NATIONAL SECURITY AGENCY

UNITED STATES OF AMERICA

# Securing Record Communications: The TSEC/KW-26

Published in 2003

CENTER for CRYPTOLOGIC HISTORY

*This publication is distributed FREE by the*
*National Security Agency.*
*If you would like additional copies, please*
*submit your request to:*
*Center for Cryptologic History*
*National Security Agency*
*9800 Savage Road, Suite 6886*
*Fort George G. Meade, MD  20755-6886*

# *Securing Record Communications: The TSEC/KW-26*

**Melville Klein**

## *Preface*

One of the missions of the National Security Agency (NSA) is to protect classified information whether in storage, processing, or transit. Collectively, *information system security (INFOSEC)* is the development and application of hardware, software, and doctrine. The "in transit" element, called *communications security (COMSEC)*, assures that the underlying information is protected from external exploitation, disruption, or misrepresentation and is available only to authorized recipients. This brochure tells the cradle-to-grave story of highly successful *cryptographic* equipment for *teletypewriter* (TTY) communications, the TSEC/KW-26 and the people who developed, produced, and fielded it. (The *italicized words* are defined in the appended glossary.)

## *Teletypewriter COMSEC*

The changes in communication technology leading up to the introduction of the KW-26 date back to 1907 with the introduction of the Start/Stop method of synchronizing printing telegraph equipment by Charles L. Krumm and his son, Howard Krumm. Until that time synchronous printing telegraph systems employed constant length codes, e.g., a five-element *Baudot*. However, these systems required very accurate means for maintaining synchronism between electromechanical transmitting and receiving instruments. "Start/Stop" overcame this drawback by resynchronizing at the start of each character, making it no longer necessary to accurately control the speed of the instruments.

Each character was assigned a unique five-unit combination of "marks and spaces" preceded by a start element and followed by a stop element. The thirty-two possible combinations accommodated the Roman alphabet and six control codes (upper case, figures, line feed, carriage return, etc.) and were adopted as an International Telegraph Alphabet #2 (IA#2). Start/stop *Teletype* began to find worldwide commercial applications about 1920. The instrument employed a typewriter-style keyboard and printed the received signals directly onto paper tape, without requiring the intermediate use of perforated tape at either end of the system. It was capable of working at a speed of forty words per minute.[1] For the first time, anyone who could type could send messages without needing a skilled operator or for that matter any attendant at the receiving end. This system was so successful that it became the dominant means of handling record traffic, but not securely.

In 1917 a young AT&T research engineer named Gilbert S. Vernam, working on new developments in telegraphy, came up with a novel (and relatively simple) scheme for encrypting TTY.[2] He mixed two Baudot-coded punched paper tapes (hole being a "+," no hole a "-"): one tape contained the *plaintext* message and the other the "*key*." These tapes were added "modulo 2" ("exclusive or") in a mechanical tape reader producing output *cipher* signal. At the receiving end, the incoming cipher is added (modulo 2) with a local copy of the identical key producing the plain text. If the key is unpredictable and "flat" (i.e., probability of a "+" equals that of "-" = ½), then the cipher text is "unbreakable" (impervious to *cryptanalysis*). The Vernam logic:

**Modulo Two Addition (*)**

| plain | key | cipher | | |
|---|---|---|---|---|
| + | * | - | = | + |
| - | * | + | = | + |
| + | * | + | = | - |
| - | * | - | = | - |

Vernam had invented the unbreakable cipher: "*one-time tape*" (OTT) for *on-line* TTY encryption. In 1919 he was granted a patent, perhaps one of the most important in the history of cryptography.

AT&T demonstrated this technique to the U.S. Army Signal School in 1918. They added two (modulo 2) relatively prime eight-foot tape loops, making a secondary key tape of one million key characters. The Signal Corps showed little interest. It wasn't until WWII that the Signal Corps adopted it for high-level TTY traffic (SIGTOT). In the 1920s AT&T marketed the Vernam system for commercial privacy applications. Though an engineering success, it was a commercial failure. Cable companies and businesses continued to use old-fashioned *codes* instead of secure encryption.[3]

Krumm and Vernam opened new vistas for TTY encryption, a far cry from the technology of the "pencil and paper" codes and ciphers for hand-keyed Morse deployed at that time. A competing technology for securing TTY messages was invented soon after Vernam: the electro-mechanical rotor machines. Though they operated off-line and were more complex devices, their operational benefits in key management considerably outweighed the production/destruction of mounds of *one-time* tapes. Invented by four men in four different countries in the 1920s, an American, a German, a Dutchman, and a Swede, wired rotor machines were the principal means of message security before and through WWII for governments and commerce.[4] During WWII the U.S. used commercial off-line rotor machines, e.g., Hagelin M209, SIGABA, SIGTOT, with government-produced key.[5]

## *Lessons Learned from WWII*

The stunning successes of Allied cryptologists in breaking the Enigma[6] and Purple did not go unheeded by the Department of Defense after the war. The military services undertook a concerted recruitment effort for engineers and mathematicians to develop a first-rate in-house cryptographic capability. The Army formed a COMSEC R/D organization within the Army Security Agency (ASA); the Navy had a comparable organization, the Naval Security Group (NSG). The senior cadres in ASA were former Signal Corps officers and noncoms.

In-house development of improved off-line rotor systems to replace the WWII rotor machines was initiated. ASA also sought a high-speed on-line OTT equipment to replace the British 5-UCO currently being used in the intelligence community. The British enjoyed great success with this system because, being fully synchronous, it could be electrically regenerated on tandem high frequency (HF) radio links. Like predecessor U.S. equipment (SIGTOT), it used “mountains” of key tape to operate on a 24/7 basis. The shear magnitude of generating, certifying, and destroying key tape and the cost of distribution and accountability limited their use to the most sensitive traffic. On the plus side, OTT systems provided *traffic flow security (TFS)* and operated directly with commercial circuits. Another inherent capability of the 5-UCO was that the operator at the receive end could maintain *crypto-synchronization* if the path delay suddenly changed by “walking up and down” the key tape (one character at a time or one bit at a time). This procedure avoided the operationally cumbersome task of a restart.

With the merger in 1949 of the service cryptologic agencies into the Armed Forces Security Agency and the creation of NSA in 1952, jurisdiction over U.S. cryptography was vested in NSA. This extended to major players outside the Department of Defense. Throughout, a primary objective was *communication security* for record traffic. Howard Barlow, chief of the Record and Data group, initiated as a high-priority research on viability of electronic encryption for TTY, namely:

> ***An affordable, inconspicuous value added adjunct to the user's communication system. It should not be a time or an operational bottleneck and [should] assure that the work factor is commensurate with the protection period.***

This was a decided break from past: in technology, tubes rather than relays and wired rotors; in cryptography, keystream generators rather than one-time tape systems; and in key management punch cards rather than key lists or wired rotors. To be retained in the replacement of the 5-UCO was the Vernam modulo-2 convention and its traffic flow security (TFS) capability.

The proposed TSEC/KW-26 development was targeted to the above requirements, i.e., to provide TFS and message security for all classifications of record traffic.

## *Development Effort*[7]

When the requirements for secure TTY were defined, the most mature electronic technology was the miniature vacuum tube. Tubes had limitations, however, related to their reliability and power consumption. Although the transistor had been invented (1947), it was not ready for "prime time." Therefore, the search was on for an alternative solution. The R/D engineers sought out leading-edge industrial partners in digital technology to implement cryptographic concepts generated in house.

The KW-26 graphically illustrated this synergism. A young engineer working in Howard Barlow's division was intrigued with the research on Bi-Magnetic cores by a former college classmate, Lyle Thompson at Burroughs Corporation Research Center. Lyle described how they were using multiple winding torroidal magnetic cores as Bi-Stable Magnetic Elements (BIMAG).[8] With appropriate interconnections, they performed the binary logic and were used to implement shift registers. This spawned ongoing technical exchanges between the logic designers at the Research Center with Howard Barlow and members of his staff for funding further research.

Concurrently in 1952, an experimental vacuum tube model of the KW-26 was being fabricated in house under Joe Hannan, a recent electrical engineering graduate, Vern Zeigler, and two Army technicians. Joe's team breadboarded a "proof of concept" model based on the Dick Chiles/Dick Marsh cryptologic and I/O guidance by Frank Mitchell, Joe's supervisor, for the plethora of communication interfaces the KW-26 would face. Charles Napier designed a novel *common fill device (CFD)*, a first of the breed, for the daily crypto-variable. It used an IBM card punched in a RemRand format (45 vice 80 columns, round vice rectangular holes). His design, fabricated in the R/D model shop, was incorporated into the breadboard. In practice the operator inserted the daily *key card* into the CFD and closed the door securely, locking the card in place. COMSEC doctrine did not permit card re-use. Therefore, to meet this requirement, the card was severed upon reopening the CFD.

The completed breadboard model required a six-foot telephone relay rack for each transmitter and receiver terminal. In 1954 TCOM, the NSA telecommunication organization, successfully tested the system on a circuit looped at an overseas site. It demonstrated the feasibility of electronic TTY encryption. The system employed the newly devised Koken crypto-*algorithm* used with a free-running TTY input. As the breadboard was being built and tested, Joe Hannan prepared the specification for an outside development contract.

## *Engineering Development Contract*[9]

The Request for Proposal (RFP) was released sole source in 1953 to the Burroughs Corporation. Its objectives were to demonstrate

- **reliable logic elements**
- **low power consumption**
- **controllable spurious radiation**
- **ease of use**
- **availability (continuous operation)**
- **in/output compatibility with associated communication systems**

The RFP was based on Fibonacci vice Koken motion. Their proposed cryptologic design was based solely on BIMAG, from the Fibonacci shift registers to the binary logic combining elements. The CFD was government furnished. After evaluation of the Burroughs bid from cost, schedule, and technical risk, NSA awarded the development contract in 1953. The initial design indicated that BIMAG were superior to vacuum tubes on reliability and power consumption (though the KW-26 clock rate was relatively slow, less than 5 kHz, the vacuum tube pentodes driving the BIMAG elements were approaching their design limit).

The first model was delivered in 1955. This model demonstrated BIMAG as a viable technology for the KW-26 logic. The torroidal cores of exposed magnet wire were mounted on “islands” along the edge of the plug-in circuit board and hand-wired while on the circuit board. Both the Burroughs and the NSA engineers recognized the next hurdle, i.e., the need for more practical packaging of BIMAG circuits in the final engineering development phase. These units also were successfully evaluated on looped TCOM circuits.

A follow-on contract for Final Engineering Development Models was awarded to Burroughs in 1955 to correct the above deficiencies. During this phase each core was packaged as a potted module with twelve I/O pins connected to six internal windings. Up to eighty of these potted modules were mounted on large multilayer printed circuit (PC) boards.

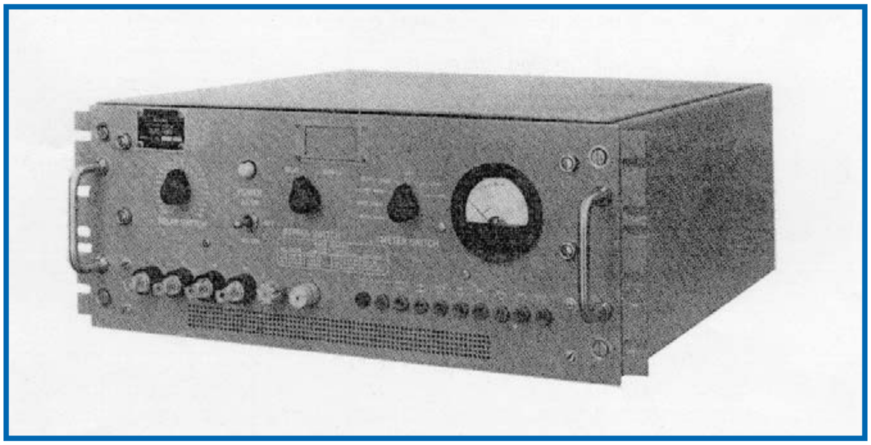
Five of these PC boards were used in the transmitter and receiver equipment. Power pentodes were mounted on each of several plug-in packages. The Burroughs engineers also "productized" the CFD. Initial deliveries began in 1957 for customer evaluation.

Environmental tests showed these models exhibited intermittent loss of *crypto-synchronization*. Extensive temperature tests (up to 125 degrees F) revealed that the ceramic capacitors were shorting out at the higher temperatures. Erie, the manufacturer, upon subsequent testing discovered a "bad batch" had been shipped to Burroughs. As a result, Erie instituted new quality control procedures, and Burroughs instituted incoming inspections. No further problems occurred. The R/D project team released the final design to the COMSEC production engineers for procurement of operational equipment. In the interim Joe Hannan and Tony Russo participated in the ongoing operational evaluation with TCOM.

## *Operational Trials*[10]

Final engineering development units were operationally evaluated on the *CRITICOMM* network (the title assigned by the JCS to those communications supporting the National SIGINT mission). The KW-26s performed very well except for the problem of dealing with transmission anomalies. They lacked the ability to "walk" up and down the *key stream* as had been possible with the 5-UCO. This limitation was later overcome by inserting a twenty-one-bit delay in an appliqué (TSEC/HW-8) between the incoming line and the receiving KW-26. Initially the operator would set the delay at 11 bits and bring up the link. If the path delay shifted abruptly, the receive operator would search for the correct delay, thereby maintaining crypto-synchronization (garbled traffic would, of course, have to be re-sent). This was effective about 90 percent of the time, thus avoiding the time-consuming

*Fig. 1. TSEC/HW-8, Transmission Delay Compensator*



restart coordination with the sending station. NSA and the Navy purchased approximately 450 HW-8s.

Services' requirements for numerous modes and speeds significantly increased the cost, schedule, and the complexity of the original engineering design. Of the modes and speed combinations possible, it is doubtful more than three or four were ever used. One option, the so-called speed normalizer, delayed the production deliveries at a time when the equipment was critically needed. This option was designed to operate via the low-speed transoceanic direct current cables, which were in their last days of service. Other costly options permitted operation through AT&T mechanical regenerative repeaters, also being replaced in the 1960s.

## Production

The NSA COMSEC Production organization

- **coordinated DoD and Community buys**
- **issued RFPs**
- **handled contract management**
- **coordinated acceptance tests**

- **provided operational support**
- **provided technician and operator training**
- **performed life-cycle spare parts acquisition**
- **coordinated change orders**
- **published manuals**
- **performed key management**
- **carried out inventory control**
- **handled decommissioning effort**

The initial production order for 1,500 for CRITICOMM and related SIGINT requirements was awarded to Burroughs in 1957. During this initial procurement there was continual pressure from other services' programs for KW-26s. Subsequent procurements running from the early 1960s produced over 14,000 units. These were procured for Navy shore facilities and shipboard use, Army and the Air Force tactical point-to-point service, and in fixed plant environments by the Defense Communications Agency, State, and CIA.

A KW-26 system (transmitter or receiver) contained over 800 cores and approximately 50 vacuum-tube driver circuits, occupying slightly more than one half of a standard relay rack. Most of the space in the rack and most of the 1-kw input power were required for the special-purpose vacuum tube circuits needed to provide compatibility with the multiple input and output circuits configurations.

## *Operational Use*

The KW-26 was the workhorse cryptosystem for the point-to-point circuits of the CRITICOMM network. TCOM also used it to provide traffic flow and content security to/from SCA SIGINT sites to in-house NSA analysts. The services used KW-26 to secure their tactical torn tape and store and forward message networks. In the early days of DCA, the KW-26 was the principal encryptor for the AUTODIN trunks; CIA and State deployed them in their point-to-point circuits.

Starting in the mid-1980s, the system was decommissioned by NSA, being replaced by the more advanced solid-state data encryptor, TSEC/KG-84.

## *Parting Lessons Learned*

In the 1950s the requirements process, lacking a command decision authority within the DoD and the intelligence community, subjected the multi-user KW-26 to

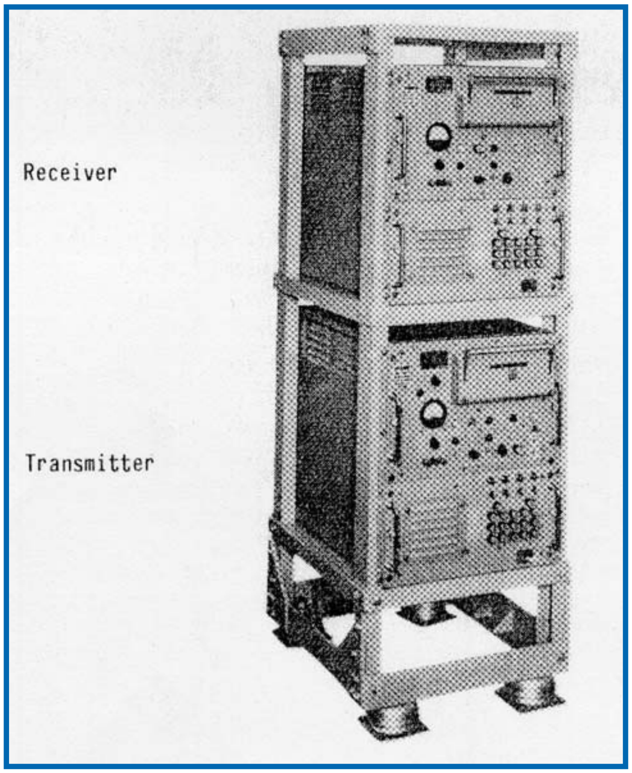


*Fig. 2. TSEC/KW-26C, electronic synchronous teletypewriter security equipment*

a plethora of engineering changes. Originally specified as a limited mode, fixed-plant equipment, the equipment had to be modified during its development to handle the numerous operational modes, e.g., shock and vibration of sixteen-inch guns being fired aboard ship. Its developers quickly realized the need for far greater understanding of user environments in preparing specifications, as well as a better mechanism to incorporate engineering changes after operational testing. To the extent possible, the handoff from R/D to Production Engineering should strive to be a "build to print" process. Having the ability to slave all the KW-26 transmitters in a communications center to a master clock would have been a useful tool to reduce preventive maintenance and improve availability.

## *Epilogue*

The KW-26 truly was a "value added" adjunct to secure point-to-point TTY communication circuits. From an operational and maintenance viewpoint, it withstood the rigors of sixteen-inch guns being fired and overall experienced very few operational outages. It met the operational objectives for a diverse set of users, particularly those in the CRITICOMM network and in the general service (GENSER) community. For over twenty-five years it served the DoD and the intelligence community, throughout the Cold War.

Decommissioning lasted several years. NSA instructed the services and other "holders of record" of the "demilitarization process" in returning the sensitive components to the Information Assurance Directorate (IAD) or other locations for secure destruction. (These were the tracks on the printed circuit boards and the CFD, which revealed information about the combining and crypto-logic.) The remains (e.g., the aluminum chassis, power supply, I/O), after having their labels removed, were melted down and discarded as scrap.

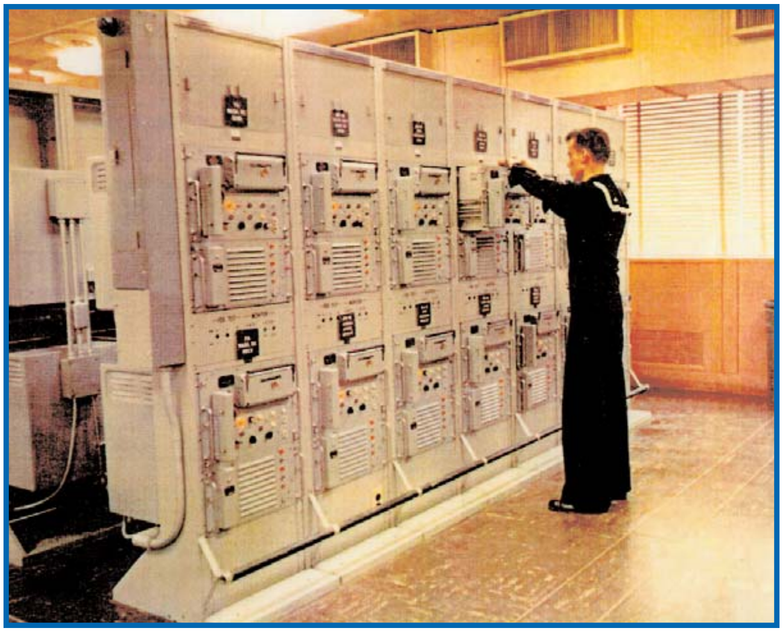


*Fig. 3. The KW-26 in operation*

When the last days of the first KW-26 became apparent, TCOM sent the first units to the NSA archives for historical preservation. The parting words of the principal TCOM transmission system engineer:

> ***I can think of no equipment that advanced the cause of secure 100 WPM Tele-typewriter service more than the KW-26. It also proved that electronic on-line encryption was not only feasible but actually enhanced system performance.***[11]

## Notes

1 (U) J.W. Freebody, *Telegraphy* (Sir Isaac Pitman, 1958)

2 (U) David Kahn, *The Codebreakers* (New York: Macmillan Co., 1967), 394

3 (U) Ibid., 397, 411, 421

4 (U) Ibid.

5 (U) Earl Flowers, David Boak: unpublished notes

6 (U) Center for Cryptologic History, *The Bombe: Prelude to Modern Cryptanalysis* (Ft. George Meade, MD: National Security Agency)

7 (U) Albert J. Meyerhoff, et al., *Digital Applications of Magnetic Devices* (New York: John Wiley and Sons, 1960)

8 (U) Ibid.

9 (U) Joseph Hannan: unpublished notes

10 (U) Richard A. Day: unpublished notes

11 (U) Ibid.

## Acknowledgments

### Contributors

Richard A. Day
Don Burkness
Stanley Disson (Burroughs)
Earl Flowers
Joseph Hannan

### Reviewers

Robert Alde
Howard Barlow
David Boak
Jerry Moskowitz
Richard Proto
Tom Prugh

# *Glossary*

**Algorithm** – A process for completing a task. An encryption algorithm is merely the access, usually a mathematical process, to encrypt and decrypt messages.

**Asymmetric Key Cipher** – Also known as public-private key cryptography system.

**Authentication** – Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

**Baudot code** – A synchronous code in which five equal-length bits represent one character. Note 1: The Baudot code, which was developed circa 1880, has been replaced by the start-stop asynchronous International Alphabet No. 2 (IA No. 2). Note 2: IA No. 2 is not, and should not be identified as, the Baudot code. Note 3: The Baudot code has been widely used in teletypewriter systems.

**Cipher** – Any cryptographic system in which arbitrary symbols or groups of symbols represent units of plain text or in which units of plain text are rearranged, or both.

**Cipher text** – Enciphered information.

**Code** – System of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length.

**Common Fill Device (CFD)** – One of a family of devices developed to read-in, transfer, or store key.

**Communications security (COMSEC)** – Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material.

**COMSEC material** – Items designed to secure or authenticate telecommunications. COMSEC material includes, but is not limited to, key, equipment, devices, documents, firmware, or software that embodies or describes cryptographic logic and other items that perform COMSEC functions.

**CRITICOMM** – The title assigned by the JCS to those communications supporting the national SIGINT mission.

**Cryptography** – Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.

**Cryptosecurity** – Component of COMSEC resulting from the provision of technically sound cryptosystems and their proper use.

**Cryptanalysis** – Operations performed in converting encrypted messages to plain text without initial knowledge of the crypto-algorithm and/or key employed in the encryption.

**Cryptology** – The study of both cryptography and cryptanalysis.

**Cryptosystem** – Associated INFOSEC items interacting to provide a single means of encryption or decryption.

**Decipher** – Convert enciphered text to plain text by means of a cryptographic system.

**Decrypt** – Generic term encompassing decode and decipher.

**Emissions security** – Protection resulting from measures taken to deny unauthorized persons information derived from intercept and analysis of compromising emanations from crypto-equipment or an Information System (IS).

**Encode** – Convert plain text to cipher text by means of a code.

**Encrypt** – Generic term encompassing encipherment and encoding.

**Encryption algorithm** – Set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key.

**End-to-end encryption** – Encryption of information at its origin and decryption at its intended destination without intermediate decryption.

**Fill device** – COMSEC item used to transfer or store key in electronic form or to insert key into a crypto-equipment.

**Hard copy key** – Physical keying material, such as printed key lists, punched or printed key tapes, or programmable, read-only memories (PROM).

**Information Assurance (IA)** – Information operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

**Information System (IS)** – the entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information.

**Information systems security (INFOSEC and/or ISS)** – Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

**Key** – Usually a sequence of random or pseudorandom bits used initially to set up and periodically change the operations performed in crypto-equipment for the purpose of encrypting or decrypting electronic signals, or for determining electronic counter-countermeasures patterns (e.g., frequency hopping or spread spectrum), or for producing other key.

**Key card** – Paper card, containing a pattern of punched holes, that establishes key for a specific cryptonet at a specific time.

**Key stream** – Sequence of symbols (or their electrical or mechanical equivalents) produced in a machine or auto-manual cryptosystem to combine with plain text to produce cipher text, control transmission security processes, or produce key.

**Off-line cryptosystem** – Cryptosystem in which encryption and decryption are performed independently of the transmission and reception functions.

**On-line cryptosystem** – Cryptosystem in which encryption and decryption are performed in association with the transmitting and receiving functions.

**One-time cryptosystem** – Cryptosystem employing key used only once.

**One-time tape** – Punched paper tape used to provide key streams on a one-time basis in certain machine cryptosystems.

**Plain text** – Unencrypted information.

**Security fault analysis** – Assessment, usually performed on Information System (IS) hardware, to determine the security properties of a device when hardware fault is encountered.

**Synchronous crypto-operation** – Method of on-line crypto-operation in which crypto-equipment and associated terminals have timing systems to keep them in step.

**Symmetric key** – the key that is used to encrypt a file or message is the same key that is used to decrypt the file or message.

**Teleprinter** – A teletypewriter that can only receive data and does not have a keyboard for transmission.

**Teletypewriter (TTY)** – A printing telegraph instrument that has a signal-actuated mechanism for automatically printing received messages. Note 1: A TTY may have a keyboard similar to that of a typewriter for sending messages. Radio circuits carrying TTY are called “RTTY circuits” or “RATT circuits.”

**Traffic-flow security** – Measure used to conceal the presence of valid messages in an on-line cryptosystem or secure communications system.

**TSEC nomenclature** – System for identifying the type and purpose of certain items of COMSEC material.

**Work factor** – Estimate of the effort or time needed by a potential perpetrator, with specified expertise and resources, to overcome a protective measure.

**Zeroize** – To remove or eliminate the key from a crypto-equipment or fill device.

(**Sources**: Federal Standard 1037c; National Information Systems Security Glossary – NST ISSI4009)