Protect/Understand Special Data Protection

Proficiency Code: A

Cryptographic devices provide the means to protect our sensitive and classified information from the enemy. Each device can both encrypt a signal for transmission and decrypt a signal to restore it back to its original format. We use digital cryptographic devices to encrypt/decrypt communications links. Within the Air Force communications networks, there are many methods of encryption including IP, end-to-end, link, bulk, and voice. All encryption uses keys and algorithms to enable securing of signals.

Like a vault in a bank, information and communications security use secret combinations to secure the data. The sender locks the transmitted information down with the secret combination, or key, and the receiver (the only person with knowledge of the key) can unlock the information assuming receiver's key is the same. In communication links, this is encryption.

Applying the same security principles to communications links provides much the same advantages to the sender, as long as the key remains secret. The economics of the encoding process greatly favor the authorized users of the communications links. The decoding required by an intruder without the secret key would need massive amounts of operations and expenses, which would start over each time a key code changes.

Going back to the combination lock example, a typical combination might consist of three numbers, each a number between 1 and 40. Let us say it takes 10 seconds to dial in a combination. There are 403 possible combinations, which is 64,000. At 10 seconds per try, it would take a week to try all combinations, though on average it would only take half that long. The computational difficulties of algorithms increase by lengthening the key segment.

The encryption process takes place as a mathematical manipulation of the sender's message, with an inverse process-taking place at the receiving end. With binary communications, the mathematical process can be simply a binary addition of a randomly chosen sequence with a similarly long portion of the message. If the randomly chosen key is at least as long as the message and used only once, the message is unconditionally secure and cannot be broken regardless of processing power.

However, this is not a very practical way to perform the encoding. As we have seen, a finite-length key can be sufficiently long to ensure conditional security; that is, determining the proper key by an exhaustive search is impossible in a practical sense. We achieve a high degree of protection by using a finite-length key and a relatively simple mathematical operation at the sending and receiving ends. The encryption applies on either a link-by-link basis or an end-to-end basis.

Data encryption uses a set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key. Systems that hold the correct key code variable can decrypt this information. The TSEC KIV–7, TSEC, KIV–19 and the KG–175D

(TACLANE) are a few of the most common devices. The different encryption methods are described in the following table.

Data Encryption Methods	
Type	**Description**
End-to-end encryption	In end-to-end encryption, two users of a distributed network each apply encryption devices at their terminal locations and agree on the classified key. End-to-end encryption provides the greatest degree of protection since the information fully encodes all the way through the network to the users' own end terminals. However, end-to-end encryption is the most difficult to implement. In order to ensure proper operation of the decoding process at the receiving end, the decryption mechanism synchronizes with the encryption mechanism. There are a number of ways to do this, but each is rendered less effective by the presence of variable delays. In addition, if the network uses switching, there must be a method for transmitting the address and signaling information in the clear, so that the network switches and control facilities can understand the overhead information.
Link encryption	Link encryption applies to each end of a communications line such as the link between two switches in a distributed network. It ensures that all information flowing on the communications line is unintelligible to an unauthorized intruder. Even the overhead, address and control information is protected. This offers traffic flow security as well as information security. *Traffic flow security* means that an observer does not know if or when information transmits on the communication line. The *major disadvantage* of link encryption is that the information has to be decoded at each nodal element of the network, thus the information is intelligible to an intruder who might penetrate the switching or processing elements of the network. Link encryption also requires more encryption devices in a typical network since the lines between the switches and nodes as well as the lines between the users and the network require individual encryption. However, in truly distributed networks and networks based on broadcasting techniques, the distinction between link and end-to-end encryption minimizes since, for the most part, the traffic moves directly between the source and destination users.
Bulk encryption	In bulk encryption, a single encryption device encrypts the information on several channels simultaneously. A typical arrangement uses a multiplexer to combine several channels into a single channel for encryption.

Data Encryption Methods	
Type	**Description**
	We typically apply bulk encryption to a trunk exiting and entering a site or base.
IP encryption	IP encryption is a type of digital encryption that enables flexible use of voice, video, and data communications while providing a secure link between users over IP based networks. IP encryptors use the TCP/IP worldwide standard to route data anywhere anytime to any user who is located on an IP based network. All users must have matching keys. Whereas end-to-end, link, and bulk encryptions use dedicated circuitry to connect directly to each other, IP encryptors use TCP/IP routing standards to link to any user. An example of an IP encryptor is a KG–175D (TACLANE)
Voice encryption	Voice encryption telephones operate reliably, with high voice quality, as both ordinary telephones and secure instruments over the dial-up public switch telephone network. The Secure Terminal Equipment (STE) is the most commonly used secure voice telephone. The Secure Terminal Equipment (STE) is the successor to the STU-III. The STE cryptographic engine is on a separately provided removable PCMCIA card. The STE data terminal provides a reliable, secure, high-rate digital data modem for applications where only data transfer (FAX, PC files, video teleconferencing, etc.) is required. All STE products are STU-III secure mode compatible with the following enhanced capabilities: • Voice-recognition quality secure voice communication. • High-speed secure data transfers (up to 38.4 Kbps for asynchronous or 128Kbps for synchronous).

Fill devices store and load cryptographic keying material. You have to have a way to initiate the use of a coding system. There are many different fill devices available to you as a technician. The keys that are stored on this type of device are either electronically loaded or manually loaded from Mylar tape using a general-purpose tape reader. With modern technology, we have advanced to where one small device can handle hundreds of keys for transfer into our encryption devices. The most commonly used fill device is the Simple Key Loader (SKL). This device holds multiple keys using multiple different formats. The SKL has taken, or is taking the place of, many legacy fill devices you may still have in your work center, such as the KOI–18, KYK–13, AN/CYZ–10 Digital Transfer Device (DTD), and so forth.

NOTE: The fill device assumes the classification of the highest-level key loaded as soon as it is loaded.

Additional Information:

Information Assurance Support Environment (IASE) hosts an online training catalog specializing in the following areas:

Cybersecurity Awareness, Cybersecurity for Senior Leaders, Cybersecurity for Professionals, Cybersecurity Technical, Cyber Law, Cybersecurity Simulations.