Glossary

Advanced Encryption Standard (AES)—a symmetric-key encryption algorithm working on 128-bit block size data with 128-, 192-, or 256-bit keys that is a Federal Information Processing Standard replacing DES, the Data Encryption Standard.

AFCRC—Air Force Cambridge Research Center.

ANSI—American National Standards Institute.

ASCII—American Standard Code for Information Exchange—The government's adoption of this code, which is ubiquitous today, made it dominant over the rival EBCDIC encoding used by IBM.

analog scrambler—cryptographic device operating on continuous (analog) signals, rather than on discrete elements like bits or letters.

asymmetric cryptography—See: public-key cryptography.

authentication—the process of determining whether an individual is whom they claim to be. Weak authentication methods might be a user name and password; strong authentication methods typically include several factors, e.g., something you are (a biometric), something you have (a physical token), and something you know (a password).

bit—short for "binary digit," the smallest unit of data stored in a computer. Bits have a single binary value, either a "0" or a "1."

block cipher—a cryptosystem on a block of symbols that sequentially repeats an internal function, called a *round*.

bps—bits per second.

CCEP—Commercial COMSEC Endorsement Program—A program set up

in the mid 1980s by NSA in an attempt to get industry to invest in building a new generation of communication security equipment.

cipher text—Unintelligible text or signal produced by a cryptographic system. (adj.: ciphertext)

Clipper—name of a chip implementing the Skipjack encryption algorithm with key recovery.

CALEA—Communications Assistance For Law Enforcement Act—a 1994 law requiring that digitally switched telephone networks deployed after 1998 be built wiretap enabled according to standards defined by the US government.

COMINT—Communications intelligence—the extraction of information for opponents communications.

COMSEC—Communications security—protection of communications against communications intelligence.

crypto wars—political battle in the US in the 1990s over the freedom to use cryptography for personal and commercial applications.

Diffie-Hellman key exchange—a process using exponentiation in modular arithmetic for negotiating a shared secret key between two parties without concealing any of the messages from opponents.

DS1—Telephone communication standard for transmitting 24 voice channels, together with signaling information, simultaneously at a rate of 1.544 megabits per second.

EBCDIC—Embedded Binary Coded Decimal Interchange Code—IBM encoding used for representing characters.

electronic surveillance—the use of electronic equipment to surveil private conversations.

EES—Escrowed Encryption Standard—an originally classified algorithm (Skipjack) that was to be implemented on tamper-resistant chips (Clipper) with escrowed keys.

Enigma—a three-rotor encryption machine developed for commercial use in the 1920s and widely used by the Nazis during World War II.

FBI—Federal Bureau of Investigation—the main criminal investigatory agency of the US government, the FBI is part of the US Department of Justice. The FBI is responsible for investigating all federal crimes

except those specifically assigned to other agencies (e.g., the Secret Service is responsible for investigating cases of counterfeiting).

FCC—Federal Communications Commission—the federal agency responsible for regulating interstate and international communication, whether by radio, television, wire, satellite, or cable.

Federal Information Processing Standard (FIPS)—an information processing guideline set for federal government departments and agencies by the National Institute of Standards and Technology, but often having wider applicability.

FISA—Foreign Intelligence Surveillance Act—a 1978 law providing for interception of communications within the United States for intelligence purposes.

Freedom of Information Act (FOIA)—A 1966 federal law establishing the public's right to obtain information from federal government agencies. The law applies to Executive Branch departments, agencies, and offices.

IP—Internet Protocol—the Internet Protocol is the method by which data travels from one computer to another over the Internet.

IP address—the IP, or Internet Protocol, address, is a unique number that devices use to communicate across a computer network.

ISDN—Integrated Services Digital Network—ongoing replacement of existing 'analog' telephone service by digital service.

KMF—Key Management Facility—a network resource that assists users in acquiring keys needed to establish secure communications.

LEAF—Law Enforcement Access Field; the law-enforcement access to the keys of the Clipper system.

mail cover—the process of recording information on the outside cover of mail as well as contents of second-, third-, and fourth-class mail, and international parcel post mail without the consent of the recipient.

message digest—a cryptographic function that takes input data (often a entire message) and outputs a short, fixed length result.

MI5—Military Intelligence 5, more accurately known as the Security Service—the British counterintelligence organization. The closest US cognate is the counterintelligence function of the FBI.

MI6—Military Intelligence 6, more accurately known as the Secret In-

telligence Service—the British foreign intelligence service. The US cognate is the CIA.

minimization—In law enforcement, the practice of limiting interception to those portions of communications that are or may be of legitimate investigative interest. In intelligence, the more limited practice of limiting interception to exclude forbidden material such as the communications of the citizens of the host country. In general, minimization may be by channel, person, time, or subject matter.

MOU—Memorandum of Understanding—a legal contract determining the obligations of two governmental entities (or between the government and a contractor) regarding joint work.

NAACP—National Association for the Advancement of Colored People—the largest civil-rights organization in the United States, founded in 1909 with the mission of "ensur[ing] the political, educational, social and economic equality of rights of all persons." The NAACP played a central role in the civil-rights movement of the 1950s and 1960s.

NBS—National Bureau of Standards—US government bureau whose responsibilities included the development of computer security standards for civilian federal agencies; renamed National Institute of Standards and Technology in 1988.

NIST—National Institute of Standards and Technology—US government bureau whose responsibilities include the development of computer security standards for civilian federal agencies.

NRC—National Research Council—research arm of the National Academy of Sciences and the National Academy of Engineering.

NSA—National Security Agency—the US government agency responsible for spying on foreign communications and for protecting military, diplomatic, and intelligence communications of the US government and its contractors.

NSDD—National Security Decision Directive—a directive issued by the president (usually classified) on military, intelligence, and security matters. Such directives, unlike Executive Orders, often change name from one administration to the next and in recent decades have also been called "national security directives," "presidential directives," and "national security action memoranda."

OCR font—Optical Character Recognition font—fonts designed to be read easily by machines.

PBX—Private Branch Exchange—a telephone switch belonging to a business or other organization rather than the phone company.

PCMCIA—Personal Computer Memory Card International Association.

PGP—Pretty Good Privacy—A program originally written by Philip Zimmerman for encrypting computer files and email. The name of the company formed to develop and market the program.

plain text—Intelligible text or signals—text or signals that have not been encrypted. (adj.: plaintext)

private key—In public-key cryptography, the key that is known only to the recipient and is used for decryption and signing.

public key—In public-key cryptography, the key that is widely available and is used by the sender to encrypt and by the receiver to verify signatures.

public-key cryptography—cryptography in which communications are controlled by two keys, one of which can be made public without revealing the other. Public key cryptography makes it possible to separate the capabilities for encrypting and decrypting.

RC2—a block cipher designed by Ron Rivest of MIT and marketed by RSA Data Security as an exportable replacement for DES.

RC4—a fast stream cipher designed by Ron Rivest of MIT and marketed by RSA Data Security.

Real ID Act—a law requiring the issuing of driver's licenses by US states to conform to federal standards that effectively create a national ID card.

realtime—something operating in "real time," i.e., without the opportunity to calculate for as long as needed.

rotor machine—a cryptographic device consisting of a machine with several rotors, a disk that implements a cipher alphabet. Each disk face has a number of electrical contacts corresponding to the letters of the alphabet, and each contact on the front face is wired to exactly one contact on the rear face. As an electrical signal passes through the rotor, the signal is carried to a new alphabetic position, just as a letter

looked up in a cipher alphabet changes to another letter. Rotor machines typically have at least three rotors.

RSA—the Rivest-Shamir-Adelman public-key cryptosystem. The security of the RSA system is based on the difficulty of factoring large numbers.

shift register—an electronic device made up of a number of *cells* or *stages*, each of which holds a single 0 or 1 of information. As the shift register operates, the data shift one or more places along the register at each tick of the clock. In addition to moving left or right, some of the bits are modified by being combined with other bits.

smart card—a plastic card, typically the size of a credit card, with an embedded microchip.

SSL—Secure Socket Layer—the transport-lay security mechanism used in Web browsing to support the secure form of the Hypertext Transfer Protocol, HTTPS.

STU-III—third-generation secure telephone unit—A US government secure telephone system constructed during the 1980s and using public-key cryptography.

symmetric cryptography—cryptography in which the capability to encrypt and the capability to decrypt are inseparable, in contrast to asymmetric cryptography.

Title III—Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 USC §2510–2521) established the basic law for interceptions performed in criminal investigations.

traffic analysis—the study of the patterns of communication. An opponent can learn a great deal about the activities of an organization without being able to understand any individual message.

transactional information—information revealed during the conduct of a transaction, e.g., the time you left the (paid) parking lot, or the source and destination of an email.

Triple DES—a block employing DES three times in a row with different keys; surprisingly this has a workfactor of 2^{108} to break (rather than the expected 2^{168}).

TSD—Telephone security device—a device that is not a complete telephone but provides encryption when installed in conjunction with a telephone. Especially, the AT&T TSD-3600.

TWG—Technical Working Group set up between NIST and NSA to implement joint work on cryptography.

Type I—A category of equipment certified only for the protection of "unclassified sensitive information" that was available without the administrative controls that applied to equipment for protection of classified information.

Type II—Equipment certified for protection of sensitive information.

Venona—a long-running project by NSA (along with other organizations such as the British Government Communications Headquarters (GCHQ) and MI5) to exploit a set of Soviet messages sent in the 1940s and the early 1950s. The messages, made vulnerable by the reuse of "one-time" keying material revealed much information about Soviet spies working against Britain and the United States.

VPN—Virtual Private Network—a dynamic network constructed from encrypted tunnels through the Internet.

VoIP—Voice over IP—transmission of voice calls over the Internet.

workfactor—the number of operations needed to break a cryptosystem.

911—In the United States and Canada, the phone number for emergency services: police, fire, and ambulance.

9/11—September 11, 2001—the day on which 19 terrorists hijacked four large passenger planes, crashing two into the World Trade Center in New York and one into the Pentagon; the fourth plane crashed in the Pennsylvania countryside.