

3A ENCRYPTOR

DESCRIPTION, INSTALLATION, OPERATION, AND MAINTENANCE

CONTENTS	PAGE
1. GENERAL	5
2. PHYSICAL DESCRIPTION	6
A. 3A Encryptor Bay	6
B. 3A Encryptor	6
C. Fan Shelf	8
3. 3A ENCRYPTOR CIRCUIT DESCRIPTION	9
A. DS3 Signal Processing	9
B. Key-Stream Generation	10
C. System Control and Alarming	12
D. Modes of Operation	12
E. TEST Mode	13
F. Control Channel Options	13
G. Remote Command Options	14
4. BAY INSTALLATION	15
A. Tools	15
B. Handling and Uncrating	15
C. Anchoring Requirements	15
D. Installing Anchors	16
E. Erecting the Bay	18
F. External Connections	19
5. 3A ENCRYPTOR INSTALLATION	21
A. Equipment Required	21
B. Unpack Shelves	21
C. Install Equipment Shelves	21
D. Install Customer-Provided Components	22
E. Select Control Channel Option	24
F. Make External Connections to the Shelves	26

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

6.	3A ENCRYPTOR RELIABILITY ACCEPTANCE CRITERIA	28
7.	VERIFY 3A ENCRYPTOR OPERATION	30
	A. Required Test Equipment	30
	B. Power-Up, Loopback, and Mode Tests	30
8.	PLACING THE 3A ENCRYPTOR IN SERVICE	37
	A. Required Test Equipment	37
	B. Verify Terminal Operation	37
9.	OPERATION	40
	A. Modes of Operation	40
	B. Loading Key Material	40
	C. Loading Key Material (Maintenance Key Reloading)	40
	D. Loading Key Material (Loading New Keying Material)	41
	E. Patching the DS3 Signal From a Regular Terminal to a Hot-Standby Terminal	43
	F. Patching the DS3 Signal From a Hot-Standby Terminal to a Regular Terminal	44
	G. Replacing Memory Backup Battery	44
	H. Verify Fan Operation	45
	I. Perform LED Test	45
10.	MAINTENANCE	46
	A. Circuit Pack Handling	46
	B. Power Unit Operation	46
	C. General Troubleshooting Information	46
	D. Loopback Test	48
	E. Overall Transmission Test	48
	F. Fuse Assignments	49
11.	MAINTENANCE VERIFICATION OF 3A ENCRYPTOR OPERATION.	50
	A. Required Test Equipment	50
	B. Power Alarm Tests	50
	C. Operational Tests	53
	D. Bypass Switch Operation	53

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

E.	Verify Remote Bypass and Remote Reset	54
F.	Patch Panel Verification	55
G.	Loopback Test	56
12.	3A ENCRYPTOR ALARM TESTING PROCEDURE	57
A.	Required Test Equipment	57
B.	Verify Remote Bypass and Remote Reset - Local Test	63
13.	3A ENCRYPTOR - SPECIAL BACK-TO-BACK VERIFICATION TESTING OF A FAILED TERMINAL	65
A.	Required Test Equipment	65
B.	Verify Terminal Operation	65
14.	IN-SERVICE ENCRYPTION TEST PROCEDURE	67
A.	Required Test Equipment	67
B.	Verify Terminal Operation	67
15.	ALARM VERIFICATION TEST PROCEDURES	71
A.	Required Test Equipment	71
B.	Alarm Verification Test Procedures	71

LIST OF TABLES

TABLE A -	3A Encryptor Input and Output Signal Specifications	77
TABLE B -	3A Encryptor Front Panel Indications and Controls	78
TABLE C -	3A Encryptor Circuit Pack Functions	80
TABLE D -	3A Encryptor Fan Shelf Indications and Controls	82
TABLE E -	3A Encryptor Equipment Designations	83
TABLE F -	Control Channel Option Switch Settings	84
TABLE G -	Select DS3 Control Bit	85
TABLE H -	Select Customer Data Bit	88

AT&T-PROPRIETARY (RESTRICTED)
 Solely for authorized persons having a need to know
 pursuant to Company Instructions

LIST OF FIGURES

Fig. 1 - 3A ENCRYPTOR BAY	91
Fig. 2 - 3A ENCRYPTOR TERMINAL	92
Fig. 3 - LEFT SIDE OF A REGULAR 3A ENCRYPTOR HOUSING SHOWING THE DS3 INPUT AND OUTPUT CONNECTORS	93
Fig. 4 - RIGHT SIDE OF A REGULAR 3A ENCRYPTOR HOUSING	94
Fig. 5 - 3A ENCRYPTOR WITH FRONT DOOR OPEN	95
Fig. 6 - 3A ENCRYPTOR FAN SHELF	96
Fig. 7 - 3A ENCRYPTOR BLOCK DIAGRAM	97
Fig. 8 - 3A ENCRYPTOR BAY FOOTPRINT	98
Fig. 9 - FRAME GROUND CONNECTION	99
Fig. 10 - 3A ENCRYPTOR BAY DISTRIBUTION PANEL	100
Fig. 11 - INSTALLING MEDECO CAM LOCKS	101
Fig. 12 - INSTALLING MEDECO KEYLOCK SWITCH	102
Fig. 13 - END VIEW OF KEYLOCK SWITCH SHOWING WIRING CONFIGURATION	103
Fig. 14 - LOCATION OF CONTROL CHANNEL SWITCHES	104
Fig. 15 - DS3 SIGNAL FRAME	105
Fig. 16 - 3A ENCRYPTOR FUSE ASSIGNMENTS	106
Fig. 17 - DSX-3 PATCHING ARRANGEMENT - TERMINAL CONNECTED BACK-TO-BACK	107
Fig. 18 - TERMINAL TEST CONFIGURATION - TWO TERMINALS CONNECTED END-TO-END	108
Fig. 19 - HOT-STANDBY PATCHING PROCEDURE	109
Fig. 20 - LOCATION OF JACKS J1 THROUGH J4	110
Fig. 21 - IN-SERVICE TEST CIRCUIT	111
Fig. 22 - HOT-STANDBY TERMINAL - ALARM VERIFICATION TEST CONFIGURATION	112
SCHEMATIC DRAWINGS	113
SD 7C474-01 - 3A Encryptor - Top Panel Circuit	
SD 7C475-01 - 3A Encryptor - Bottom Panel Circuit	
SD 7C476-01 - 3A Encryptor - Main Housing	
SD 7C478-01 - 3A Encryptor - Fan Shelf Circuit	
SD-7C479-01 - 3A Encryptor - Bay Application Schematic	

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

1. GENERAL

- 1.01** This manual describes the AT&T 3A Encryptor and provides installation, operation, and maintenance information. The 3A Encryptor is a bi-directional digital data encryption/decryption unit that operates at the DS3 data rate of 44.736 Mb/s. This unit has been designed in accordance with the interconnection specifications in AT&T Technical Advisory No. 34 and is compatible with all transmission facilities operating at the DS3 level of the North American digital hierarchy. Table A lists the 3A Encryptor input and output signal specifications.
- 1.02** This manual has been completely reissued to provide updated information regarding initial turn-up procedures as well as the addition of new tests between the 3A Encryptor and the local and remote alarm systems. Additional Sections have been added to include detailed procedures to perform back-to-back out-of-service performance tests, to generate and verify each 3A Encryptor alarm or status indication, and to perform in-service encryption verification tests. Since extensive revisions have been made, change arrows have not been used to indicate the paragraphs which have been changed.
- 1.03** The 3A Encryptor product line consists of a 7-foot world class bay, the Regular 3A Encryptor, and a Hot-Standby 3A Encryptor which is used to provide backup service for up to 11 Regular 3A Encryptors. The 3A Encryptor has been designed around the concept that transmission of the DS3 signal is to be maintained during an encryption failure. Consequently, the 3A Encryptor will automatically route the DS3 signal around the encryption circuitry if the unit's self-checking feature detects a failure condition.
- 1.04** The 3A Encryptor can be ordered with the standard -24 volt dc powering plan or with an optional -48 volt dc powering plan.
- 1.05** The 3A Encryptors use U.S. Government approved encryption algorithms to ensure communications protection and ease of practical implementation.

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

2. PHYSICAL DESCRIPTION

A. 3A Encryptor Bay

- 2.01 The 3A Encryptor Bay (Figure 1) is a 7-foot tall world class bay and holds up to four 3A Encryptors and their associated fan shelves. The bay is approximately 84 inches high, 26 inches wide, and 10.2 inches deep and weighs approximately 375 pounds when fully equipped.
- 2.02 The encryptor bay is prewired to provide external power and circuit connections to the shelves. All power and alarm connections to the bay are made to terminal blocks which are mounted on the distribution panel. The distribution panel is located at the top of the bay. From the distribution panel, connectorized power and alarm cables are routed down the right side of the bay to the appropriate shelf positions.
- 2.03 All external connections to the bay are made to the terminal blocks at the top of the bay with the exception of the DS3 input and output signal connections which are made directly from the DSX-3 Cross-Connect Panel to the appropriate 3A Encryptor.

B. 3A Encryptor

- 2.04 The 3A Encryptor shelves consist of 14 circuit packs mounted in a steel housing with lockable front and rear doors. The encryptors are approximately 14 inches high, 19.5 inches wide, and 10.2 inches deep and weigh approximately 60 pounds. Mounting brackets are included which are attached during installation. The brackets are secured from inside the encryptor housing so that, once installed, the terminal cannot be removed from the bay without generating a local and remote alarm.
- 2.05 Two 3A Encryptor models, a Regular and a Hot-Standby, are normally provided in a typical installation. The difference between the two models is that the Regular terminal is equipped with four connectors on the left side of the housing. These connectors are used to connect the input and output DS3 signals from the 3A Terminal to the DSX-3 Cross-Connect Panel. The Hot-Standby terminal input and output signal connections are made using patch-cord connections between a Patch Panel, located on the front of the Hot-Standby terminal, and a similar Patch Panel located on the front of a Regular terminal. The front panel of the 3A Encryptor is shown in Figure 2 while the DS3 input and output connectors on the left side of a Regular terminal are shown in Figure 3. The front panel indications and controls for the 3A Encryptor are described in Table B.
- 2.06 Figure 4 shows the right side of the 3A Encryptor housing where the connectors for the power, alarm (local and remote), and status indications (remote) are located. A cable is provided with the bay cabling for interconnecting the encryptor shelf power and the fan shelf power. A battery holder is also mounted on the right side of the encryptor housing to hold the memory backup battery, used to retain the encryptor keying material in the event of a power interruption.
- 2.07 The 3A Encryptor housing contains a circuit pack shelf assembly which is accessible by opening the front door of the encryptor. The shelf assembly configuration, containing 14 plug-in units, is shown in Figure 5. The rear door provides access to

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

the rear of the unit and its backplane. The circuit packs for all encryptor versions are identical with the exception of the Bypass Switch plug-in unit and the two Power Units. These three units are dependent on the power option selected. The circuit packs for each powering option are listed in Table C.

- 2.08** The circuit pack designations are stamped on the circuit pack levers and are also printed on the bottom rail of the mounting frame. The only circuit packs with faceplates are the RIU (Remote Interface Unit) and the two Power Units. The RIU faceplate has two pushbutton switches (designated LOOP TEST and TEST) which are used to activate an internal loopback connection and out-of-service test procedure for testing the operation of a terminal. The red ON LED (light-emitting diode) lights when the loopback connection has been activated by pressing the LOOP TEST pushbutton switch. Pressing the TEST pushbutton switch activates the automatic test procedure and at the conclusion of the test either the green PASS or red FAIL LED will turn ON to indicate the test results.
- 2.09** The LOOP TEST and TEST switches are pushbutton switches where the center section of the switch is recessed and pressed, with a blunt non-conducting probe, to activate the loopback connection and loopback test, respectively.
- 2.10** Each circuit pack has a red alarm LED mounted on the front edge of the printed circuit board or on the faceplate of the unit. This LED is labeled HDWR FAIL on the RIU circuit pack and ALM/OFF on the two Power Units. On the circuit packs without faceplates, the alarm LEDs are not labeled but can be recognized by their red color. These alarm LEDs are controlled by the self-checking circuitry of the 3A Encryptor and will light when the unit detects a faulty circuit pack. The HARDWARE FAILURE alarm LED, located on the front panel of the 3A Encryptor, will also turn ON.
- 2.11** The ALM/OFF LED alarm on the two Power Units is controlled by the internal circuitry of the two circuit packs and will light when a problem is detected or when the Power Unit is turned OFF. The Power Units can be turned OFF by releasing the retaining clip, located on the circuit pack lever, and allowing the lever to fall forward. Miniature pin jacks on the faceplate of the Power Units are used to measure the circuit pack's input and output voltages.
- 2.12** The Bypass Switch circuit pack is unique among the 3A Encryptor plug-in units since it is powered directly from the secondary power source rather than by the Power Units which provide power to each of the circuit packs within the terminal. This allows the terminal to operate in the BYPASS mode and uses the Bypass Switch plug-in unit to pass the DS3 signal around the encryption circuitry in the event of a failure of the primary power source. A green LED is mounted on the BYP SW plug-in unit and is always lighted as a reminder that power is applied to the unit when the power to the encryption circuit packs has been turned OFF.
- 2.13** A 247-type Key Insertion Device (KID) is used to load keying material into the 3A Encryptor through the KEY LOADER connector, located on the bottom panel of the encryptor. The 247A KID is a metal unit approximately 3 inches by 5 inches by 1 inch with a 25-pin jack. The jack is inserted into the KEY LOADER connector plug, located on the Bottom Panel of the 3A Encryptor, whenever keying material is to be loaded into the terminal.

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

C. Fan Shelf

- 2.14 A fan shelf is required for each 3A Encryptor shelf and is approximately 5 inches high, 19.5 inches wide, 10.2 inches deep, and weighs approximately 10 pounds. Each fan shelf is equipped with two fans mounted on the front, two connectors on the right side, and alarm LEDs and an ACO (alarm cutoff) switch on the left front (Figure 6). The two fans are designed to pull air through the 3A Encryptor and exhaust it out through the front of the fan shelf. Connector P1, located on the right side of the shelf, is connected to the bay power cable, while the encryptor power cable, also provided with the bay cabling, connects to connector P2 and provides power to the 3A Encryptor shelf and also furnishes the alarm connections to the fan shelf.
- 2.15 Three fuses, mounted on a bracket on the right side of the fan shelf, are located behind the hinged front cover of the shelf as shown in Figure 6. The top fuse (F3) protects the power alarm circuit, the middle fuse (F1) protects FAN-A, and the lower fuse (F2) provides protection for FAN-B. The fuses and alarm LEDs are described in Table D.

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

3. 3A ENCRYPTOR CIRCUIT DESCRIPTION

3.01 The 3A Encryptor is a bi-directional terminal that encrypts a DS3 plain-text signal in the transmitting direction of transmission and decrypts an encrypted DS3 signal in the receiving direction of transmission. Functionally, the 3A Encryptor can be divided into three operations: DS3 signal processing, key stream generation, and system control and alarming. Figure 7 is a block diagram showing the functional relationship between the circuit packs used in the 3A Encryptor.

A. DS3 Signal Processing

- 3.02** Since the 3A Encryptor is a bi-directional terminal, encryption and decryption operations are occurring simultaneously for the DS3 signals in each direction of transmission. For convenience, the encryption process will be discussed first, followed by the decryption process. While the encryptor and decryptor share some common circuitry, the encryption and decryption processes are completely independent operations. In addition, the encryption circuitry provides information to control the operation of the far-end decryption process by sending essential information to the receiving terminal via a special control channel used by the 3A Encryptor.
- 3.03** The Line Interface Unit (LIU) checks for the presence of a standard DS3 input signal with B3ZS (binary 3 zeroes substitution) line coding. The LIU decodes the B3ZS line format and sends the signal to the Reframer Unit (RFU). If an input signal is not present, a LOSS OF INPUT alarm is sent to the system controller circuitry. The LIU also checks the input signal for the presence of a BLUE signal and notifies the system controller if a BLUE signal is present. (A BLUE signal is a standard network trouble-indicating signal consisting of a framed DS3 signal of alternating ones and zeroes.)
- 3.04** The RFU encrypts the incoming signal by adding an internally generated encryption key stream to the plain-text DS3 signal. In this process the DS3 framing and control information, as well as the customer's data bits, are also encrypted. To restore the framing and control information, the unencrypted DS3 signal is routed to a multiplexer which locates the framing and control bits and overwrites those bits with the original framing and control bit information.
- 3.05** To verify proper synchronization at both ends of the system, the encrypted framing bit is inserted in the control channel and transmitted to the far-end terminal where it is compared to the framing bit in the incoming DS3 signal. If the two terminals are properly synchronized, the two framing bits will be identical. If the bits are not identical, a synchronization alarm will be generated and a resynchronization procedure will be initiated.
- 3.06** To ensure that the transmitter output is an encrypted signal, the incoming plain-text DS3 signal is compared to the output of the multiplexer which should be an encrypted signal. If the two signals are identical, an internal plain-text output indication will be generated, and the terminal will automatically switch to either the CLEAR or BYPASS mode of operation. The switching of the terminal to either operating mode will generate a local and a remote alarm.

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

- 3.07 The multiplexer is also used to provide the CLEAR mode of operation. The CLEAR operating mode consists of the unencrypted DS3 signal plus the control channel data. The same process used to restore the original framing bits is also used to provide the original unencrypted signal at the multiplexer output.
- 3.08 The signal at the output of the RFU is reapplied to the LIU. As a result of the encryption process and the addition of the control channel data, the DS3 signal parity will change. The LIU recalculates the parity of the signal and inserts the new value of the parity bits into the DS3 signal. The LIU also restores the B3ZS line format and applies the signal to the Line Driver Unit (LDU) to be amplified and sent to the network facility.
- 3.09 Decrypting the received encrypted DS3 signal is essentially the same process which was used to encrypt the original signal. The received signal is applied to the LIU, and the B3ZS line format is decoded. The signal is routed to the RFU where the control channel information is recovered and used by the receiving 3A Encryptor. An encryption key stream, identical to the one used to encrypt the DS3 signal, is added to the received signal. The addition of the encryption key stream and the received encrypted signal results in unencrypted customer data bits and encrypted framing and control bits. As in the encryption process, the signal is then applied to a multiplexer where the unencrypted framing and control bits are restored to the DS3 signal. The signal is reapplied to the LIU where new parity bits are generated and the B3ZS line format is restored. Finally, the signal is sent to the LDU where it is amplified and transmitted to the network facility.
- 3.10 The bypass circuitry is contained on the Bypass Switch (BYP SW) circuit pack. The bypass path is a through path that routes the DS3 signal from the input of the terminal, around the encryption circuitry, to the output of the terminal. The bypass path provides a protection path so that if a problem is detected in the encryption transmission path, the applied DS3 signal will be switched automatically (a BYPASS ON alarm will also be generated) to the bypass path to maintain DS3 signal continuity over the transmission facility. To ensure that the bypass path is operational, the Bypass Switch circuitry continually monitors the bypass transmission path. If a failure is detected, a BYPASS FAILURE alarm will be generated. The BYPASS operating mode can also be selected manually.
- 3.11 Problems detected in encryptor operation generally result in a switch to the CLEAR operating mode. The CLEAR operating mode is an unencrypted DS3 signal which contains the control channel information. The presence of the control channel allows encryption to be resumed when the problem has been resolved. The synchronization test, described in paragraph 3.05, is performed before encryption is resumed to ensure that the encryption and decryption circuitry are properly synchronized.

B. Key-Stream Generation

- 3.12 Each 3A Encryptor generates two completely independent 44.736-Mb/s key streams. The plain-text DS3 signal is encrypted by adding it to an encryption key stream signal. To decrypt the encrypted signal, an identical encryption key stream is added to the signal a second time. To provide a decryption key stream identical to the

**AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions**

encryption key stream, the encryption circuitry controls the generation of the decryption key stream by sending information to the receiving terminal over the control channel. Consequently, each 3A Encryptor must generate an encryption key stream to encrypt the transmitted signal and send the necessary control information to the far-end terminal so that it is capable of generating an identical key stream to decrypt the received encrypted signal.

- 3.13 The encryption key stream generation process begins with a request by the Session Key Generator (SKG) circuit pack for the Random Number Generator (RNG) to generate a set of initialization vectors. The SKG uses the initialization vectors to program the Pseudo-Random Data Generator (PRDG) and to generate session keys which are used to produce the encryption key stream. The initialization vectors are also transmitted to the far-end 3A Encryptor where they are used to program the receiving PRDG so that an identical set of session keys can be used to generate the decryption key stream.
- 3.14 When the terminals at both ends of the system are ready, the PRDGs are started synchronously with the DS3 signal. The output of the PRDG is used as the input to the encryption and decryption key stream generators. Since the generators operate on different session keys, each generator will provide a dissimilar pseudo-random data stream which results in the generation of a different key stream output.
- 3.15 The processes for producing the encryption and decryption key streams in a terminal are identical except for the source of the initialization vectors. Initialization vectors for the encryption key stream are obtained from the RNG, while the vectors for the decryption key stream are supplied over the control channel from the far-end transmitting terminal.
- 3.16 The Synchronization Channel Controller (SCC) oversees the operation of the control channel. During the handshaking required to synchronize the two 3A Encryptors, the SCC automatically places the encryptors in the CLEAR operating mode. During the synchronization process, the SCC compares the encrypted framing bit from the transmitting terminal with the encrypted framing bit at the receiving terminal. If the framing bits match, the units are considered synchronized and encryption/decryption of the DS3 signal will begin.
- 3.17 During the normal operation of the 3A Encryptor, the SCC continually compares the framing bits at both ends of the system. If a loss of synchronization is detected, the terminal will switch to the CLEAR operating mode and a new synchronization cycle will start. If the SCC is unable to reestablish synchronization, the appropriate alarms will be generated, the terminal will remain in the CLEAR mode, and the SCC will continue to attempt to resynchronize the two terminals.
- 3.18 Once encryption/decryption of the DS3 signal has been started, the SKG will begin a continual process of checking the operation of the PRDGs and the key stream generators. The SKG also performs diagnostic tests on the PRDG, the RNG, its own circuitry, and the alarm circuits.

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

C. System Control and Alarming

- 3.19 The System Control Unit (SCU) monitors the operation of the signal processing and key stream generating sections of the terminal. If a problem is detected, the SCU issues the commands to protect the DS3 signal and the keying material. The SCU will continue to monitor the terminal operation so that, if possible, the terminal can be returned to normal operation. The SCU also monitors the switches on the front of the terminal and controls the operation of the alarm and status indications. Under the direction of the SCU, the RIU controls the actual control, status, and alarm signals applied to and leaving the 3A Encryptor.

D. Modes of Operation

- 3.20 The 3A Encryptor has three operating modes: NORMAL, CLEAR, and BYPASS. A 3-position MODE SELECT switch allows each of these modes to be selected manually.
- 3.21 The NORMAL operating mode provides the encryption and decryption process of the terminal. The NORMAL mode is manually selected by placing the MODE SELECT switch in the NORMAL position. The control channel is present in the DS3 signal when the 3A Encryptor is operating in the NORMAL mode.
- 3.22 The CLEAR operating mode of the 3A Encryptor provides an unencrypted DS3 signal as well as control channel information. The CLEAR mode is manually selected by placing the MODE SELECT switch in the CLEAR position. The CLEAR mode is automatically selected during the resynchronization process. Whenever the receiving 3A Encryptor detects that the far-end terminal is in the BYPASS operating mode, the near-end terminal will automatically switch to the CLEAR operating mode until the far-end terminal is once again capable of processing the DS3 signal. The control channel is present in the DS3 signal when the 3A Encryptor is operating in the CLEAR mode.
- 3.23 The BYPASS operating mode provides a DS3 signal protection path and is automatically selected if the terminal's self-check routines detect problems in the encryption signal path. The BYPASS mode routes the incoming DS3 signal around the encryption/decryption circuitry and places the unencrypted signal on the network facility. When the terminal at either end of the system is operating in the BYPASS mode, the terminal at the far-end detects the absence of a control channel and automatically switches to the CLEAR operating mode. When the control channel is restored, and no other operational problems exist, both terminals will automatically return to the NORMAL operating mode. The BYPASS mode can be manually selected by operating the MODE SELECT switch to the BYPASS position. The control channel is not present in the transmitted DS3 signal when the 3A Encryptor is operating in the BYPASS mode.
- 3.24 The CLEAR operating mode should be manually selected whenever the DS3 signal is to be patched from a Regular terminal to a Hot-Standby terminal. Using the CLEAR mode minimizes the number of hits to the DS3 signal during the patching process. No transmission hits to the DS3 signal occur when the terminal is operated between the CLEAR and NORMAL operating modes.

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

E. TEST Mode

- 3.25** In addition to the three regular operating modes, the 3A Encryptor also has a TEST mode. The TEST mode can only be manually selected by opening the front door of the terminal and pressing the LOOP TEST pushbutton switch, located on the faceplate of the RIU. This operation activates an internal loopback connection between the encryptor output and the decryptor input and also lights the red ON LED. Pressing the TEST pushbutton switch initiates an internal test sequence to verify the operation of the terminal by encrypting a known DS3 signal using fixed session keys, then decrypting the signal and checking the results. When the test is completed, either the green PASS or red FAIL LED, located on the faceplate of the RIU, will light to indicate the test results.
- 3.26** Opening the front door of the 3A Encryptor to operate the TEST mode will cause the customer's signal to switch to the bypass path and will zeroize the keying material and session keys. The encryptor will exit the test mode when the front door is closed. To return to normal operation, close and secure the front door and reload keying material. Normal operation will be resumed after the unit is initialized and synchronized.

F. Control Channel Options

- 3.27** The DS3 signal is composed of a data frame which is divided into seven subframes. Each subframe is divided into eight blocks, each block containing a DS3 control bit and 84 customer data bits. To form the control channel, used by the 3A Encryptor, it is necessary to use at least 1 bit in each DS3 frame.
- 3.28** The following control channel options are listed in their order of preference. The first three options, X-data bit, stuffing bit, and limited stuffing, are recommended because they utilize otherwise unused bits for use as the control channel. The framing bit and fixed data bit options are not recommended if one of the first three options can be used. The framing bit and fixed data bit options share bits being used for another function to form the control channel. Using the framing bit or fixed data bit control channel options will result in the generation of errors in the customers data or in the DS3 framing bits.
- 3.29** X-DATA BIT CONTROL CHANNEL: Included in the DS3 control data is a 9-kb/s maintenance control channel. In normal operation, only a small portion of the 9-kb/s capacity is used (1 bit per second). This option utilizes the normally unused capacity to form a control channel of approximately 8999-kb/s which has a minimal effect on the DS3 control data and no effect on customer data.
- 3.30** STUFFING BIT CONTROL CHANNEL: This option locates the control channel in the stuffing bits used to "fill-in-the-blanks" when the DS3 signal was formed. Locating the control channel in the stuffing bits has the advantages of providing a high data-rate control channel (from 20- to 40-kb/s) and not affecting the customer data or the DS3 control data. A high data-rate control channel allows quicker encryptor response because less time is required to communicate between the two terminals.

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

- 3.31 LIMITED STUFFING BIT CONTROL CHANNEL:** This option overwrites the stuffing bit of a specific subframe rather than using stuffing bits in every subframe and is useful when encrypting video signals. This limits the data rate of the control channel to one-seventh that of the regular stuffing bit control channel. This is the lowest data rate of the control channel options, but it has the advantage of not affecting customer data or the DS3 control data.
- 3.32 FRAMING BIT CONTROL CHANNEL:** This option uses 1 framing bit from each DS3 master frame to form a 9-kb/s control channel. This option also has no affect on customer data but does alter the network framing data. There should be little affect on the network due to the redundancy built into the DS3 signal. Some non-AT&T multiplex terminal equipment may be susceptible to framing bit errors should this option be selected.
- 3.33 FIXED DATA BIT CONTROL CHANNEL:** This option establishes a 9-kb/s control channel by overwriting 1 bit in each DS3 master frame. This option affects customer data and will result in a 50-percent error rate in the customer data bit selected for the control channel.

G. Remote Command Options

- 3.34** Two remote command options are available on the 3A Encryptor: A remote bypass option and a remote reset option. The remote bypass option recognizes a contact closure on the remote bypass leads as a command to operate the terminal to the BYPASS operating mode. The unit will remain in the BYPASS mode until a remote reset command is sent or if the terminal is manually reset by pressing the RESET/LAMP TEST pushbutton swith on the front of the 3A Terminal at either end of the facility. The remote reset option recognizes a momentary closure on the remote reset leads as a command to reset the terminal. A remote reset command has the same effect as pressing the RESET/LAMP TEST pushbutton switch on the front of the terminal as described in Table B. The remote option leads are factory-wired to the terminal strips at the top of the bay as shown in Bay Application Schematic, SD-7C479-01.

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

4. BAY INSTALLATION

A. Tools

4.01 The following tools are required to install the 3A Encryptor Bay:

QUANTITY	CODE	DESCRIPTION
1	Tool Kit 33	Vacuum
1	Tool Kit 76B	Drilling Hammer
1	R-3055	Safety Goggles
1	R-4875	Compression Tool

B. Handling and Uncrating

Warning 1: Do not stack the bays more than two high during shipping or storage.

Warning 2: The shipping container is designed to lay lengthwise on the floor and is so marked. Do not ship or store containers in a standing position.

4.02 When removing containers from the shipping van, place on a dolly truck in a horizontal shipping position. Verify that the container has not been damaged. Handle all containers with care and take precautions not to drop the unit.

4.03 Uncrate all material in quarters separate from the equipment room to minimize dust, lint, and other undesirable particles which could create maintenance problems to other equipment.

4.04 All bays are shipped in a dust-protection, antistatic, plastic bag and placed in a wooden container. The bay is laid in the container with the front or equipment side facing up and should be uncrated in its horizontal shipping position.

4.05 A pinch bar and a claw hammer are required to uncrate the bay and must be used with care to avoid damaging the bay. Using the pinch bar or claw hammer in nailed areas, remove the top cover of the container; then, remove the container side and end plates. Next, remove the plastic bag and all foreign material. The bay may be left on the container bottom until brought to the bay location for mounting.

C. Anchoring Requirements

4.06 The number of bolts required to anchor the bay is determined as follows:

- (1) Isolated bay • 4 bolts
- (2) Multi-bay lineup • 2 bolts per bay

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

- (3) Hardened site • 4 bolts per bay
- (4) Earthquake area • 4 bolts per bay
- 4.07 Two types of anchors are used on concrete floors, self-drilling anchors or Loxin expansion shields. Self-drilling anchors are used in most cases.
- 4.08 Self-drilling anchors come in two sizes, 1-1/2 inches in diameter with a 3/8-16 size bolt, and 2 inches in diameter with a 1/2-13 size bolt. Refer to the job order for the specific size to use.
- 4.09 When using the Loxin-type anchor, a 5/8-inch diameter hole is required. The depth of the hole is determined by the length of the anchor, which is either 1-1/2 or 2 inches. Associated with the anchor is a 3/8-16 size bolt.

Note: In all drilling operations, the Tool Kit 33 vacuum cleaner must be used.

- 4.10 When drilling in an office with DR-90 equipment in service on the same floor, mounting holes shall be drilled for the 3/8-16 by 1-1/2 inch Loxin expansion shield. Drill holes using a 1/2-inch electric drill with a 5/8-inch diameter carbide-tipped worm-fluted drill bit.

Note: When using worm-fluted drills, it is necessary to drill a centering hole or make a slight impression in the surface to be drilled to prevent the worm-fluted drill from "walking". Use a standard straight or spiral-fluted drill bit for this purpose.

- 4.11 When mounting the bay on a wooden floor, drill a pilot hole to accept a 3/8-16 lag bolt, or equivalent.

D. Installing Anchors

Drilling

- 4.12 Refer to the job floor plan for bay location and lay out the floor using a marking pencil or a felt pen. The bay footprint is shown in Figure 8. A 1/16-inch clearance must be left when mounting bays side by side.
- 4.13 The technique for drilling holes with self-drilling anchors is different than using carbide bits. With the carbide bit, the more pressure exerted on the tool the faster the hole will be drilled. The secret of drilling holes with self-drilling anchors is not to apply excessive pressure (i.e., do not lean on the tool, but simply let the weight of the tool do the work). Apply only enough pressure to control the tool.
- 4.14 All roto-stop hammers combine simultaneous rotation and hammering action. If excessive pressure is applied on the roto-stop hammer, the hammering action is negated. Also, the self-drilling anchor teeth will have a tendency to burn or break. This is often encountered where the concrete hardness is in excess of 4000 psi.
- 4.15 A self-drilling anchor should be used to drill only one hole.

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

4.16 To install self-drilling anchors using the R-9430 roto-stop hammer:

- (1) Select the proper chuck head and seat it on the shank.
- (2) Position and lock the chuck/shank assembly in the hammer.
- (3) Insert and seat the anchor in the chuck.
- (4) Operate the hammer without rotation to embed the teeth and position the anchor.
- (5) Flip the roto-stop control lever to engage rotation and drill until the chuck is 1/16 inch from the concrete.

Caution: Always hold the auxiliary handle when rotation is engaged. Let the tool do the work. Apply only enough pressure to control the tool and to keep it from climbing on the shank.

- (6) Stop the tool and lift up approximately 1 inch to disengage impact; then, start the tool and withdraw the anchor.
- (7) Disengage rotation and, holding the anchor, start the tool to expel the concrete cuttings.
- (8) Use the vacuum to clean cuttings from the hole in the concrete.
- (9) Insert and lightly seat the expansion plug in the anchor.
- (10) Insert the anchor in the hole and set with the impact of the tool until the chuck is 1/16 inch from the concrete.

Note: Larger size anchors may require hand setting with a flush holder and a 2- to 3-pound hammer to obtain a flush installation.

- (11) Break off the chucking cone.
- (12) Remove the cone from the chuck with the ejector key.

Removing Stuck Anchors

4.17 Self-drilling anchors have a tendency to get stuck in the floor when the roto-stop hammer is lifted. The two main reasons self-drilling anchors get stuck are: a new chuck head causes slippage, or the anchor was not perpendicular to the floor when drilling was started.

Note: If the chuck head is new, moisten the tapered portion of the self-drilling anchor and apply concrete dust to it.

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

- 4.18 To remove a stuck anchor, set the roto-stop hammer on the stuck anchor and continue drilling for a short period of time to seat the roto-stop hammer on the anchor. Then, stop the tool and lift the anchor approximately 1/2 inch. While holding the roto-stop hammer in the lifted position, restart the tool and continue lifting until the anchor is removed from the floor.

Note: When the roto-stop hammer is lifted approximately 1/2 inch, the shank is not exposed to the hammering action.

- 4.19 An alternate method is to grip the anchor with a pair of groove-joint pliers and turn back and forth while pulling up on the anchor.
- 4.20 If the anchor breaks and the broken part is below the floor line, use a new anchor and drill in an alternate location.
- 4.21 When hard aggregate is encountered, it is recommended that the roto-stop hammer be stopped, switched to hammering only, and be operated for a short period of time. The hammering action of the tool will shatter the aggregate surface and allow continued drilling. It may be necessary to repeat this procedure several times depending on the aggregate.
- 4.22 To install the self-drilling anchor, remove the anchor and clean out the hole with the vacuum. Place the red plug into the anchor, reinsert the anchor into the hole, and expand until flush. Snap off the cone.

Check Anchor Seating

- 4.23 Using the R-4416A tool will normally ensure a properly expanded anchor; the results obtained when using other methods may not be as certain. If there is any question whether the anchor has been properly expanded, test it as described in the following paragraph.
- 4.24 Place a bushing or several washers with holes larger than the diameter of the shield or anchor over the anchor and insert a screw or a bolt (or a stud with a nut attached) into the anchor. Tighten the screw, nut, or bolt with a suitable wrench or screwdriver. If the anchor can be easily withdrawn from the hole as the parts are tightened, it has not been securely set and must be replaced. A new hole must be drilled far enough away from the original hole to provide secure material for a new hole. If self-drilling anchors are used, a new anchor must be used for drilling the hole.

E. Erecting the Bay

Warning: Do not hold the blue bay side panels when lifting or joggling the bay into position; use the bay framework for this purpose. The panels can be removed by releasing the quarter-turn captive screws, located at the top and bottom of the panels.

- 4.25 Move the bay to its floor location. Exercise care when moving the bay to avoid sudden shock or strain.

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

- 4.26 The bay can be placed in position by two or more people. For added safety, three 5/8-11 holes are located on the top of the bay. These holes are for lifting when required. Assemble the 5/8-11 eye bolt and tie off with rope to a solid structure overhead.
- 4.27 Lift the bay and place it in position over the anchors. Visually inspect the bay for signs of damage.
- 4.28 Loosely assemble the washer and nut on the anchor stud.
- 4.29 Verify that the bay is level and can be aligned with adjacent bays using junction plates. Junction plates are to be assembled using two 840060164 0.216-24 by 1/4-inch screws per plate. When junction plates can be assembled to an adjacent bay, it can be assumed that the bays are level.
- 4.30 Secure the bay to the floor.

F. External Connections

Ground Connections

- 4.31 The frame-ground (ring ground) connection provided for each bay serves two purposes: to provide a direct earth ground connection for lightning protection and to provide a common ground potential for electrostatic discharge protection. Therefore, the frame ground is the first common wiring connection made after the bay is in place.
- 4.32 All bay frames are provided with grounding connectors. Terminate or crimp the 54720 compression "C" tap to the ground wire (or ring ground) in the cable rack as shown in Figure 9.
- 4.33 All ground connections shall provide a low-resistance contact with the metal framework of the bay. If necessary, remove paint to expose bare metal for the connection.

Power Connections

- 4.34 The 3A Encryptor bays can be powered by either -24 volts dc or -48 volts dc. Care should be taken to ensure that the encryptor and fan shelves to be installed correspond to the power being supplied to the bay. Table E lists the available equipment numbers and their applications.
- 4.35 Two independent power feeds (A and B) are routed from the office battery to the power terminal block on the left side of the Bay Distribution Panel as shown in Figure 10. The following office battery connections are to be made in accordance with information provided in SD-7C479-01, 3A Encryptor Bay Application Schematic, which is included with this manual. Connect the negative lead of the A power feed (-PWR A) to the terminal 1 PWR connector. Connect the positive lead of the A power feed (+PWR A) to the terminal 1 RTN connector. Connect the negative lead of the B power feed (-PWR B) to the terminal 2 PWR connector. Connect the positive lead of the B power feed (+PWR B) to the terminal 2 RTN connector.

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

Alarm and Monitoring Connections

- 4.36 Alarm and monitoring connections are made to the wire-wrap terminal blocks, located on the right side of the Bay Distribution Panel, as shown in Figure 10. Specific information for making the alarm and monitoring connections is supplied in SD-7C479-01, 3A Encryptor Bay Application Schematic, which is included with this manual.

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

5. 3A ENCRYPTOR INSTALLATION

A. Equipment Required

5.01 The following tools and equipment are required to install a 3A Encryptor Terminal Shelf and Fan Shelf in a 3A Encryptor Terminal Bay.

- Slot-head screwdriver
- Ratchet wrench and 3/8-inch socket

B. Unpack Shelves

5.02 Open the shipping cartons and check the equipment for visible damage. Check the equipment numbers stamped on the upper right sides of the encryptor shelves and the fan shelves to verify that the correct equipment has been received and that all components operate on the proper office battery voltage (i.e., -24 V dc or -48 Vdc). Table E lists the equipment numbers and their applications.

5.03 The KEY LOADER connector, located on the left side of the 3A Encryptor front panel, is shipped with a plastic dust cover to protect the connector. This dust cover should be kept and used to cover the connector between key loading sessions.

C. Install Equipment Shelves

5.04 If the bay side-panels are in place on the right and left sides of the bay, remove them by loosening the screws at the top and bottom of the panels.

Install Fan Shelf

5.05 The 3A Encryptors are installed in the bay from the bottom up as shown in Figure 1. Fan Shelf 1 is installed at the bottom of the bay with the accompanying 3A Encryptor shelf mounted directly above. To install Fan Shelf 1, align the shelf mounting brackets with the third and fifth holes on the bay uprights and secure the shelf using two 12-24 thread-cutting screws on each bracket. The remaining shelves in the bay are aligned by placing the unit on the shelf below and aligning the unit with the holes in the bay uprights. The holes used to secure the shelves to the bay are specified in the Table shown below.

SHELF	MOUNTING HOLES
Fan Shelf 1	3 and 5
Encryptor Shelf 1	10, 12, 14, and 16
Fan Shelf 2	22 and 24
Encryptor Shelf 2	29, 31, 33, and 35
Fan Shelf 3	41 and 43
Encryptor Shelf 3	48, 50, 52, and 54
Fan Shelf 4	60 and 62
Encryptor Shelf 4	67, 69, 71, and 73

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

Install Encryptor Shelf

- 5.06 The 3A Encryptor Shelf is designed to prevent the undetected removal of the shelf from the bay framework. This is accomplished by using mounting brackets that interlock with the bay mounting frame and attach to the 3A Encryptor housing from the inside of the housing.

Note: If the MEDECO* security switch lock has not been factory installed perform the installation procedure specified in Section 5.11, Steps 2 through 10.

Warning: The 3A Encryptor circuit packs contain static-sensitive components. Before handling the circuit packs, wear an antistatic wrist strap and connect it to the jack on the lower right corner of a grounded 3A Encryptor housing or to a known frame ground. The 3A Encryptor jack is designated GROUND WRIST STRAP HERE.

- 5.07 The procedure to install the 3A Encryptor shelf is specified below.
- (1) Open the front door and remove the following circuit packs from the left end of the circuit pack mounting shelf: RIU, SCU, PRDG, SKG, and RNG.
 - (2) On the left side of the equipment housing, remove the four nuts which secure the two mounting brackets to the left side of the housing and remove the brackets.
 - (3) Position the fingers of the right-side mounting brackets around the bay upright. The encryptor panel should be resting on the fan shelf which should already have been mounted in the bay.
 - (4) Position the fingers of the left-side brackets around the bay upright and slide the brackets to align the studs with the holes in the left side of the encryptor housing.
 - (5) Resecure the brackets to the encryptor housing using the four nuts removed in Step 2.
 - (6) Align the mounting brackets with the holes in the bay uprights (see paragraph 5.05) and secure the brackets to the bay with 12-24 thread cutting screws.
 - (7) Replace the five circuit packs removed in Step 1.

D. Install Customer-Provided Components

- 5.08 The customer will provide the following components, which are required for each 3A Encryptor:

- Two MEDECO* security cam locks, part number 63-0750-61-M12

* Registered trademark of MEDECO Security Locks, Inc.

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

- One MEDECO* security switch lock, part number 65-2601-102-61
- Three MEDECO* guard collars, part number CP-070131

Install MEDECO Locks

- 5.09** The MEDECO cam lock is used in the INTERLOCK positions on the front and rear doors and screws into captive nuts mounted inside the housing. To install the cam locks follow the procedure specified below and refer also to Figure 11.
- (1) Position the guard collar on the head of the lock.
 - (2) Insert the lock and collar into the opening in the front panel of the 3A Encryptor.
 - (3) Position the washer and tighten the retaining nut.
 - (4) Repeat Steps 1 through 3 for the rear panel of the 3A Encryptor.
- 5.10** The MEDECO switch locks are used for the LOADER ENABLE switches. Four wires with push-on connectors are used to connect these switches to the encryptor circuitry. These wires are located in the wiring harness near the switch panel position. As shown in Figure 12, two sets of three terminals are provided on the back of the switch (six terminals total). For this application, two terminals on each side of the dividing tab are to be used. The terminals on each side of the dividing tab perform identical functions and are interchangeable.
- 5.11** To install the LOADER ENABLE switch lock follow the procedure specified below and refer also to Figure 13. If the switch locks have been factory installed proceed to Section 5.12.

Note: The following procedure should also be used to replace a defective MEDECO switch lock.

- (1) Remove the Fan Shelf from the bay by removing connectors P1 and P2 from the right side of the shelf. Loosen the two screws on one side of the shelf and then remove the two screws from the opposite side of the shelf.
- (2) Loosen the Bottom Panel faceplate by removing three nuts from along the front of the housing bottom. It will be necessary to remove several of the plug-in units to gain access to the three nuts.
- (3) Carefully pull the faceplate away from the main housing.
- (4) Position the guard collar on the head of the lock.
- (5) Insert the lock and collar into the opening in the Bottom Panel faceplate.
- (6) Position the lock washer and tighten the retaining nut being careful not to damage the adjacent LED or its connecting wiring.

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

- (7) Connect the blue and green wires to the terminals on one side of the dividing tab. Connect the blue wire to the terminal labeled C (common) as shown in Figure 13. Connect the green wire to the terminal labeled NO (normally open).
- (8) Connect the orange and green with white stripe wires to the terminals on the other side of the dividing tab. Connect the orange wire to the terminal labeled C. Connect the green with white stripe wire to the terminal labeled NO.
- (9) Carefully replace the faceplate on the front of the housing. The use of excessive force could damage either the switch, the LED, or the panel wiring.
- (10) Replace the three nuts on the three studs on the inside of the housing to resecure the Bottom Panel faceplate.
- (11) Install the Fan Shelf in the bay by replacing and/or retightening the two screws on each side of the shelf. Ensure that the Fan Shelf flange is seated properly and provides a secure seal between the bottom of the 3A Encryptor Shelf and the top of the Fan Shelf to maintain adequate air flow through the encryptor.
- (12) Reattach connectors P1 and P2 to the right side of the shelf and retighten the two screws on each connector.

E. Select Control Channel Option

- 5.12** The 3A Encryptors at each end of the transmission path must select the same control channel option for compatible operation. To form the encryptor control channel, it is necessary to use at least 1 bit in each DS3 frame. Figure 14 shows the location of switches S1 through S5, on the Reframer Unit circuit pack (TL98), which are used to select the control channel configuration. Figure 15 summarizes all bits associated with the DS3 frame as a reference in selecting the control channel option. The switches on switch blocks S1 through S5 must be set to the same settings on four RFU circuit packs (two at the near end terminal and two at the far end terminal) to achieve compatible control channel operation. The control channel option to be used, for each system application, is normally determined by regional operations personnel.
- 5.13** The following control channel options are listed in their order of preference. The first three options, X-data bit, stuffing bit, and limited stuffing, are recommended because they utilize otherwise unused bits for control channel use. The framing bit and fixed data bit options are not recommended if one of the first three options can be used because these options share bits being used for another function. Using the framing bit or fixed data bit control channel options will result in the control channel generating errors on the framing or customer data bits being used.

X-Data Bit Control Channel

- 5.14** The X-data bit control channel option uses the maintenance channel formed by the X-control bits of Subframes 1 and 2 to form the control channel. To select the X-data bit for control channel use, set switches S1 through S5 on the RFU circuit pack (TL98) as shown in Table F.

**AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions**

Stuffing Bit Control Channel

- 5.15 The stuffing bit control channel uses the stuffing bits in the DS3 frame. The stuffing bit control channel option is selected by setting switches S1 through S5 on the RFU circuit pack (TL98) as shown in Table F.

Limited Stuffing Bit Control Channel

- 5.16 The limited stuffing bit control channel option uses a single specified stuffing bit in the DS3 frame. The limited stuffing bit control channel option is selected by setting switches S1 through S5 on the RFU circuit pack (TL98) as shown in Table F.

Framing Bit Control Channel

- 5.17 The framing bit control channel option uses one framing bit (F1 or F0) from each DS3 frame to form the control channel. This option should be selected with care since some non-AT&T multiplex terminal equipment may be susceptible to framing bit errors should this option be selected. This control channel option is used by selecting one framing bit in the DS3 frame as follows:

- (1) Set all switches on switch blocks S1 through S5 to the open (0) position.
- (2) Set switches S4-4 and S5-3 to the closed (1) position.
- (3) Select the subframe and the framing bit in that subframe, chosen as the control channel bit, and set switches S3-1 through S3-4 and S4-1 and S4-2 as specified in Table G.

Fixed Data Bit Control Channel

- 5.18 The fixed data bit control channel uses one customer data bit per DS3 frame to form the control channel. As shown in Figure 15, customer data is arranged in blocks of 84 data bits plus an associated DS3 control bit. Selecting the fixed data bit control channel option requires the selection of the particular data bit to be used for the control channel plus the DS3 control bit following the customer data bit as follows:

- (1) Set all switches on switch blocks S1 through S5 to the open (0) position.
- (2) Set switches S4-4 and S5-3 to the closed (1) position.
- (3) Set switches S1-1 through S1-4 and S2-1 through S2-3 as shown in Table H for the customer data bit selected for use as the control channel bit.
- (4) Set switches S3-1 through S3-4 and S4-1 and S4-2 as indicated in Table G for the control bit following the customer data bit selected for use as the control channel bit.

Example: If the control channel uses customer data bit 24 in the data block preceding the C23 control bit, set the switches in accordance with the following procedure.

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

- (1) Set all switches on switch blocks S1 through S5 to the open (0) position.
- (2) Set switches S4-4 and S5-3 to the closed (1) position.
- (3) Set switches S3-1 and S3-3 to the closed (1) position. (See Table G, Subframe 2, Control Bit C23.)
- (4) Set switches S1-1, S1-4, and S2-2 to the closed (1) position. (See Table H, Customer Data Bit 24).

F. Make External Connections to the Shelves

Alarm and Status Lead Connections

- 5.19 The alarm and status leads are connected to the office alarm system and to the remote monitoring center. To provide the alarm and status connections, connect the bay alarm and status cable to the alarm and status connector on the center right side of the 3A Encryptor shelf (see Figure 4).

DS3 Connections to the Regular 3A Encryptor

Warning: Connecting the 3A Encryptor into an operational DS3 system will cause a service interruption while the DS3 cables are being connected. To prevent a service interruption the signal should be rerouted to an alternate facility, using approved company operating procedures, during this patching procedure.

- 5.20 The DS3 signal input and output connections to the Regular 3A Encryptor are made to the plugs located on the lower left side of the encryptor shelf as shown below:
- (1) Plug P5 • T-IN, plain-text DS3 signal input
 - (2) Plug P6 • T-OUT, encrypted DS3 signal output
 - (3) Plug P7 • R-IN, encrypted DS3 signal input
 - (4) Plug P8 • R-OUT, plain-text DS3 signal output

DS3 Connections to the Hot-Standby 3A Encryptor

- 5.21 There are no direct cable connections from the DSX-3 Cross Connect Panel to the Hot-Standby 3A Encryptor. All DS3 signal connections to the Hot-Standby 3A Encryptor are made between the Patch Panels on both the Regular and Hot-Standby terminals. To prevent alarms from being generated due to the lack of a DS3 input signal to the Hot-Standby terminal, it is recommended that the transmitting and receiving sections of the Hot-Standby unit be looped back on each other and a DS3 input signal be provided to the input of the terminal. This can be accomplished by connecting a patch cord between jacks 2 and 4 of the Hot-Standby terminal and

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

connecting a second patch cord between jack 1 of the Hot-Standby terminal and jack 1 of any Regular terminal. This also ensures that a known working terminal is available to patch in place of a failed Regular terminal should the need arise. (Inserting a patch plug into jack 1 of a working terminal will not cause a hit or any disruption of service being applied to the Regular terminal being used to provide a DS3 signal to the Hot-Standby terminal.)

Power Connections

- 5.22** Power connections to the 3A Encryptor are made via the Fan Shelf. A cable, provided with the encryptor shelf, is used to provide power from the Fan Shelf to the encryptor. Fuses for the 3A Terminal are mounted in the fuse block located on the Distribution Panel. Each 3A Encryptor and Fan Shelf is powered by a primary and a secondary power source (an "A" feed and a "B" feed). The primary power source is provided for the encryption circuitry plus Fan-A, while the secondary power source supplies power to the bypass or protection transmission path and Fan-B. The power sources are protected by the fusing arrangement shown in Figure 16. This figure shows that the primary power circuit utilizes both a main and an alarm (indicating-type) fuse while the secondary power circuit utilizes an indicating-type fuse in the alarm position (the main fuse position is equipped with a dummy fuse).
- 5.23** Power connections to the 3A Encryptor bay are to be made as follows:
- (1) Remove the primary and secondary power fuses (three fuses) from the fuse blocks at the top of the bay associated with the terminal under test. The fuse assignments are specified in Figure 16.
 - (2) Open the front door of the 3A Encryptor and remove both Power Units from the shelf (471AB and 471BA for -24 volt operation, or 474AB and 474BA for -48 volt operation). Also remove the Bypass Switch plug-in unit (TL100 for -24 volt operation or TL107 for -48 volt operation).
 - (3) Ensure that the cable connecting jack J4, located on the right side of the 3A Encryptor panel, and jack J2, located on the Fan Shelf, is in place and that both connectors are securely fastened.
 - (4) Install the fuses in the BDFB which supply the -24 or -48 volt battery to the 3A Encryptor panel or bay under test. Fuses will be required in both the "A" and "B" feeds. Verify that voltage is present at Terminal Strip TB1, located in the Distribution Panel at the top of the bay (see Figure 10).
 - (5) Insert the fuses, for the panel under test, into their appropriate positions in the "A" and "B" feed fuse positions in accordance with the information furnished in Figure 16. Install the Main fuse first followed by the Alarm fuse. Whenever the "A" or "B" feed is providing power only to the Bypass Switch plug-in unit the Main fuse position will be equipped with a dummy fuse.
 - (6) Insert the TL100 or TL107 Bypass Switch plug-in unit into the encryptor shelf. Also insert the two power units (471AB and 471BA for -24 volt operation, or 474AB or 474BA for -48 volt operation) into the encryptor shelf.

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

6. 3A ENCRYPTOR RELIABILITY ACCEPTANCE CRITERIA

6.01 The following paragraphs define recommended 3A Encryptor acceptance criteria in terms of practical operating objectives. The acceptance criteria defined in paragraphs 6.02 and 6.03 place requirements on the percentage of time the unit is expected to encrypt the DS3 data stream and on the frequency of session key changes.

6.02 When trying to determine the likelihood of the encryptor being in the CLEAR, or nonencrypting mode, it is important to recognize that certain external circuit conditions will cause the unit to cycle between the encrypting and nonencrypting modes of operation until reliable encryption can be resumed. These circuit conditions have been excluded from the proposed acceptance criteria in paragraph 6.03. Examples of such excluded circuit conditions are:

- **Input Signal Impairments** The encryptor and decryptor sections of the 3A Terminal are designed to operate with an input signal that is compatible with AT&T Technical Advisory 34 in terms of format, jitter, level, etc. Impairments such as excess jitter or loss of frame will cause the encryptor to revert to the CLEAR operating mode. Also, the decryption process at the receiving end of the system is checked against the encryption process at the transmitting end of the transmission path using the built-in communication channel of the 3A Encryptor. Errors introduced by the interconnecting transmission facility can be interpreted as decryption errors and can result in the unit operating in the CLEAR mode. On radio equipment, transmission path fading will probably be the most likely source of impairment. Even with fading, the impact on encryptor performance will be slight, since the 3A Encryptor will continue to encrypt down to bit error rates as great as 10^{-3} . However, as a 10^{-3} transmission error rate is approached, there is an increasing probability that the terminal will cycle between the ENCRYPT and CLEAR modes of operation. During normal undisturbed propagation conditions, when the residual errored seconds on the system are only a few per day (less than 10 errored seconds per day), the impact on ENCRYPT-to-CLEAR mode cycling will be negligible.

- **Hardware Failures** The impact of a hardware failure, though expected to be infrequent, will depend on the specific failure involved. However, it is known that some hardware failures will result in excess cycling between the ENCRYPT and CLEAR operating modes. Cycling between the ENCRYPT and CLEAR modes, associated with an identifiable hardware trouble, has been excluded from the proposed acceptance criteria.

- **Miscellaneous** Also excluded from the proposed acceptance analysis are ENCRYPT-to-CLEAR mode cycling events associated with operator intervention or abnormal environmental conditions.

6.03 The considerations in the preceding paragraph lead to the following recommended acceptance criteria:

- (1) The acceptance test period shall be 30 days of service, excluding periods when there are identifiable problems due to input signal impairments, system transmission impairments, 3A hardware problems, or operator intervention as discussed in paragraph 6.02.

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

- (2) The 3A Encryptor shall have no significant effect on the network data-error performance characteristics during the acceptance test period. Specifically, the contributions of the encryptors to DS3 transmission impairments shall not exceed 3 errored seconds per day.
 - (3) The 3A Encryptor will not use the same encryption session keys for more than 25 consecutive hours during the acceptance test period.
 - (4) A 3A Encryptor/Decryptor pair will not be out of the encryption mode for more than 0.01 percent of the acceptance test period. This permits a total of 51 encryption session cycles during the 30-day period. Thirty of these cycles will be due to the required, programmed session key changes every 24 hours.
- 6.04** The proposed encryption reliability of 99.99 percent is consistent with the need to provide daily session key changes and, at the same time, provide a very high level of data security.

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

7. VERIFY 3A ENCRYPTOR OPERATION

7.01 This section contains procedures for testing the 3A Encryptor prior to turnup for service. Proper installation of the 3A Encryptor is verified by applying power to the encryptor and its associated fan shelf and performing internal and external tests to verify that the encryptor is operating properly.

A. Required Test Equipment

7.02 The following test equipment, or equivalent, is required to perform verification tests on the 3A Encryptor.

- 1 • Telecommunications Techniques Corporation T-BERD 305 DS3 ANALYZER equipped with a T-BERD 201 T-CARRIER ANALYZER (cover) option
- 1 • Digital Multimeter

B. Power-Up, Loopback, and Mode Tests

Caution: Before applying power to the 3A Encryptor, all fuses associated with the terminal or terminals under test shall be removed from the fuse panel. The fuse panel is located at the top of the bay. Open the door of the 3A Encryptor(s) and remove the two power units (471AB and 471BA for -24 volt operation, or 474AB and 474BA for -48 volt operation). Also remove the Bypass Switch plug-in unit (TL100 for -24 volt operation or TL107 for -48 volt operation).

- 1 Ensure that the cable connecting jack J4, located on the 3A Encryptor Panel, and jack J2, located on the Fan Shelf, is in place and that both connectors are securely fastened.
- 2 Install the fuses in the BDFB which supply the -24 or -48 volt battery to the 3A Encryptor panel or bay under test. Fuses will be required in both the "A" and "B" feeds. Verify that voltage is present at Terminal Strip TB1, located in the Distribution Panel at the top of the bay. The Distribution Panel configuration is shown in Figure 10.
- 3 Insert the fuses for the panel under test into their appropriate positions in the "A" and "B" Feed fuse positions in accordance with the information furnished in Figure 16. Install the Main fuse first followed by the Alarm fuse. Whenever the "A" or "B" feed is providing power only to the Bypass Switch plug-in unit the Main fuse position will be equipped with a dummy fuse.

Caution: The power for each panel is supplied from either the "A" or "B" Feed depending on its location in the bay. The power for the Bypass Switch plug-in unit is supplied from a separate source than the power provided for the encryption circuitry. Two fuse positions (a Main and Alarm)

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

have been provided but only the Alarm position fuse is required to provide power for the Bypass Switch plug-in unit. A dummy fuse is furnished for the Main fuse position when that fuse assignment provides power for the Bypass Switch plug-in unit. Whenever the Main fuse provides power to the encryption path both the Main and Alarm fuses must be installed. It is important that the Main fuse be inserted before the Alarm fuse to prevent the Alarm fuse from being blown since the two fuses are in parallel. The Alarm fuse is intended to provide a visual indication of a blown fuse since the 74-type fuse required for the Main fuse position is not an indicating-type fuse.

Requirement 1: Both fans in the Fan Shelf shall be operating.

Requirement 2: The ALARM LED, located on the Fan Shelf, shall be ON.

- 4 Remove the two TL98 Reframer Unit (RFU) plug-in units from the encryptor shelf and set the control channel switches (S1 through S5) for the DS3 bit which has been selected by regional operations personnel. (See Table F, G, or H and the TL98 plug-in unit figure which provides the information required to set the DS3 control channel bit for this application.) It is imperative that the switch settings on both TL98 plug-in units are identical and must match the switch settings of the TL98 RFUs at the far end station. When this has been completed, reinsert the plug-in units into their original shelf positions.

Caution: ESD grounding wrist straps must be used whenever removing or handling the 3A Encryptor plug-in units.

- 5 Insert the TL100 (or TL107) Bypass Switch plug-in unit into the encryptor shelf.

Requirement 1: The GREEN LED, located on the front edge of the TL100 or TL107 Bypass Switch plug-in unit, shall be ON.

Requirement 2: The BYPASS ON LED, located on the Top Panel, shall be ON.

- 6 Operate the MODE SELECT switch to the NORMAL position.

- 7 Insert the two Power Units (471AB and 471BA for -24 volt operation, or 474AB and 474BA for -48 volt operation) into the encryptor shelf. The front door of the encryptor being tested shall remain open.

Requirement 1: The following LEDs, located on the 3A Encryptor under test, shall be ON: MAJOR ALARM, DOOR OPEN, KEY ZEROIZED, LOSS OF INPUT, SYNC CYCLE, and BYPASS ON.

Requirement 2: The ALM/OFF LEDs, located on the two Power Unit plug-in units of the 3A Encryptor under test, shall be OFF.

Requirement 3: The ALARM LED, located on the Fan Shelf, shall be OFF.

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

- 8 Operate the LOOP TEST pushbutton switch (located on the faceplate of the TL105 Remote Interface plug-unit).
- Requirement:** The ON LED, located on the faceplate of the TL105 plug-in unit, shall be ON.
- 9 Press and hold the TEST pushbutton switch (located on the faceplate of the TL105 plug-in unit).
- Requirement:** ALL LEDs on the 3A Encryptor shall be ON **except** the ALM/OFF LEDs located on the faceplate of the two Power Units. This includes one RED LED on each of the plug-in units in the encryptor shelf (two LEDs, a GREEN and a RED, are used on the Bypass Switch plug-in unit) as well as each LED on the Top and Bottom Panel.
- 10 Release the TEST switch. The 3A Encryptor is performing a self-test routine. During this sequence observe the indications specified in the following requirement.
- Requirement:** The SYNC CYCLE LED will remain ON for approximately 5 seconds. The SYNC CYCLE LED will turn OFF and the ENCRYPTOR ON LED will turn ON. After a few seconds, the PASS LED, located on the faceplate of the TL105 plug-in unit, will turn ON. (Should the FAIL LED turn ON instead of the PASS LED, repeat the test to ensure that the test routine was performed properly. Normally, when the FAIL LED turns on there is a failure on one of the plug-in units. This failure indication is normally accompanied by the RED LED on the front edge of the failed unit also turning ON to identify the circuit pack which is the source of the self-test failure.)
- 11 Close and lock the front and rear doors of the 3A Encryptor.
- Requirement 1:** The DOOR OPEN LED, located on the Top Panel of the 3A Encryptor, shall be OFF.
- Requirement 2:** The MAJOR ALARM, KEY ZEROIZED, LOSS OF INPUT, SYNC CYCLE, and BYPASS ON LEDs shall be ON.
- 12 Set the controls of the T-Berd 305 DS3 Test Set Transmitter and Receiver to provide a test signal in accordance with the following settings.

TRANSMITTER SECTION		RECEIVER SECTION	
FUNCTION	SETTING	FUNCTION	SETTING
TRANSMIT OUTPUT	DSX	RECEIVE INPUT	HIGH
PATTERN	2 ¹⁵ -1	CATEGORY	LOGIC
TIMING	INTERNAL	RESULT (SCROLL)	ERRORS
TEST	CONTINUOUS	PRINTER CONTROL	OFF

AT&T-PROPRIETARY (RESTRICTED)
 Solely for authorized persons having a need to know
 pursuant to Company Instructions

Note 1: In the following tests the DS3 test signal will be connected to the 3A Encryptor under test. The test signal can be connected to the terminal directly at the Transmitter or Receiver inputs or outputs, using the appropriate Seaelectro- or BNC-to-Coaxial adapters, or the test signal can be applied and measured at the DSX-3 Cross Connect Panel (preferred test configuration). If the test signals are applied at the DSX-3 Cross Connect panel the terminal performance will be measured in its normal system operating configuration including all connecting cabling. For measurements made at the DSX-3 Cross Connect Panel change the T-BERD 305 RECEIVE INPUT level to DSX. The HIGH level should be used only if measurements are to be made directly at the output of the 3A Encryptor Terminal. When the terminal is to be measured in the 3A Terminal bay the system will be evaluated in a test-only mode. The Input and Output jack designations for the Regular and Hot-Standby 3A Terminals are shown below.

<u>REGULAR TERMINAL</u>	<u>HOT-STANDBY TERMINAL</u>
P5 TRMTR • INPUT	Jack 1 TRMTR • INPUT
P6 TRMTR • OUTPUT	Jack 2 TRMTR • OUTPUT
P7 RCVR • INPUT	Jack 4 RCVR • INPUT
P8 RCVR • OUTPUT	Jack 3 RCVR • OUTPUT

Note 2: If testing is to be performed by applying a test signal at the 3A Terminal under test, connect the DS3 signal from the T-BERD 305 test set transmitter to 3A Transmitter Input plug P5. Connect the 3A Transmitter Output to the 3A Receiver Input by connecting a cable between Transmitter Output plug P6 and Receiver Input plug P7. Connect the DS3 signal from the 3A Receiver Output plug, P8, to the DS3 test set RECEIVE INPUT jack. If testing is to be performed by applying a test signal at the DSX-3 Cross Connect Panel (the preferred testing procedure since testing will include all interconnecting cabling) proceed to Step 13. (If testing is to be performed at the 3A Encryptor proceed to Step 15.)

- 1 3** At the DSX-3 Cross Connect Panel connect the DS3 Signal from the test transmitter to the IN jack associated with the Regular 3A Encryptor Terminal under test as shown in Figure 17. (This jack will be associated with the MUX side of the DSX-3 Cross Connect Panel.)
- 1 4** At the DSX-3 Cross Connect Panel connect the signal from the OUT jack associated with the Regular 3A Encryptor Terminal under test to the test receiver input as shown in Figure 17. (This jack will also be associated with the MUX side of the DSX-3 Cross Connect Panel. The 3A Terminal Transmitter Output will automatically be looped to the 3A Terminal Receiver input by the normal through jack used in the DSX-3 Cross Connect Panel.)
- 1 5** Connect the 247A Key Insertion Device (KID) to the KEY LOADER connector, located on the Bottom Panel of the encryptor under test.

Caution: ALWAYS connect the 247A KID to the KEY LOADER connector **BEFORE** turning the **LOADER ENABLE** keylock switch to the **ON** position. ALWAYS turn the **LOADER**

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

ENABLE keylock switch to the OFF position BEFORE removing the KID from the KEY LOADER connector. When the LOADER ENABLE keylock switch is turned ON, voltage is applied to some of the connector pins. The prescribed loading sequence prevents the possible shorting of powered connector pins while inserting or removing the 247A KID to/from the KEY LOADER connector.

1 6 Operate the LOADER ENABLE keylock switch to the ON position.

Requirement 1: The LOADER ENABLE ON LED shall be ON.

Requirement 2: The READY-PRESS LOAD LED shall be ON.

Note: If the ERROR-PRESS LOAD LED turns ON instead of the READY-PRESS LOAD LED an error may have occurred in the software loading process within the 3A Terminal. Disregard the indication and proceed with Step 17. If the LED indication continues after repeated attempts to load key material a problem exists with either a plug-in unit in the 3A Terminal (TL101 - SKG) or the keying material supplied by the EEPROM mounted in the 247A KID.

1 7 Operate the LOAD pushbutton switch.

Requirement 1: Within approximately 3 seconds, the READY-PRESS LOAD LED will turn OFF and the LOADING COMPLETED LED will turn ON.

Requirement 2: The KEY ZEROIZED and ENCRYPTOR ON LEDs shall be OFF. The MAJOR ALARM, SYNC CYCLE, and BYPASS ON LEDs shall be ON.

Note: If the ERROR-PRESS LOAD LED turns ON repeat this Step. If the LED indication continues after repeated attempts to load key material a problem exists with either a plug-in unit in the 3A Terminal (TL101 - SKG) or the keying material supplied by the EEPROM mounted in the 247A KID.

1 8 Operate the LOADER ENABLE keylock switch to the OFF position.

Requirement: The LOADER ENABLE ON LED shall be OFF.

1 9 Remove the 247A KID from the KEY LOADER connector.

2 0 Simultaneously press and hold the LOAD and RESET/LAMP TEST pushbutton switches. Release both switches after approximately 1 full second.

Requirement: The SYNC CYCLE LED will be ON. After approximately 10 seconds the SYNC CYCLE LED will turn OFF and the ENCRYPTOR ON LED will turn ON.

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

- 2 1 Operate the MODE SELECT switch to the BYPASS position.
- Requirement:** The MAJOR ALARM, SYNC CYCLE, and BYPASS ON LEDs shall be ON. (There may be a delay of a few seconds before the 3A Terminal switches from the NORMAL mode to the BYPASS mode.)
- 2 2 Operate the MODE SELECT switch to the NORMAL position.
- 2 3 Operate the RESET/LAMP TEST pushbutton switch.
- Requirement:** The BYPASS ON LED will turn OFF and only the SYNC CYCLE LED will be ON. After a period of time the SYNC CYCLE LED will turn OFF and the ENCRYPTOR ON LED will turn ON. (The time interval can extend from as short as 5 seconds to as long as 30 seconds.)
- 2 4 Reset the DS3 test receiver and monitor the error performance of the 3A Terminal under test.
- Requirement:** The terminal shall run error free. Measure the error performance for approximately 1 minute before proceeding to the next test.
- 2 5 Operate the MODE SELECT switch to the CLEAR position.
- Requirement 1:** The ENCRYPTOR ON LED shall turn OFF and the SYNC CYCLE LED will turn ON.
- Requirement 2:** The DS3 test receiver shall continue to show that no errors have occurred when the terminal has switched from the ENCRYPTOR ON mode to the CLEAR mode.
- Requirement 3:** After approximately 30 seconds the MAJOR ALARM LED will turn ON.
- 2 6 To test the Hot-Standby terminal generate the test signals at the 3A Terminal Bay by applying the signal from the T-BERD 305 Test Transmitter into jack 1 of the Hot-Standby terminal to be tested (set the TRANSMIT OUTPUT level of the T-BERD 305 Test Set to DSX). Connect the Transmitter Output of the Hot-Standby terminal to the Hot-Standby Receiver Input by connecting a cable between jacks 2 and 4. Connect a cable between jack 3 of the Hot-Standby Receiver to the RECEIVE INPUT jack of the T-BERD 305 Test Receiver (set the RECEIVE INPUT level of the T-BERD 305 Test Set to HIGH). Repeat Steps 1 through 25 using the input and output information specified in this Step. If the Hot-Standby terminal is the last terminal to be tested, proceed to the next Section of this Practice.
- Note 1:** When all back-to-back testing of the 3A Encryptors for this installation has been completed, contact the personnel at the station where the remote alarms

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions

will be monitored and verify that the local and remote alarms are generated correctly and that the remote bypass and reset commands are operational. The alarm testing procedure is specified in Section 12.

Note 2: After completing the tests specified in this Section and while awaiting the completion of testing at both ends of the system prior to placing the 3A Terminal equipment in the transmission path it is recommended that the terminals be connected in pairs simulating end-to-end system operation. This connection can be completed at the DSX-3 Cross Connect Panel using two patch cords as shown in Figure 18. In addition, a test signal should be applied at the transmitter input of each terminal and, wherever possible, the error performance of the terminal pairs should be monitored until the terminals are ready to be placed in service.

AT&T-PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions