this effort was remarkably successful.

In 1949, Claude Shannon, a professor of electrical engineering at MIT, published a paper entitled "The Communication Theory of Secrecy Systems" in the *Bell System Technical Journal*. In 1967, David Kahn, a journalist who had been interested in cryptography since childhood, published a massive history of cryptography called *The Codebreakers*. In

between, no overtly cryptographic work of any significance saw public print in the United States,[5] though various papers whose cryptographic significance is not immediately apparent did.[6]

NSA successfully suppressed cryptographic work in other parts of the US government. Probably as a result of this, application of cryptography to the nuclear command and control system did not get underway until directly ordered by President John Kennedy in the early 1960s.[7]

Horst Feistel's Group at the AFCRC

There was, however, one very significant failure of NSA's territorial ambitions.

Cryptography can play a number of roles that are not explicitly parts of communication. One of these is distinguishing between friends and enemies. During World War II, US warplanes began to carry *Identification Friend or Foe* (IFF) devices to reduce the chance that they would be shot down by "friendly fire." Early IFF devices were analog and were not very secure against replication by opponents seeking to impersonate US forces. IFF without cryptography eventually evolved into a system called the Mark X, which is now an essential component of air traffic control and is used by civilian aircraft, and many military ones, all over the world.

In the early 1950s, the US Air Force recognized the need to improve its IFF equipment and turned to the established cryptographic authorities for help. The Armed Forces Security Agency, NSA's immediate predecessor, had little interest in the problem, and so the Air Force set out on its own. A prototype cryptographic IFF device was built at the Air Force Cambridge Research Center (AFCRC) using the recently developed transistor. Central among this project's objectives was to show that the equipment could be made small enough to fit in a fighter's nose. At this point, the project crossed the path of a man whose role in modern cryptography has been widely underappreciated, despite the fact that he is recognized as the "father of the Data Encryption Standard."

In 1934, the 20-year-old Horst Feistel moved to the United States from Germany. Seven years later, the Japanese attacked Pearl Harbor, the US declared war on Japan, and Germany, in an act of bravado, declared war on the US. Feistel, on the verge of becoming a US citizen, was put

under "house arrest"—he could move freely around Boston, where he lived, but was required to report his movements if he went to visit his mother in New York. On January 31, 1944, the restraints were suddenly lifted and Feistel became a US citizen. The following day he was given a security clearance and began a job at the AFCRC.[8]

Feistel, who says that cryptography had interested him since he was in his teens, recalls that when he mentioned his interests shortly after arriving at his new job, he was told that it was not the time for a German to be talking about cryptography. His career in cryptography had to wait until after the hot war against Germany was over and the Cold War against the Soviet Union was underway.

Several years later, Feistel, who had by now built a research group in cryptography at the AFCRC, discovered that the Air Force's cryptographic IFF system was on its way to being put into service without what he considered adequate evaluation. He put his team of young mathematicians, supported by a number of academic consultants, to work analyzing the new system. The group alternately found weaknesses in the original design and discovered how to fix them. Over a period of several years it made a major contribution to modern cryptography, developing the first practical block ciphers.[9]

Although Feistel's group at the AFCRC was in steady communication with NSA and seems thereby to have exerted a profound influence on cryptographic design in that organization, NSA appears eventually to have succeeded in shutting down the Air Force work. In the late 1950s, the group dissolved. Horst Feistel moved, first to MIT's Lincoln Laboratory and then to its spinoff, the Mitre Corporation. In the mid 1960s, Feistel, who devoted himself to one problem throughout his career, attempted to set up a new cryptographic development group at Mitre. He was forced to abandon the project as a result of what was perceived at Mitre as NSA pressure.[10] At this point, Feistel found a new champion, IBM, and moved to the Watson Laboratory in Yorktown Heights, New York.

The 1960s

In 1965, Representative Jack Brooks of Texas authored a thoroughly non-controversial law providing for the purchase and leasing of computer equipment (Brooks Act 1965, 89-306(f)). The law decreed that the Secretary of Commerce was authorized to "make appropriate recommendations to the President relating to the establishment of uniform Federal automatic data processing standards" (ibid., 89-306(f)). Thus the responsibility for setting civilian computer standards fell to the National Bureau of Standards (NBS), which already determined everything from standard US time (based on an atomic clock in Boulder, Colorado) to methods for testing the flammability of fabrics. The new series were called Federal Information Processing Standards; their purpose is to provide incentives for industry to manufacture what the US government needs. Although FIPS are only binding on government organizations, the enormous purchasing power the government brings to bear causes most FIPS to become de facto commercial standards.[11] This assignment of responsibility to NBS was later to prove difficult for the Department of Defense, but there were no objections when the Brooks Act was passed.

In 1967, a non-technical phenomenon had a profound effect on the course of cryptographic technology. Despite NSA's efforts, David Kahn's book *The Codebreakers* was published. Kahn was neither a mathematician nor an engineer, but a historian, and his book focuses far more on the military and diplomatic impact of codebreaking than on its technique. Nonetheless, Kahn explained everything he knew about cryptography and cryptanalysis. All of a sudden, there was a book in print that explained rotor machines and at least mentioned that they had been succeeded by purely electronic devices. Furthermore, what explanation of the technology the book did contain was wrapped in an extensive explanation of why the subject was important. The result was a wave of interest in cryptography that rippled through the engineering world.

IBM was also interested in cryptography in the late 1960s. The company had undertaken to provide automatic teller machines for Lloyds Bank in London. Lloyds, which planned to have several hundred of the machines scattered around London, had a scenario for disaster. It imagined a gang with a confederate inside the post office, which, in Britain,

ran the telephone system. The members of the gang would drive around London visiting the teller machines at the start of a bank holiday weekend, when the machines had just been stocked with thousands of pounds of cash apiece. The post office confederate would call each machine in turn and tell it to hand out all its money. At the end of the evening the gang would be several million pounds richer. Nobody else would be likely to notice anything but the fact that some of the machines had run out of money till Tuesday morning, when the bank holiday weekend ended. By then the money would no doubt be sitting comfortably in a bank in Zurich, a city whose bankers had not taken the previous day off.

IBM hired Horst Feistel, who continued with his life's work. Colleagues recall that Feistel had been talking back in the 1950s about much larger systems than could be built at the time. Now, a quarter century later, electronics had caught up with Feistel's imagination. The work resulted in a number of cryptographic systems. One was used in the IBM2984 banking system and was commonly called Lucifer.[12]

The 1970s

The US Data Encryption Standard

In the early 1970s, some people at the National Security Agency and some at the National Bureau of Standards[13] recognized that the Privacy Act of 1974 and other federal laws, together with the increasing use of computers and digital communications by the federal government, would require that approved cryptography be available to government users other than NSA's traditional national-security clients.

NSA was reluctant to provide equipment of its own design to a wider range of users. Its reasoning is easy to imagine. Cryptographic secrecy was part of NSA's security philosophy. The designs of NSA cryptographic systems were uniformly classified SECRET NOFORN,[14] and the equipment in which they were implemented was classified CONFIDENTIAL. The tamper-resistance technology being used today to put SECRET algorithms in UNCLASSIFIED chips did not yet exist. Any equipment that was to be put in the hands of uncleared users would have to embody an unclassified cryptographic algorithm. NSA was afraid, however, that, by making public an algorithm it had designed itself, it would reveal in-

formation about its design philosophy and potentially compromise other equipment. A system that was made public would be widely available to attack. If it was broken, and if it resembled other NSA cryptosystems, the attack might work against those as well.

Following the FIPS process, NBS published a solicitation for a standard cryptographic system in the *Federal Register* (USDoC 1973). The process by which the Data Encryption Standard was selected has never been adequately explained, and the identity of the other contestants, if there were any, has not become public. On the face of it, IBM submitted the winning algorithm and NSA, acting as a consultant to the NBS, approved it. In fact it is generally agreed that NSA had a substantial hand in determining the algorithm's final form (Bayh 1978).

Public-Key Cryptography

During the academic year 1974–1975, Whitfield Diffie and Martin Hellman, working at Stanford University, and Ralph Merkle, at the University of California at Berkeley, discovered a new concept in cryptography that was to have profound implications for policy as well as for technology.[15]

The idea was that the capacity to encrypt messages and the capacity to decrypt messages were not, as had always been taken for granted, inseparable. It was possible for one person to have a key that would encrypt messages in such a way that decrypting them required a different key, held by a different person. Diffie, Hellman, and Merkle called the new concept *public-key cryptography*.

Instead of having one key that could both encrypt and decrypt messages, like a conventional cryptosystem, a public-key system had two keys. What was essential was that with one key, called reasonably enough the *public key*, it was very hard to figure out the corresponding *private key* that could be used to decrypt a message encrypted with the public key. Exactly how hard? Just as hard as breaking a cryptogram produced by encrypting something with the public key.

Public-key cryptography has two implications: if I know your public key and want to send you a secret message, I can encrypt it with your public key, and, since only you know your private key, only you will be able to read the message. I don't need to share a secret with you in order to send you a secret message.

Not only did public-key cryptography make a major contribution to key management, it provided a *digital signature* that could be used on electronic documents. Suppose I receive a message from you encrypted with your private key. If I decrypt the message and find that it makes sense, I have evidence that, unless someone else knows your private key, the message must have come from you.

Although the research that led to this new field was carried on in academia, it grew out of two very practical considerations. Diffie had been trying for years to figure out how to build a system that would secure every telephone in the country. Getting away from the traditional need to distribute secret keys from a central facility brought this vision a step closer to reality. By what seems to be coincidence, Diffie had also been thinking about signatures for years. Around the time of Diffie's arrival at Stanford in late 1969, his new boss, John McCarthy, had given a paper on what we would now call Internet commerce, and Diffie had begun wondering what would play the role of the signed contract in the new environment.

In 1976, Diffie and Hellman published a paper entitled "New Directions in Cryptography," which contained a partial solution to the problem of creating a public-key cryptosystem. This system, commonly known as *Diffie-Hellman key exchange*,[16] provides an additional feature with policy implications that took years to be recognized: the creation of truly ephemeral keys.

In early 1977, Diffie and Hellman's paper was read by a team of three young faculty members at MIT, Ron Rivest, Adi Shamir, and Len Adleman. With a far better grasp of number theory than the three West Coast researchers, Rivest, Shamir, and Adleman quickly found a solution to the problem Diffie and Hellman had posed. They named the resulting system after their initials: RSA (Rivest et al. 1978).

The Meyer Affair

Public-key cryptography created quite a splash. In August of 1977 it was described in Martin Gardner's column in *Scientific American*, and requests for the MIT technical report came from around the world. Rivest was scheduled to present the work at an Institute of Electrical and Electronics Engineers (IEEE) meeting in Ithaca, New York, in October. The

IEEE received a letter from one "J. A. Meyer" warning that, because foreign nationals would be present, publication of the result was a potential violation of the International Traffic in Arms Regulations.

This was the first that Rivest and his colleagues had heard of ITAR. Aside from an address in Bethesda, Maryland, J. A. Meyer was unidentified. Nonetheless, the MIT scientists took the warning seriously and halted distribution of their paper. Then an enterprising *Science* journalist, Deborah Shapley, discovered that Meyer worked at the National Security Agency. NSA denied any connection with Meyer's letter, and the MIT scientists decided to resume distribution of the paper (Shapley and Kolata 1977). Rivest spoke on the results at the Ithaca conference, and for the moment the furor subsided.

But 1978 brought new problems. Two inventors filed for patents and found themselves subjected to secrecy orders under a little-known provision of US patent law that permits the federal government to order an inventor to keep secret not only the substance of the invention but the fact that the order has been issued. The first of these inventors was Carl Nicolai, a garage-shop entrepreneur in Seattle who had developed a telephone scrambler based on spread-spectrum technology. The second was George Davida, a professor of computer science at the University of Wisconsin. Davida's invention, more technical than Nicolai's, was a way of combining linear and nonlinear finite automata in a cryptosystem. Most patent secrecy orders are placed on inventions growing out of government-sponsored secret work. Almost all of the remainder are directed at patents filed by large corporations,[17] which have little motivation to argue with the government's decision.[18]

Fights about secrecy orders are rare. But, despite the aspect of the law that makes the order itself secret, both Nicolai and Davida chose to fight. Ultimately, both orders were overturned—Nicolai's ostensibly on the grounds that a mistake had been made and the invention should not have been declared secret in the first place; Davida's on the pretext that, since it had earlier appeared as a Computer Science Department technical report, it could not effectively be kept secret.

Research Funding and Publication Rights

In the late 1970s action developed on another front: funding. Frederick Weingarten was a program officer at the National Science Foundation (NSF). One day in 1977 "two very grim men" walked into his office and informed him that he was "probably" breaking the law by funding cryptography research through the NSF (Weingarten 1997; Burnham 1980, pp. 139–140). He was not, but a new battle ensued.

Len Adleman submitted a research proposal to the NSF, whereupon the MIT scientist found himself in the midst of an inter-agency conflict regarding funding. Because Adleman had proposed research in cryptography, the NSF had sent the application to NSA for review. Now NSA wanted to support Adleman's work. Unwilling to accept funding from NSA for fear that the agency's requirement of prior review could lead to classification of his work, Adleman was caught in a bind: since he had an alternative source of support, the NSF—whose purpose is to support "non-mission-oriented" research—now refused to support him.

Adleman's concerns tied in with another issue that had disquieted the research community: in 1979, the director of NSA, Admiral Bobby Inman, warned that open publication of cryptography research was harmful to national security. Inman threatened that, unless academia and industry could come to a satisfactory compromise with his agency, NSA would seek laws limiting publication of cryptographic research.

Adleman's problem was resolved when it was decided that both NSF and NSA would fund cryptography research. While NSF would make applicants aware of the alternate source of grants, it would not require them to accept NSA support.

Inman's concerns led to the creation of an American Council on Education study panel consisting of mathematicians and computer scientists from industry and academia and two lawyers, including the representative from NSA. The panel recommended a two-year experiment in which NSA would conduct pre-publication reviews of all research in cryptography (ACE 1981). Submissions would be voluntary, reviews prompt. The academic community feared that this process would have a chilling effect on the emerging field, but the experiment proved successful. Concerns eased when relatively few authors were asked to modify their publications. There have been NSA requests that an author not

publish, and the agency has made suggestions for "minor" changes in some papers (Landau 1988, p. 11), but the research community reports that such requests have been modest in number. In an ironic twist, there was even an incident in which NSA apparently aided in the publication of cryptography research that the Army had tried to silence.[19]

The 1980s

The conflicts of the 1970s appeared to have abated. Behind the scenes, however, NSA's efforts to limit civilian research in cryptography continued. The result was a protracted delay in any widespread application of cryptography to civilian communications.

For example, in 1982 the NBS issued a *Federal Register* solicitation for algorithms for a public-key cryptography standard (USDoC 1982). RSA Data Security (the corporation formed by Rivest, Shamir, and Adleman) was interested in having the RSA algorithm become a federal standard, but the NSA was not. At the intelligence agency's request, NBS's plan to develop a federal standard for public-key cryptography was shelved (USGAO 1993b, p. 20).

Commercial Comsec Endorsement Program

In the mid 1980s, NSA changed its approach to broadening cryptographic coverage of American communications. Even though the initial promises that DES would be exportable had been broken, NSA was distressed by the algorithm's widespread availability[20] and was looking for a way to put the lid back on the box. Aided by the development of tamper-resistant coatings for chips (Raber and Riley 1989), NSA embarked on a program to supply equipment whose functioning was secret to a much wider user base.

Not only did NSA intend its new Commercial Comsec Endorsement Program (CCEP) to secure a much wider range of American communications, including industrial communications, NSA intended the program to do it with industry money.[21] As announced, the program was open to companies that had SECRET facility clearances and were willing to contribute expertise and funding to the development of secure versions of their products.[22]

Type I (High Grade)	Type II (Medium Grade)	
Winster	Edgeshot	Voice ($\leq$ 100 KB)
Tepache	Bulletproof	Data ($\leq$ 10 MB)
Forsee	Brushstroke	High speed ($\approx$ 100 MB)

Table 3.1
CCEP cryptomodules.

The most significant feature of the new program, however, was that it would provide a new category of equipment certified only for the protection of "unclassified sensitive information" but available without the tedious administrative controls that applied to equipment for protection of classified information. The traditional equipment was termed Type I, the new equipment Type II. Thus NSA was sponsoring the production of equipment directly competitive with DES.

The new undertaking was essentially a marketing effort, and in this situation NSA acted the same way commercial organizations often do: it began to undercut its previous "product line." The agency announced that it would not support the recertification of DES at its next five-year review, due to take place in 1988, and told the banking community so in a letter to the chairman of X9E9, the security standards committee.

It didn't wash. The bankers and their DES suppliers, few of whom were members of CCEP, were furious at the attempt to scuttle efforts on which they had been pressed to spend money only a few years earlier. Banking, furthermore, was international and had successfully negotiated special export arrangements in acknowledgement of this fact; secret American technology would not satisfy its worldwide need for security. In the end, NBS showed some backbone; in 1988 it recertified DES over NSA's objections. NSA had second thoughts about the wide availability of Type II equipment and, citing the Computer Security Act of 1987, imposed restrictions on its availability arguably as onerous as those for Type I equipment.[23] As a result, Type II products never approached market success, and few were ever manufactured.

The STU-III

Although technically not a part of CCEP,[24] the third-generation secure telephone unit, STU-III, shared a lot of its technical and administrative approach. The project began in 1983 and, like CCEP, incorporated Type I and Type II devices. The first instruments were delivered in late 1987.[25] Unlike CCEP, they have been a dramatic success, with over 300,000 installed by the mid 1990s.[26]

With CCEP and STU-III, NSA began using public-key cryptography. The exact method, called Firefly, was kept secret[27] but appears to employ the same exponentiation operations used by commercial gear (AWST 1986).

NSDD-145

In September 1984, President Ronald Reagan issued a National Security Decision Directive (NSDD-145) establishing a federal policy of safeguarding "sensitive, but unclassified" information in communications and computer systems—a directive with NSA's fingerprints all over it (Brooks 1992). In 1985 the president's Assistant for National Security Affairs, John Poindexter, sent out a directive implementing NSDD-145 by putting a Defense Department team in charge of safeguarding all federal executive-branch departments and agencies *and their contractors*.[28]

The Poindexter directive, as it came to be known, attracted a lot of attention. Federal executive-branch contractors included a fair number of civilian companies, many of which had little or nothing to do with secret work. Mead Data Central (a supplier of databases, including the Lexis and Nexis systems, which provide law cases and news and magazine stories respectively) was one of the companies affected. Jack Simpson, the president of Mead, told Congress: "We have had a number of visits to inquire about our system, how it works, who uses it, whether we would be amenable to controls or monitors, and whether the Soviets used it. On April 23, 1986, AFMAG [Air Force Management Advisory Group], five people came; September 29, US Government Intelligence Committee, CIA, NSA represented; October 7, FBI; October 21, FBI. Cordial visits, but asking the same questions." (Simpson 1987, p. 328) Cordial though these visits may have been, their effect was chilling. The National

Technical Information Service (NTIS), a database of unclassified federal scientific and technical material, had been part of Mead's information systems. After the visits from representatives of federal agencies, Mead got rid of NTIS. "This may have removed Mead Data Central from concern under NSDD-145," Simpson told Congress. "I guess I wonder about other information providers of NTIS." (ibid.) He got it right.

In 1986, Assistant Secretary of Defense Donald Latham said: "I am very concerned about what people are doing, and not just the Soviets. If that means putting a monitor on NEXIS-type systems, then I am for it." (Schrage 1986) The FBI visited various university libraries, attempting to discover what scientific information foreign students were accessing. Here the government agents ran into an unexpected obstruction: the librarians insisted on subpoenas before they would release information.

A committee of the House of Representatives examined NSDD-145. Legislators saw an inappropriate incursion of presidential authority into national policy, and a turf battle developed. "[T]he basement of the White House and the backrooms of the Pentagon are not places in which national policy should be developed," Representative Jack Brooks declaimed (Brooks 1987, p. 2).

NSA backpedaled. "NSDD-145 in no way sets NSA as a computer czar," Lieutenant General William Odom, NSA's director, told the representatives. "[O]ur role with the private sector is one of *encouraging, advising and assisting* them with regard to their security needs. We view our role, then, as one that is clearly *advisory* in nature. . . ." (Odom 1987, p. 281)

Many in industry and academia beheld NSDD-145 in a different light. "[Latham] is talking about monitoring private computer systems, private information sources, and unclassified data, and we find that incredible," Jack Simpson said before the House Committee (Simpson 1987, p. 328). Cheryl Helsing, chair of the Data Security Committee of the American Bankers Association and a vice president of BankAmerica, told the committee: "NSA's new . . . algorithms . . . absolutely cannot be used by the banking industry. Those conditions might well be appropriate for national defense related security, but are clearly inappropriate for use in our industry." (Helsing 1987, p. 113) Indeed, NSA's encryption algo-

rithms threatened years of development work by the banking industry. Eventually NSA decided to accept the use of old DES-based technology[29] in the financial industry, but in the interim "sixteen months ... elapsed while we worked to educate the NSA about our business," Helsing told Congress (ibid., p. 114).

Shortly after the congressional hearings on NSDD-145 began, the Poindexter directive was withdrawn.[30] "The policy was a good idea, in response to a real security threat," explained a senior Defense Department official. "The problem was that no one thought through all the implications." (Sanger 1987)

The Computer Security Act

The experience with NSDD-145 and NSA's behind-the-scenes actions convinced some US representatives that legislation was needed to reestablish which agency was in charge of assessing the security of civilian computer systems. NSA tried hard to convince the representatives that it was the right agency for the job. "[W]e are beginning to see civil agencies study and understand the usefulness of mechanisms resulting from [NSA's] earlier work," NSA Director Odom testified.

NSA could lead the way; it had "talent": "The [NSA] National Computer Security Center has a staff of more than 300 people," Odom told Congress (Odom 1987, pp. 294–295). He reminded the legislators that NSA already had responsibility for providing security for defense computer systems: "My concern with [the Computer Security Act] in its current form, then, it would create a wasteful, redundant bureaucracy that would busy itself with finding solutions to problems in computer security for the civil and private sector, while another government entity would be busy seeking the same solutions for the defense sector" (ibid., p. 296).

Congress did not buy the NSA director's arguments. The National Bureau of Standards (soon to be renamed the National Institute of Standards and Technology—we will refer to the agency as NIST from here on) was put in charge of developing computer security standards for the civilian sector. The representatives observed that developing civilian standards was a very different game from developing military ones, and that NIST had 22 years' experience with it whereas NSA had none.[31]

The report by the House Government Operations Committee described the concerns about giving such a charge to the intelligence agency: "NSA has made numerous efforts to either stop [work in cryptography] or to make sure it has control over the work by funding it, pre-publication reviews or other methods." (USHR 100-153 *Computer Security Act*, p. 21)[32]

The House committee was explicit that NIST was to be in charge, although NIST was to consult with NSA in the development of computer security standards, including those for cryptography: "By putting NSA in charge of developing technical security guidelines (software, hardware, communications) . . . [NIST], in effect, would on the surface be given the responsibility for the computer standards program with little to say about most of the program—the technical guidelines developed by NSA. This would jeopardize the entire Federal standards program." (USHR 100-153 *Computer Security Act*, p. 26)

The Computer Security Act (Public Law 100-235) was written to ensure that NIST would have responsibility for developing standards for the protection of "sensitive, but unclassified, information." All that remained was to fund the NIST program.

The NSA's Response

The NSA felt it had been had. A TOP SECRET NSA memo described what had occurred as follows:

- In 1982 NSA engineered a National Security Decision Directive, NSDD-145, through the Reagan Administration that gave responsibility for the security of all US information systems to the Director of NSA, eliminating NBS from this.
- This also stated that we would assist the private sector. This was viewed as Big Brother stepping in and generated an adverse reaction.
- Representative Jack Brooks, chairman of the House Government Operations Committee, personally set out to pass a law to reassert NBS's responsibility for Federal unclassified systems and to assist the private sector.

- By the time we fully recognized the implications of Brooks' bill, he had it orchestrated for a unanimous consent voice vote passage.

Clinton Brooks
Special Assistant to the
Director of the NSA
April 28, 1992

Congress legislates, but agencies implement; the ball game wasn't over. Under the Computer Security Act, NIST had been given additional responsibilities, but now it needed funds to go with the new responsibilities. NSA, the largest employer of mathematicians in the United States, had a vast operation working on issues of computer security and cryptography that dwarfed NIST's efforts. In 1987 NSA's *unclassified* computer security program had 300 employees and a budget of $40 million (USHH 102 *Threat of Economic Espionage*, p. 176); NIST's 1987 computer security operation had 16 employees and a budget of $1.1 million (USC-OTA 1994, p. 164). The Congressional Budget Office estimated that implementation of the Computer Security Act would cost NIST $4 million to $5 million dollars annually (USHR 100-153 *Computer Security Act*, p. 43).[33] It was time for Congress to appropriate the funds, but circumstances conspired to make that difficult.

During the Reagan-Bush years, the White House favored funding the Defense Department over funding civilian agencies, and NIST, part of the federal regulatory apparatus, was very much out of favor with a number of Republicans, some of whom were even in favor of eliminating the Department of Commerce. The Gramm-Rudman-Hollings Act[34] severely constrained discretionary funding. Yet by 1990 NIST's operation had a staff of 33 and a budget of $1.9 million.[35]

After the passage of the Computer Security Act, NSA began negotiating with NIST over their respective responsibilities in the development of cryptography. NSA went directly to Raymond Kammer, the acting director of NIST, to discuss drafting a Memorandum of Understanding (MOU) delineating the two agencies' responsibilities under the Computer Security Act. Kammer, the son of two NSA employees, was deeply concerned about protecting national-security and law-enforcement interests

in cryptography. His instincts were to defer to the intelligence agency on control over civilian cryptography standards.[36]

The debate surrounding the Computer Security Act, as well as the act itself, had made it clear that NIST was in charge of developing civilian computer security standards. The MOU between NIST and NSA mandated that NIST would "request the NSA's assistance on all matters related to cryptographic algorithms and cryptographic techniques" (USDoCDoD 1989, p. 2). A Technical Working Group (TWG), consisting of three members each from NIST and NSA, would review and analyze issues of mutual interest, including the security of technical systems, *prior to* public disclosure (USDoCDoD 1989, p. 3). The opportunity to vet proposed standards before any public airing put NSA in a controlling position in the development of civilian computer standards.

In making civilian computer security standards part of NIST's bailiwick, the Computer Security Act had placed decisions regarding the approval of these standards in the hands of the Secretary of Commerce. The MOU changed this so that, although appeals could still be made to the Secretary of Commerce, members of the Defense Department were free to appeal proposed NIST standards to the Secretary of Defense before any public airing. Appeals of TWG disagreements would go to the Secretary of Commerce *or* the Secretary of Defense, and from there to the president and the National Security Council (the same group that had promulgated NSDD-145).

The Government Accounting Office was appalled. Milton Socolar, a special assistant to the Comptroller General, told Congress: "At issue is the degree to which responsibilities vested in NIST under the [Computer Security] act are being subverted by the role assigned to NSA under the memorandum." (Socolar 1989, p. 36) Congress's research arm, the Office of Technology Assessment, described the MOU as "ced[ing] to NSA much more authority than the act itself had granted or envisioned, particularly through the joint NIST/NSA Technical Working Group" (USC-OTA 1987, p. 164). NIST Acting Director Raymond Kammer, who had signed the document, disagreed: "As I've heard people interpreting the . . . memorandum of understanding, it occurs to me that many individuals doing the interpreting are perhaps starting from a perspective I don't

share, namely that NSA has had some trouble accepting the act. My experience in the months that I have been negotiating and working with the current management of NSA is that they fully understand the act, and that their understanding and my understanding are very consistent. I have no reservations about their willingness to implement the act as written." (Kammer 1989)

Representatives Jack Brooks and Daniel Glickman viewed the Digital Signature Standard as a test of who was running the show on civilian computer standards;[37] they were proved right.

The Digital Signature Standard

Many breaches of confidentiality are difficult to detect, and even when a breach is clear it is often not at all clear where the problem lies. In light of this, any attempt by a litigant to claim that the insecurity lies with bad cryptography and thus force the protection techniques into the open is likely to fail. On the other hand, digital signatures—as a consequence of their function of resolving disputes between users of electronic networks—are certain to give rise to litigation over the adequacy of the signature methods. This is all the more true because digital signatures are a novel idea in commerce, whereas the notion of protecting messages by encryption is well established even though the details of particular methods may be unfamiliar. It is therefore necessary to provide a public digital signature mechanism that is open to examination by cryptographic researchers and expert witnesses in order to foster the public confidence necessary to achieve acceptance of the new technology.

In the spring of 1989, representatives from NIST and NSA began meeting to develop a set of public-key-based standards. First on the agenda was a digital signature standard to be included in the FIPS series. NIST proposed the Rivest-Shamir-Adleman algorithm (USGAO 1993b, p. 20). During its very public twelve-year lifetime, no cryptanalytic attacks had succeeded in breaking that algorithm. It was an accepted industry standard for digital signatures, and several standards organizations had formally adopted it. But in Technical Working Group meetings the NSA representatives rejected RSA. Presumably they objected to its flexibility, which allowed it to be used for purposes of confidentiality as well as authenticity. Raymond Kammer concurred in the decision, arguing

that the infrastructure needed for public-key management made RSA an unwieldy digital signature standard. Kammer ignored the fact that any digital signature standard adopted for widespread use would entail a key management facility.

Through 1989 and 1990 the Technical Working Group of NIST and NSA representatives met once a month, and each month no progress was made. "We went to a lot of meetings with our NSA counterparts, and we were allowed to write a lot of memos, but we on the technical side of NIST felt we were being slowrolled on the Digital Signature Standard," recalled Lynn McNulty, NIST's Associate Director of Computer Security, "In retrospect it is clear that the real game plan that NSA had drawn up was the Capstone Chip and Fortezza card—with key escrow all locked up in silicon."[38]

A year after the meetings on digital signatures began, NSA presented its proposal: an algorithm it had developed itself. NSA's justification for its algorithm was a "document, classified TOP SECRET CODEWORD, [that] was a position paper which discussed reasons for the selection of the algorithms identified in the first document" (USDoC 1990b). According to NSA, the proposed algorithm was based on unpatented work done by Taher ElGamal when he was a graduate student at Stanford University under Martin Hellman (ElGamal 1985). Outside the agency even that was questioned. The algorithm had been developed by David Kravitz at NSA (Kravitz 1993), and the technique bore a strong resemblance to one developed by the German mathematician Claus Schnorr, who had patented his algorithm in the United States and in various European countries.[39] Concerned about potential patent conflicts, NIST officials went to negotiate with Schnorr over selling his rights, but the government did not want to pay his asking price (reputed to have been $2 million).

NIST proposed Kravitz's algorithm as the Digital Signature Standard (USDoC 1991b). The computer industry objected to this because the algorithm was not interoperable with digital signatures already in use. The proposed standard had a 512-bit key size, but Bell Labs scientists had already shown that the Kravitz algorithm was not particularly secure with a 512-bit key (LaMacchia and Odlyzko 1991; Beth et al. 1992). Furthermore, it was significantly slower than the RSA algorithm in signature verification, taking roughly 10 times as long on comparable processors.[40]

In abandoning the RSA algorithm in favor of the proposed NSA algorithm, NIST had traveled a considerable distance from the Computer Security Act.

Critics saw the dark hand of NSA behind NIST's bumbles. When questioned by a congressional committee, NIST director John Lyons denied such pressure. "What's your response to charges that NSA, either directly or through the National Security Council, continues to control NIST's computer security program?" Representative Jack Brooks asked Lyons. "My response is that it's not true," said Lyons. "We're running our program. We consult with them, according to the 1987 legislation, but they know and we know that we make these decisions." (Lyons 1992, p. 176) The record, released after Freedom of Information Act litigation, told a different story. A January 1990 memo from the NIST members of the Technical Working Group said: "It's increasingly evident that it is difficult, if not impossible, to reconcile the requirements of NSA, NIST and the general public using the approach [of a Technical Working Group]." (USDoC 1990a) Completely contrary to Congress's wishes, NSA was making the decisions on civilian cryptography.[41]

In its report on the Computer Security Act, the House Government Operations Committee said "NSA is the wrong agency to be put in charge of this important program." (USHR 100-153 *Computer Security Act*, p. 19) Congress concurred and passed the measure. It looked as if the intelligence agency had made an end run around Congress. Under the Computer Security Act, NIST was supposed to develop cryptography standards for the public sector, but the combination of the MOU and NSA's clout prevented such an outcome. Lynn McNulty later commented: "We bent a hell of a lot backwards to meet national security and law enforcement requirements, but we didn't do much to meet user requirements." Various government observers, including the Office of Technology Assessment and the General Accounting Office, concluded that the MOU had put NSA in the driver's seat—not at all the intent of the Computer Security Act.[42]

The proposal for a Digital Signature Standard was put forth in 1991. Public objections resulted in modifications, including a flexible key size (key sizes from 512 to 1024 bits are permitted, in jumps of 64 bits). On May 19, 1994, over strong protests from industry and from academia,

the government adopted DSS as Federal Information Processing Standard 186, announcing that the "Department of Commerce is not aware of patents that would be infringed by this standard" (USDoC 1994c).[43]

Ceding Even More Control

While Congress waited to see how NIST would handle implementing a digital signature standard, a transfer of power was occurring behind the scenes. In the drafting of the MOU, NSA had recommended that the FBI be part of the Technical Working Group; NIST staffers had objected, and this clause was dropped (USDoC 1989). But Kammer, the acting director of NIST, was concerned that his agency was not properly equipped to develop civilian cryptography, the job Congress had handed to it. He and Clinton Brooks, advisor to NSA's director, shared their concern with the FBI.

Their initial reception was cool. "The first couple of times [we went there] they said, 'Why are you bothering us?'" recalled Kammer. "They kept giving inappropriate responses; the FBI didn't understand the issue. Cryptography is a somewhat peripheral issue to the FBI." Brooks and Kammer presented the dangers of encrypted telecommunications, but it took the FBI some time to understand. "Ray and I kept encountering lots of blank stares," Brooks said later. "What we were encountering was a lack of appreciation that digital communications was here. Wiretapping was just doing clips, or going to the phone office. But the phone companies had all gone digital. The next step [in understanding] was that encryption was going to exist on the digital lines."[44] To the FBI the cryptographic issues seemed futuristic.

There was a clash of understandings. "A successful FBI agent," Kammer explained, "kicks in the door, arrests the guy, and goes on to the next case." The issues NIST and NSA were raising were more subtle. "A successful NSA man … well give him a hard problem and the first thing he'll do is sit down and think—sometimes for a very long time."[45] NSA had been thinking about strong cryptography for a long time, but the FBI did not have any experts remotely close to the area. The closest the Bureau had were agents working on defeating electronic locks and alarms.

After a number of visits to the FBI over several months, Brooks and

Kammer encountered James Kallstrom, Chief of the Special Operations Branch of the New York Field Office. "It was obvious," Kallstrom recalls, "that encryption had been around a long time. What was new here was it had never been an issue before for the general public. Old encryption didn't work; it was too bulky, you sounded like Donald Duck. But in the late eighties we could see that it wouldn't be very long before cheap encryption would be around that would put us out of business."[46]

Kallstrom's tenure in New York undoubtedly shaped his viewpoint. Historically, New York State has relied heavily on electronic surveillance.[47] For example, over a third of the 1994 Title III electronic surveillances occurred in New York State.[48] California, whose big cities suffer similar problems of drugs and crime, had one-eighth as many.[49]

Kallstrom could not imagine law enforcement without wiretapping and did not want wiretapping to disappear from law enforcement's arsenal. He went to work: "From the standpoint of this becoming an issue in the government, from the standpoint of law enforcement, we were the user, the customer. An Interagency group was formed; the squeaky wheel was us. We went to both [NIST and NSA]. We have a long-standing relationship with NSA; we have a responsibility for counter-terrorism and intelligence." NSA was immediately part of an interagency group focusing on problems of domestic use of strong cryptography. NIST joined shortly afterwards. "It wasn't a function of official policy. We have always recognized NSA as a premier agency [in intelligence]. NIST was also at the table."[50]

By 1991 the FBI had formulated a policy that included shoring up its ability to perform electronic surveillance, particularly wiretaps, and preventing the establishment of unbreakable cryptography in the public sector. Efforts in support of this policy included the Digital Telephony Proposal and the concept of key escrow, which were introduced to the public in 1992 and 1993 respectively.

In negotiating the MOU, NSA had sought to include the FBI as a full-fledged member of the Technical Working Group (which would have meant that two-thirds of the participants came from either law enforcement or national security). After that effort was rebuffed by NIST scientists, Kammer and Brooks brought the FBI in by different means. The FBI's involvement in encryption issues buttressed NSA's position.

With the end of the Cold War, law-enforcement issues were significantly closer to the public's heart than national-security concerns. By replacing national-security concerns over cryptography with law-enforcement concerns, the FBI succeeded in returning much of the control of civilian cryptography to NSA.

"The whole Digital Telephony [effort] came out of [our meetings]," Clinton Brooks said some time later.[51]