Module 7 – Conditional Access and Security

Summary
In this module, students will learn engineering theory and operational information about Conditional Access and Security.

Outcomes
When they complete this module, students will be more knowledgeable about Conditional Access, and as a consequence will be more able to operate, maintain, and troubleshoot this kind of system.

Module Objectives
Upon successful completion of this module, students will be able to:

• Understand the concept of Conditional Access in a digital system.
• Identify key applications for Conditional Access in the cable system.
• Describe the implementation of Conditional Access.
• Understand how digital information is encrypted.
• Understand the role of public and private keys.
• Be aware of the various standards that exist for Conditional Access.
• Describe the security interfaces within a digital set-top unit.
• Describe the role of the technician in supporting Conditional Access.
• Demonstrate familiarity with the use of Smart Cards in Conditional Access Systems.

Prerequisites
Students should have read Chapter 7 of DigiPoints, Volume 2.

Length
3 hours
Materials/Preparation for Instructor

- One workbook per student
- The instructor should read Chapter 7 of *DigiPoints, Volume 2*, and complete review questions from the chapter.
- System-specific information about Conditional Access and programming security, as available, including:
  - Kind of equipment used.
  - Encryption methods used.

Supplies/Equipment

- Flip chart or board, markers
- Overhead projector or LCD

Audience

The intended audience will be mid- to senior-level technicians or other associates who are seeking an understanding of digital basics.
Module Outline

This is an introductory level module that will provide a review of the following topics:

Objectives.............................................................................................................................1
Introduction ..........................................................................................................................2
What is Conditional Access?.............................................................................................3
High-Speed Data Access via Cable Modem .................................................................5
How Conditional Access Works ......................................................................................9
OpenCable Standards for Conditional Access ............................................................22
The Harmony Agreement .............................................................................................26
Practical Digital: The Role of the Technician...............................................................27
Summary ............................................................................................................................28
Appendix.............................................................................................................................30
Objectives

Tell students that when they have completed this module, they will be able to accomplish these objectives.

- Understand the concept of Conditional Access in a digital system.
- Identify key applications for Conditional Access in the cable system.
- Describe the implementation of Conditional Access.
- Understand how digital information is encrypted.
- Understand the role of public and private keys.
- Be aware of the various standards that exist for Conditional Access.
- Describe the security interfaces within a digital set-top unit.
- Describe the role of the technician in supporting Conditional Access.
- Demonstrate familiarity with the use of Smart Cards in Conditional Access Systems.
Introduction

Ask students the following questions:

- What purpose does Conditional Access provide?
- Identify possible applications for Conditional Access.

Tell students that this module will increase their knowledge of how Conditional Access is implemented.

EXPLAIN

Overview

- Explain that this session will investigate the concepts that support conditional access such as:
  - Security protocols (encryption/decryption “rules”) that implement encryption/decryption keys
  - Security interfaces to the set-top unit
- Relationship between the security interfaces and the security protocols that operate across it:
  - As specified by CableLabs OpenCable™ specifications
What is Conditional Access?

DISCUSS

Explain to the students that Conditional Access is:

- Control mechanisms
- Data structures
- Data commands that:
  - Provide selective access or denial of specific services

READ THE DEFINITION AND REMIND STUDENTS TO WRITE IT IN THEIR WORKBOOKS WB 7.3

Definition: Conditional Access systems make use of signal security, which is any technology, such as encryption, that can prevent a signal from being received except by authorized users.

REFER TO WB 7.4

Refer students to Workbook Exercise 1. Have the students complete the exercise by labeling the components in the diagram as you identify them.

REFER TO VA 7.1

- Implementation of CA may include several encryption/decryption processes (or components in a digital system).
- For example in video systems:
  - Satellite uplinks are typically encrypted.
  - Corresponding decryption occurs at the receiving headend.
  - Before distribution in the cable system, the signal is re-encrypted.

Finally, the signal is decrypted at the authorized subscriber’s set-top.

- In data applications, data security (encryption) can be applied at the:
  - Headend file server.
  - Cable modem.

EXPLAIN

Tell the class that in our discussions today, references to CA at the set-top also apply to security that is included in cable modem design.

Definition from Scientific-Atlanta’s Glossary of Encryption Technology

Trace the signal path and point out the conditional access roles of the Digitization Center, IRT, IRD, and set-top.
• Practical implementation of encryption/decryption process is possible in one of two methods:
  • Integrated circuit components:
    ◊ VA 7.1 is an example.
  • Circuitry on cards:
    ◊ Inserted into the component
    ◊ Renewable security
    ◊ Removed and replaced when necessary
    ◊ Two examples of such cards are:
      • Smart cards
      • PC cards

Tell the class that Conditional Access was part of the cable system long before digital technology was deployed:

  • In analog systems, signal scrambling is a form of Conditional Access:
    ◊ Generally, the video sync pulse is modified rendering the video signal “unintelligible” to unauthorized viewers.

**DISCUSS**

**DISCUSS**

**Conditional Access Applications**

Explain to the class that:

  • Within the CATV industry, the traditional application for CA has been to prevent signal piracy of premium services in one-way systems.
  • The subscriber perceived little benefit from Conditional Access and as a result:
    ◊ Set-top clones evolved that illegally descrambled (decrypted) the premium service.
      • Services without payment
  • In two-way digital systems, system security benefits both the operator and the subscriber.

**Discuss the new services that two-way capability makes possible**
High-Speed Data Access via Cable Modem

Explain to the class that security is important when high-speed data access is used to connect an employee at home to his employer’s corporate LAN.

- An employee working at home can access data that includes:
  - Confidential information
  - New or proprietary product designs
  - Corporate marketing strategies
- The employer may employ its own data encryption techniques.
- The employer may also insist that the cable operator provide additional data security.

EXPLAIN

Electronic Commerce

Explain that in electronic commerce two devices are competing to provide service:

- The home computer.
- The TV plus the digital set-top terminal.

Point out that applications of electronic commerce include:

- “Bank at home” application where using a home terminal the subscriber can:
  - Access account information
  - Transfer balances
  - Pay bills
- Credit card transactions

Tell the class that when electronic commerce uses a PC (home computer) the security issues and implementations are similar to the work at home scenario discussed earlier.
• The service provider employs security (data encryption) for:
  ◊ Passwords
  ◊ Personal identification numbers (PIN)
  ◊ Systems access

DISCUSS

• There will also be a requirement for secure transport of such data since:
  ◊ The transport cable is a shared medium.

EXPLAIN

Point out that when the set-top rather than the PC, is used for electronic commerce, it must:

• Perform all security functions at the subscriber end.
• Decrypt the service provider’s security measures.

DISCUSS

**Subscriber Identification and Digital Signature**

Tell the class that as paper based and face-to-face transactions move to the electronic age, there is a requirement to:

• Replace the conventional signature with an electronic version that:
  ◊ Remains legally binding
  ◊ Provides proof that the individual has agreed to the particular transaction

Explain that advanced encryption techniques can provide:

• A digital signature that is created from the following:
  ◊ User’s original document
  ◊ Special encryption particular to the user

Lead discussion about possible risks of shared media vs. dedicated phone wire.
DISCUSS

Protection of System Software and Downloads from the Headend to the Digital Set-Top Terminal

Tell the class that:

- Software/Firmware applications within the set-top often require updates or “bug-fixes”.
- These updates can be downloaded over the cable.
- If the updates are to provide access to new features/applications then preventing piracy of the download is important.

DISCUSS

Multiple Service Providers in a Single Network

Explain to the class that:

- Traditional cable systems are closed systems where the cable operator:
  - Owns the distribution facility
  - Provides content to the subscriber
- In the new communications market, the service provider may:
  - Purchase access from the cable operator
  - Own the programming content
- Long distance telephony is an example of such a model where the long distance connection to the subscriber may be provided by the:
  - The cable operator or
  - The local telephone company

EXPLAIN

Explain to the class that new applications for the cable operator will likely follow this model where multiple set-top boxes dedicated to one or more applications are installed in the network.

- Multi-level encryption methods provide:

©SCTE
◊ Selective decryption of data streams
◊ Ability to decrypt data streams from different content providers
◊ Migration path for the set-top unit to a consumer product which consumers can purchase at retail outlets
◊ Conditional Access will be implemented by removable cards.

Ask students for examples of similar uses of removable cards.
How Conditional Access Works

Explain to the class that:

- Digital Conditional Access requires encryption of data.
- Data encryption is achieved by either:
  - A code, or
  - A cipher.
- The code method is an encryption/decryption process where:
  - A table of letters, words or phrases is substituted for those in the original message
  - Each party involved in the data transaction has access to this table.
- The main advantage of the code method is its simple implementation.
- The main disadvantages are:
  - Fixed code
  - Requires code storage in either:
    - Machine memory
    - Human memory
  - All parties have access to the code, which makes breaking the code relatively easy
- The cipher method is an encryption/decryption process which:
  - Employs a mathematical algorithm and a key to modify a bit-stream into an unintelligible cryptogram
  - Uses a key that is a string of bits that determines the output of the algorithm
- Each new key will generate a different ciphertext output.
- The original bit stream (message) is termed plaintext.
- The encrypted bit stream (message) is termed ciphertext.
- The main advantages of cipher method are:
  - More secure process than code
  - Easily generated by computer processors due to their mathematical basis

Standards for data encryption will be discussed later.

Algorithm = Mathematical formula.
Secret Keys

Explain that in conventional data encryption processes:

- The same key is common to both encryption and decryption processes.
- The encryption process converts original data (plaintext) to ciphertext.
- Ciphertext is transmitted to the receiver.
- The receiver decrypts the data.
- The result is the original plaintext message.
- The key makes the encryption unique.
- Data security depends on:
  - Keeping the key secret
  - Only the sending and receiving parties having access to the key

Explain to the class that since:

- The output of the algorithm (ciphertext) is dependent on the key:
  - There is no need for the algorithm to be kept secret.
- This allows the algorithm to be:
  - Coded in firmware
  - Mass produced
  - Used in several systems (shared)
- The algorithm must be significantly complex to disallow recovery of plaintext by:
  - Trial and error applications with random secret keys

Tell the class that the most widely used secret key encryption scheme is the Data Encryption Standard (DES).

- Adopted in 1977 by the National Bureau of Standards.

Inform the class that:

- In broadcast scenarios, the cipher method works extremely well.
- The same content is distributed to multiple recipients.

*DES will be discussed in the next section.*

*A two key system will be discussed later.*
• Each set-top contains:
  ◊ The decryption algorithm
  ◊ The secret key

• Key disadvantages of this method are:
  ◊ The storage of the key must be physically secure to avoid:
    • Theft of the key
    • Cloning of set-top terminals

Point out that the secret key alone does not provide sufficient security for enhanced, two-way applications.
EXPLAIN
REFER STUDENTS TO WB 7.10-7.11, AND REMIND THEM TO COMPLETE THE SENTENCE ABOUT THE GOAL OF DES.

Data Encryption Standard (DES)

Background

Explain that DES

• Was first issued by the National Institute of Standards and Technology (NIST) in 1977.
• Provides an encryption algorithm for use in protecting federal unclassified information.
• Prevents unauthorized disclosure or undetected modification of information during:
  ◊ Data transmission, and
  ◊ Data storage
• Is reviewed every five years to determine whether the algorithm should be:
  ◊ Affirmed,
  ◊ Revised, or
  ◊ Withdrawn.
• Is based on the work of IBM
• Has been adopted as an American National Standard X3.92-1981/R1987

Technical Overview

Explain that DES:

• Is a publicly owned cryptographic algorithm.
• Converts plaintext to ciphertext using a 56-bit key.
• Decryption converts the ciphertext to plaintext using the same key and the same algorithm as the encryption process.

Point out that the goal of DES is to completely scramble the data and key such that every bit of ciphertext is dependent upon:

• Every bit of data plus every bit of the key

Explain that DES consists of:

• 16 “rounds” of operations that mix the data and key together using the fundamental operations of permutation and substitution

Plaintext = original data (message).

Ciphertext = encrypted data.
DISCUSS

Emphasize to the class that:

- In order to decrypt the data, authorized users must have access to the key that was used in the encryption process.
- Employing a different key will provide a different encrypted data stream (ciphertext).
- The security of the data depends on the security provided for the key.
- Key management follows FIPS 171, Key Management Using ANSI X9.17.

Discuss the relative complexity of DES vs. a simple code method of conditional access.


EXPLAIN AND REMIND THE STUDENTS TO CONTINUE TAKING NOTES IN THEIR WORKBOOK ON WB 7.10-7.11

Security Provided by DES

Tell the class that the security provided by DES is dependent on the following parameters:

- Mathematical soundness of the algorithm
- Length of the key
- Key management
- Mode of operation
- Implementation

Explain that modifications of the DES methodology decrease its security and are not in accordance with the standard.

Public Keys

Tell the class that public key encryption:

- Simplifies the management of encryption keys.
- Provides additional functionality for applications such as digital signatures for use in electronic commerce.
- Tends to be more secure than secret keys because of improved management of:
  ◊ Key creation
  ◊ Key protection

EXPLAIN

Explain to the class that the disadvantage of the secret key system is that the key is distributed to many parties.

- The probability increases of illegal copies of the key existing.
Explain that public key encryption does not distribute multiple copies of the same key.

- It employs a combination of two keys, called:
  ◦ The public key
  ◦ The private key
- To decrypt the data, the encryption algorithm requires both keys to match.
- What one key encrypts the other decrypts.
- Typically:
  ◦ The public key encrypts.
  ◦ The private key decrypts.

The process of public key encryption can be explained in stages:

Stage 1
- Each end system generates a pair of keys to be used for the encryption/decryption process.

Stage 2
- Each end system publishes its public encryption key.
- The key is placed in a public register or file which generates a “certificate” that:
  ◦ Binds the end systems name to its public key through a digital signature
- This process is specified in ITU-T X.509.
- The authorized user stores the companion private key.

Stage 3
- A service provider transmitting messages to a subscriber will encrypt the messages using the subscriber’s public key.

Stage 4
- The subscriber’s set-top decrpts the encrypted message using its private key.
- The private key is typically stored:
  ◦ In the set-top terminal
  ◦ In a removable card

Identify stages of encryption on VA 7.3
Examples of end systems are headend IRDs or IRTs and digital set-tops.

Digital signatures will be covered later in this guide.
EXPLAIN

Explain that the public key encryption algorithm is called a “trap door, one way function.”

- Encryption with the public key is easily done.
- Decryption without the private key (the trap door) is difficult.

A one-way function is easier to perform in one direction than in the other, unless the trap door is available.

DISCUSS

Tell the class that digital envelope protocol is a variation of the public key system which allows message encryption by a combination of:

- Public key encryption
- Secret-key cryptosystem

Refer the class to the example in the DigiPoints text.

EXPLAIN AND REMIND STUDENTS TO NOTE IN THEIR WORKBOOKS, WB 7.14.

An example is shown in DigiPoints.

Explain that the main advantages of the digital envelope protocol are:

- The high-speed of a secret key system
- Key management convenience of public key encryption

Point out that the PowerKEY™ Conditional Access System is a commercial example of the digital envelope protocol.

PowerKEY™ is owned by Scientific-Atlanta.

The secret keys are called control words.

- Control words provide the first level of encryption by operating on the content part of MPEG-2 video, audio or data streams.
  - Change rapidly to increase system security
  - Are accessed by the use of mid-level keys called multi-session keys
- Multi-session keys are transmitted to the set-top decoders on MPEG-2 Entitlement Management Messages (EMMs), that are encrypted by public keys.
  - An RSA public key algorithm generates the public keys.
  - The set-top decoders use private keys to access the multi-session key within the EMM.

EMMs were discussed in Module 5.

RSA is discussed next as a sidebar.
EXPLAIN

REFER STUDENTS TO THEIR WORKBOOKS, WB 7.15-7.17 AND TO THE APPENDIX TO CHAPTER 7 IN DigiPOINTS, VOLUME 2.

APPENDIX: What is RSA?

Tell the class that RSA is:

- A public-key cryptosystem used for both:
  - Data encryption
  - Data authentication
- Becoming the de facto standard in the CATV industry
- Adopted by:
  - Scientific-Atlanta for use in its PowerKEY™ system
  - CableLabs® as the core of its multilayer security network security architecture

EXPLAIN

Tell the class that the RSA cryptogram is based upon coefficients of equations that are part of the RSA algorithm.

- The keys are pairs of these coefficients.
- The public key is one pair of coefficients:
  - Stored in a public registry
- The private key is another pair of coefficients:
  - Accessed only by the authorized user
- The coefficients that are the public and private keys are used in another equation that includes the strings of binary numbers being encrypted.
- The result of the second equation is the encrypted message.
- Decryption is a similar process, using the coefficients of the keys in an equation that includes the encrypted message.
- The process of determining the coefficients can be performed by a computer due to its complexity.
- Once the coefficients are determined RSA can be used for:
  - Data Privacy
  - Data Authentication
- Encryption and decryption occurs without any sharing of private keys.

Note that this material is in the appendix to Chapter 7.

An example of the way these coefficients are chosen is provided for students with advanced mathematical background in the DigiPoints text.
• Each participant only requires:
  ◊ Other participant’s public key
  ◊ Their own private key
• Messages can be sent using only public keys, however:
  ◊ Only the corresponding private keys can:
    • Decrypt the message (for privacy application)
    • Sign the message (for digital signature application)
• Examples of RSA privacy encryption and digital signature generation are provided in the Workbook and in the *DigiPoints, Volume 2*, Sidebar.

Instructor Note: Tell the students that the example uses an advanced mathematical operation called “modulus” (mod for short). Show how mod works by the example $7 \mod 3 = 1$. The answer, 1, is the remainder of 7 divided by 3.

**EXPLAIN**
**DISPLAY VA 7.4**
**REFER TO WB 7.18**

**Digital Signatures**
Tell the class that digital signatures:
• Have been developed to protect data exchanges from fraud.
  ◊ When two parties share a secret key, one party can forge a message from the other, encrypt it with the secret key and claim it originated from the other party.
• Electronic banking and commerce are emerging applications where account information could be fraudulently altered.
• The digital signature:
  ◊ Verifies author, date and time of signature
  ◊ Authenticates data contents at time of signature
  ◊ Is verifiable by third parties to resolve disputes
• There are several ways to generate a digital signature. These will be discussed below.

**Point out that all messages are strings of 1s and 0s, which the algorithm treats as binary numbers, rather than binary code representing other information.**

**The examples of encryption and decryption using RSA are given in the workbook for students with advanced mathematical background.**
Digital Signatures Using Public and Private Keys

Tell the class that the creation of the digital signature is based upon the reversal of the order in which the public and private keys are typically applied to the algorithm.

- User A transmits an encrypted message using its own private key.
- User B decrypts the message, using User A’s public key.
- The encrypted message serves as User A’s digital signature since:
  - Only User A could have generated this data stream.
- Data is authenticated since the message cannot be altered without access to User A’s private key.
- RSA encryption is an example of this type of digital signature.

Explain that implementing a digital signature in this manner requires that three copies of the entire message must be stored:

- One in plaintext for each party’s use
- One in ciphertext to allow for:
  - Verification of original contents in case of dispute

Point out that the disadvantages of this method are:

- Increased storage requirement over documents without digital signature
- Reduced data security as:
  - Anyone can decrypt the message, using User A’s public key.
DISCUSS

Tell the class that security can be increased by employing a variation in the method above.

- Encrypt the message with User A’s private key.
- Encrypt again with user B’s public key.
- Only a user who has access to both User A’s private and public keys can decrypt the transmitted ciphertext.
- The main disadvantage is that the use of the encryption/decryption algorithm is increased from two to four times during communication.

Discuss tradeoffs of simplicity and security.
EXPLAIN

Other Methods of Generating a Digital Signature

Explain that the digital signature can be generated by:

- Creating a message authentication code by applying special algorithms such as:
  - A one-way hash function
  - The MD5 message digest algorithm

In each of these methods, only the message code or message digest is computed.

- Less storage required
- Decreased security

WORKBOOK EXERCISE #2, WB 7.20

Refer students to workbook exercise #2. Review answers as a group.

Details of these algorithms may be found in Data and Computer Communications, 5th Edition, by William Stallings.

Allow ten minutes for completion of exercise.
OpenCable™ Standards For Conditional Access

Encryption/decryption used for conditional access can be done either by:

- Circuitry that is an integral part of the components of a digital system, or
- Circuitry on removable cards that are inserted into the component

Retail distribution of set-top terminals favors removable cards. Smartcards have been used for security in satellite receivers.

- Smartcards are a type of removable card.

Point of Deployment (POD) modules are a new standard for removable cards.

- Specified by CableLabs OpenCable™ initiative
- Are a type of PC card

OpenCable’s objective is to promote set-top interoperability through specifications covering interfaces.

- Host – POD
- Headend and host
- Host devices and consumer devices

Host - POD interface specification

- Is called the OpenCable™ Host – POD Interface Specification, IS-POD-131-INT01-991027
- Includes all security functions, and out-of-band signaling functions
- Enables any OpenCable compliant device to deliver a cable system’s secure digital video services.

Refer to the Chapter 7 Appendix for details of smartcards.

Host-POD interface specification sources:

- SCTE DVS 064
- SCTE DVS 085
- SCTE DVS 131
- SCTE DVS 167r1
- SCTE DVS 178r1
• Evolved from several standards
  ◊ SCTE DVS 064, which specifies a National Renewable Security Standard
  ◊ SCTE DVS 085, which specifies Basic Security Tools for DAVIC 1.0. SCTE DVS 085 specified a POD with two interfaces: a CA0 interface between a set-top terminal and a removable security device, and a CA1 interface between the security device and a smartcard
  ◊ SCTE DVS 131, the Point of Deployment (POD) Module Interface Proposal
  ◊ SCTE DVS 167r1
  ◊ SCTE DVS 178r1

• Implemented by a layered protocol
  ◊ Physical layer protocol is implemented in both the host and POD module.
  ◊ Data link and MAC protocols are implemented in the POD module only.

• Division of processing and signaling allows the differences between manufacturers to become POD module implementations.
  ◊ The host can be used with several vendor implementations of POD modules.
  ◊ RF processing and QPSK demodulation and modulation are done in the host.
  ◊ Remainder of the processing, including processing of conditional access messages, is done in the POD module.

• Types of host-POD interfaces:
  ◊ Standardized bi-directional access to an out-of-band RF front end
  ◊ Inband MPEG-2 transport stream input and output
  ◊ CPU interface

DISPLAY VA 7.5

Point out the system illustrated in VA 7.5 shows a host with both QPSK and DOCSIS returns, allowing for potential relocation of the receiver to systems not equipped for DOCSIS return.
- Two types of host modem:
  ◊ QPSK
  ◊ High-speed data (DOCSIS)
- Use of either RF or telephony return path signaling

- An extended channel specified in the interface between the POD module and the host supports delivery of IP packets across the POD interface.
  ◊ Supports applications such as web browsing, or pay-per view reportback

Refer to CableLabs specification IS-POD-131-INT01-001027 for further details of the interface.

EXPLAIN
REFER TO WB 7.25

Appendix: Smart Cards
Tell the class that a smart card is:
- An integrated circuit embedded into a credit card sized plastic card
- Different from a conventional magnetic stripe card in that:
  ◊ It offers more functionality
  ◊ Data security is greater
- The integrated circuit:
  ◊ Stores information in electronic form
  ◊ Controls use of information
- There are two types of smart cards:
  ◊ Intelligent
  ◊ Memory
- An intelligent card contains a central processing unit that:
  ◊ Stores and processes information
- A memory card contains storage capacity that:
  ◊ Holds a value which can be “spent”
- Smart cards can be either:
  ◊ Contact
  ◊ Contactless
  ◊ Combination

Central Processing Unit = microprocessor.
• Contact smart cards are inserted into a card reader.
  ◊ Reads and writes to and from the integrated circuit occur when an electrical connection is made between the card reader and a plate on the face of the card.
  ◊ Power for the integrated circuit can be supplied via contacts on the smart card.

• Contactless smart cards perform data communication between:
  ◊ An internal antenna and integrated circuit
  ◊ A receiving antenna at the transaction point

• Combination card functions as both contact and contactless cards.

• In a CATV system, the intelligent smart card is used:
  ◊ To store parameters to build an encryption/decryption key
  ◊ As a debit card for Pay Per View events
The Harmony Agreement

Tell the class that the Harmony Agreement was created to allow operators to “mix and match” digital video components from different vendors.

- Both Motorola and Scientific-Atlanta are part of this agreement.
- Both companies will produce products under the following open standards:
  - MPEG-2 Video
  - Dolby Digital Audio
  - MPEG-2 Transport
  - ATSC System Information
  - ITU-J83B Modulation
- The Harmony Agreement is:
  - Endorsed by CableLabs
  - Incorporated into SCTE digital standards
- Under the Harmony Agreement:
  - SA will use Motorola core encryption algorithm which is based on the DES.
  - Operators will not have to duplicate transmission of programming and content to implement dual Conditional Access.
  - Vendors will be able to use their own Conditional Access technology as another layer of encryption.
- The POWERKEY™ system is an example.
Practical Digital: The Role of the Technician

Discuss
Refer to WB 7.27

Tell the class that:

- In analog systems, filters and interdiction are used to block premium channels.
- In digital systems, digital encryption and decryption is built into the cable system.
  ◊ The only visible component of the system may well be the POD module.

Refer to WB 7.30-7.31

Complete Lab 1 in the Workbook, if set-top terminals and POD modules are available.
Summary

In summing up, tell the class that:

• Conditional Access is a vital part of a digital system that has evolved from operating as a security measure that benefits only the cable operator to being an integral component in protecting subscriber data in emerging applications such as:
  ◊ Pay per view
  ◊ Electronic commerce
  ◊ Work at home local area networks

• Encryption is a vital part of Conditional Access.

• Central to the encryption process is the key, which may be:
  ◊ Secret
  ◊ Public

• Secret keys are:
  ◊ Shared only by each party involved in the data transmission
  ◊ More susceptible to security breaches

• In a public key system:
  ◊ Improved security occurs when a combination of both public and private keys are utilized.
  ◊ Decrypting a message requires both the public and private keys.
  ◊ This private key is not shared.

• Digital signatures are a companion technology to encryption that verifies both:
  ◊ The sending party
  ◊ The message content

• However, digital signatures add processing overhead.

• Cable telecommunications standards for Conditional Access have been specified by the CableLabs OpenCable™ specifications.
Wrap Up

Ask students to complete the Test Your Knowledge section, Workbook Exercise #3.

Review answers as a group.
Appendix

Workbook Exercise # 1

Complete Workbook Exercise #1 by labeling the components in the diagram of a digital system where Conditional Access processes occur as your leader identifies them.

Instructor note: The components named below have been blanked out in Figure 1 of the student’s workbook.

Component names:
- Digitization center
- IRT
- IRD
- Out-of-band Modulator
- Set-top decoder
Workbook Exercise # 2

Write a short description of the following Conditional Access keywords. Answers are taken from Learning Enough to be Dangerous: Glossary

**Ciphertext** – The result of a cipher encryption of a message.

**Conditional Access** – Control mechanisms, data structures and commands that provide for selective access and denial of specific services.


**Digital signature** – Grouping of data that only one entity can produce, but which all others can verify with the sender’s public key.

**Plaintext** – Content of an unencrypted message.

**Public key** – Algorithms that encrypt and decrypt using different, but mathematically linked, keys.

**Secret key** – Key used in symmetric algorithms that encrypt and decrypt messages. A secret key is shared by each party to the data.

**Smart card** – Credit card size device with embedded memory and/or processor.
**Workbook Exercise # 3**  
*Answers to the questions at end of student workbooks.*

1. Name five emerging applications of conditional access in a cable telecommunications system, and indicate what benefits accrue to the subscriber and to the operator as a result of CA in these applications.

<table>
<thead>
<tr>
<th>Application</th>
<th>Subscriber Benefits</th>
<th>Operator Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>High-speed Data Access via Cable Modem</td>
<td>Allows the subscriber to access sensitive or confidential corporate computer data from home or another location away from work.</td>
<td>Work at Home and Small Office/Home Office are attractive markets which can only be served if the customer is satisfied data is secure.</td>
</tr>
<tr>
<td>Electronic Commerce</td>
<td>Convenience of conducting many transactions by computer terminal at home</td>
<td>This is a growing market that can include new applications for set-top terminals as well as for cable modems.</td>
</tr>
<tr>
<td>Subscriber Identification and Digital Signature</td>
<td>Provides a way to have the remote equivalent of a signed document.</td>
<td>Allows the operator to offer many versions of electronic commerce.</td>
</tr>
<tr>
<td>Protection of System Software and Downloads from the Headend to the Digital Set-Top Terminal</td>
<td>The subscriber is not inconvenienced by the need to be at home specifically to let an installer into the house when the changes are made.</td>
<td>Allows the operator to add features to set-top terminals and fix “bugs” without a truck dispatch.</td>
</tr>
<tr>
<td>Multiple Service Providers in a Single Network</td>
<td>Provides a way to get more applications from more sources. Also, is a way to facilitate retail sales of set-top terminals.</td>
<td>May make it easier to get into new markets.</td>
</tr>
</tbody>
</table>
2. What is the difference between a code and a cipher?

*The code method is the simpler of the two. The parties who will be exchanging data each keep a table of letters, words, or phrases, which are substituted for those in the original message. Although the code method is simple to implement, it has the disadvantage that the code is fixed, must be stored in either machine or human memory, and must be shared by all parties using it. This makes breaking the code relatively easy.*

*The cipher is a more complex method of encryption, and is usually more secure than a code. A cipher uses a mathematical formula (algorithm) to change a stream of message bits into an unintelligible cryptogram. Because of their mathematical basis, ciphers can be easily generated by computer processors.*

3. In encryption, what is a key, and how is it used?

*The key is a short bit string that controls the output of the algorithm used for encryption (e.g., by providing a value for a variable in the algorithm).*

4. What is the shortcoming of a secret key encryption system, and how is the shortcoming overcome in a public key system?

*Because the keys in a secret key system are kept and shared by all parties who use the system, security can become a problem. A public key system uses two types of keys: a public key and a private key. The public key is given to anyone who needs to communicate with the receiving party, and is used to encrypt the message. The private key is only held by the receiving party, and must be used to decrypt the message. Because the private key is not distributed beyond the intended receiving party, it tends to be more secure.*

5. What is DES?

*DES is the Data Encryption Standard issued by NIST (the National Institute of Standards and Technology, formerly the National Bureau of Standards) in 1977 to provide an encryption algorithm for use in protecting federal unclassified information from unauthorized disclosure or undetected modification during transmission or while in storage. It is a published, secret-key standard, which is widely used for data encryption.*
6. What characteristics must be part of a digital signature?

A digital signature has the following properties:
- It verifies the author, the date, and the time of the signature
- It authenticates the contents at the time of the signature
- It is verifiable by third parties to resolve disputes.

7. What are the two interfaces specified by the DVB MultiCrypt approach to conditional access?

The CA0 and the CA1 interfaces.

8. What is the difference between a PC card and a smart card? Where do each fit into a cable telecommunications conditional access system?

A PC card is an interface card that plugs into an electronic device such as a personal computer or digital set-top terminal. It contains electrical contacts that make contact with internal connections in the electronic device.

A smart card is a credit card sized plastic card with a special type of integrated circuit embedded into it. These cards are different than conventional magnetic stripe cards, in that they have more capabilities and data is far more secure. The integrated circuit holds information in electronic form and controls the information's use. It includes memory that can hold stored monetary or other values, information about the user, or entire applications.

In the DVB specification for conditional access, the CA0 interface is the interface between the conditional access device (PC card) and the set-top unit. In the DVB specification for conditional access, the CA1 interface is the interface between the conditional access device (PC card) and a smart card.
9. You are a technician in a cable system that uses a digital set-top terminal equipped with a smart card interface for conditional access. During a visit to a customer’s house to fix an unrelated problem, the customer informs you that he cannot get Video-On Demand, for which he supposedly subscribes. What could be some causes of the problem?

*If the system uses a smart card as part of the conditional access system, the subscriber may have inserted the card incorrectly, or used someone else’s smart card. Sometimes, the subscriber may even attempt to use a conventional credit card as the smart card!*
Laboratory Exercise #1

Scope
This laboratory exercise is intended to allow the student to participate in the installation and operational issues that are associated with conditional access systems currently in use at system headends or at the training facility.

General Introduction
Conditional access systems make use of signal security which is any technology, such as encryption, that can prevent a signal from being received except by authorized users. Several parts of a digital system are involved in implementing Conditional Access.

Instructor note: Relate the key components identified in Visual Aid, VA 7.2 – Digital System with Conditional Access, to the actual conditional access system in use at the headend or lab facility.

The key components are identified in VA 7.2 – Digital System with Conditional Access.

- Digitization center
- IRT
- IRD
- Out-of-band Modulator
- Set-top decoder

The physical implementation of the encryption/decryption process at the set-top decoder is performed by integrated hardware or by removable cards. The removable card approach is generally known as renewable security because it is easily removed and replaced when necessary due to upgrades or fixes to a security breach.

In this laboratory, we will concentrate on the encryption processes that occur at the subscriber’s residence. The laboratory is written with the assumption that a “mini-cable” system is available at the headend or laboratory facility (i.e., the leader or instructor will have access to a video source, video encoder, channel modulator, set-top decoder and television to facilitate the laboratory exercises below).

Instructor Note: Some of these tasks may not be applicable to the conditional access system implemented at this location. Consult the headend personnel to choose appropriate tasks for the laboratory.

---

1 Definition from Scientific-Atlanta’s Glossary of Encryption Technology.
1. **Physical dimensions/constraints of the POD module**
   The instructor will pass around an example of a POD module. Physically examine it and discuss its use.

2. **Host interface to the POD module**
   The instructor will provide a set-top terminal with an OpenCable-compliant POD interface. Locate the interface on the terminal and discuss any design constraints that may impact the installer or customer.

   Instructor Note: Discuss constraints such as: slot location and procedure for insertion/removal of the card and why they may have been incorporated into the design.

   Instructor Note: Some design constraints are intentional. For example, the manufacturer or operator may have located the interface at the rear of the set-top terminal to physically remove it from the buttons and indicators intended for customer use.

   Instructor Note: Exercises 1 – 5 focus on the consequences of improper use of the POD module either by the installer or by the customer. Due to their similar nature, these could be performed as a single exercise.

   Initially perform the remaining tasks as a demonstration. Then select one or two students from the class to perform the same tasks.

3. **Attempted set-top operation without POD installed**
   Application: Improper installation or customer use of smart card/decoder.

   Outline:
   Following local set-up procedures, the instructor will apply power to the system. Verify system is operational and authorized video is displayed on the TV/monitor. Remove the POD module. Determine functionality of the system.

4. **Attempted set-top operation with improperly installed POD module**
   Application: Improper installation or customer use of POD module.

   Outline:
   Following local set-up procedures, the instructor will apply power to the system. Verify system is operational and authorized video is displayed on the TV/monitor. Remove power. Remove the POD module and then attempt to install in an improper manner such as upside down or reversed. Discuss preventative measures that are part of the equipment design to prevent improper installation.
Instructor note: Simulate attempted improper installation. Show the difficulty in fitting the card into the equipment incorrectly and highlight the cause (slot on card, pin location, etc.)

5. **Attempted set-top operation with invalid POD module**

Application: Improper installation or customer use of POD module.

Outline:

Following local set-up procedures, the instructor will apply power to the system.

Verify system is operational and authorized video is displayed on the TV/monitor.

Remove power.

Remove the POD module and install a different PC card.

Re-apply power.

Determine functionality of the system.

Instructor note: Explain that not all PC cards are identical. Internal circuitry is specific to the application.