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

Module Objectives
Upon successful completion of this module, the student 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
Read DigiPoints, Volume 2, Chapter 7.

As you complete this module, you should be filling in answers and definitions for the items found on the following pages.
Module 7 – Conditional Access and Security

Take notes on the following pages as your instructor covers the topics in this session. For some topics, key points are identified. You should add to them with supplementary information from the class discussions. For other topics, you will need to fill in key points as requested in the workbook.

Constructing meaningful notes in this way helps you to understand the subject and can serve as a valuable future reference.
What is Conditional Access?

Conditional Access is the control mechanism, data structure and commands that provide for selective access and/or denial of specific services.

Complete this definition as provided by Scientific-Atlanta’s *Glossary of Encryption Technology*: Conditional Access systems make use of signal security.

Implementation of Conditional Access in a digital system may include several encryption/decryption processes.
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 instructor identifies them.

Figure 1
Digital System with Conditional Access

[Diagram of a digital system with Conditional Access processes, labeled with components such as Satellite, Headend, Subscriber Premises, etc.]
CA Applications

Traditionally, Conditional Access has been used in the CATV industry to prevent signal piracy of premium services.

In analog systems, the video synchronization pulse is modified, rendering the video signal “unintelligible” to unauthorized viewers.

Two-way digital systems have introduced new and alternate applications.

List the key needs for security which conditional access solves for each of the following applications.

High-Speed Data Access via Cable Modem

Electronic Commerce

Subscriber Identification and Digital Signature
Protection of Software and Downloads from the Headend to the Digital Set-Top Terminal

Multiple Service Providers in a Single Network
How Conditional Access Works

Encryption of data is accomplished by either a code or a cipher.

List the key points of each method and their advantages and disadvantages.

Code method

Cipher Method
Secret Keys

In conventional encryption, the secret key is common to both encryption and decryption processes.

The ciphertext is transmitted to the intended receiver, who applies the key to a decryption algorithm. The result is the original plaintext message.

The secret key makes the encryption unique.
The output of the encryption/decryption algorithm is dependent on the secret key.

What does the data security depend on?
Data Encryption Standard (DES)

DES is an example of a secret key encryption process.

DES was established in 1977.

DES prevents the unauthorized disclosure or undetected modification of data during data transmission or storage.

DES is a publicly owned cryptographic algorithm.

A secret key performs the conversion of plaintext to ciphertext.

Both the encryption and decryption processes employ the same algorithm and secret key.

What is the bit size of this key?
Complete this sentence: The goal is to completely scramble the data and key so that…

Employing a different secret key will produce a different encrypted data stream (ciphertext).

List the parameters that determine the security provided by DES.
Public and Private Keys

Public keys simplify the management of encryption keys.

List the advantages of public key encryption over secret key encryption.

Public key encryption employs a combination of two keys, a public and a private key.

To decrypt the data, the algorithm requires that the public key and private key “match.”
Figure 3 (VA 2.7.4) below, summarizes the public key encryption process.

![Figure 3](Encryption Using a Public Key)

The process can be partitioned into four stages. Describe each stage.

Stage 1

Stage 2

Stage 3

Stage 4
Digital Envelope Protocol

Digital Envelope Protocol is a variation on the public key system that employs a combination of the public key system and the secret key cryptosystem. List the advantages of this method.

PowerKey™ is a commercial example of digital envelope protocol.

The secret keys are called control words that encrypt the content of the MPEG-2 video stream.

The control words are changed rapidly to provide additional security.

Access to the control word is achieved via mid-level, multi-session keys.

Public keys generated using the RSA public key algorithm encrypt EMMs that contain the multisession keys.

The decoder receives the EMMs containing the multi-session keys and decrypts them using private keys.
RSA

RSA is a public-key cryptosystem that is used for both data encryption and data authentication.

Evolving to become the de facto standard in CATV industry.

Examples of RSA use for data encryption and data authentication are shown on the next page.

Data authentication is also known as a digital ____________________.
An example of RSA privacy encryption

Let Alice’s computer send a message, \( m \), to Bob.

Alice’s computer generates the ciphertext, \( c \), by processing the following equation:

\[ c = m^e \mod n \]

where,

\( m \) = original message
\( e, n \) = Bob’s public key, generated by the encryption algorithm

Mod is a mathematical operation called modulus. The result of using it is the remainder generated when one of its operators is divided by the other.

Alice transmits \( c \) to Bob.

Bob recovers the original plaintext message \( m \) by processing the following equation:

\[ m = c^d \mod n \]

where,

\( c \) = ciphertext
\( d, n \) = Bob’s secret key, also generated by the encryption algorithm

Since only Bob knows \( d \), only Bob can decrypt.

An example of RSA authentication

Let Alice send a message to Bob, where Bob is assured that the message is authentic.

Alice’s computer generates a digital signature, \( s \), by processing the equation:

\[ s = m^d \mod n \]

where,

\( m \) = the original message (plaintext)
\( d, n \) = Alice’s private keys

Alice transmits \( m \) and \( s \) to Bob.

To authenticate the signature, Bob’s computer processes the following equation:

\[ m = s^e \mod n \]

where,

\( m \) = original message
\( s \) = digital signature
\( e, n \) = Alice’s public keys
Anyone can send an encrypted message or verify a signed message using only public keys but only someone in possession of the correct private key can decrypt or sign the message.
Digital Signatures

Digital signatures have been developed to protect data exchanges from potential fraud.

List the properties of a digital signature:

There are many ways to generate a digital signature; one such method is illustrated in Figure 4.

---

**Figure 4**
Simple Digital Signature Process
Digital Signatures using Public and Private Keys

This method of creating a digital signature is based on the fact that the algorithms that use the combination of public and private keys allow the keys to be used in any order.

An example:
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.

List the advantages and disadvantages of this method.

Improved security can be obtained if the encryption scheme above is used twice as follows.
Encrypt the message with User A’s private key.
Encrypt again with user B’s public key.
Only a user who has access to User A’s private and public keys and User B’s private key can decrypt the transmitted ciphertext.

Identify the main disadvantage in this method.
Workbook Exercise # 2

Write a short description of the following conditional access keywords:

Cipher –

Ciphertext –

Conditional Access –

DES –

Plaintext –

Public key –

Secret key –
OpenCable™ Standard 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 by circuitry on removable cards that are inserted into the component.

Smartcards have been used for security in satellite receivers.

Are Smartcards removable or integral components of a system?

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

Specified by CableLabs® OpenCable™ initiative.

A type of PC card

What is the difference between a Smartcard and a PC card?
The OpenCable™ objective is to promote set-top interoperability through specifications covering the following interfaces.

**Host – POD**

Headend and host

**Host devices and consumer devices**

**Host - POD interface specification**

- 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 systems’ secure digital video services
- 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
    - 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

How does this make it easier to offer set-top terminals as retail consumer products?

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
- In-band MPEG-2 transport stream input and output
- CPU interface
Two types of host modem

- QPSK
- High-speed data (DOCSIS™)

Use of either RF or telephony return path signaling.

An extended channel is 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.
Smart Cards

A smart card is a credit card sized plastic card with an embedded integrated circuit.

It offers greater functionality and increased data security over a conventional magnetic stripe card.

There are two types of smart card. List the key points of each.

Intelligent

Memory

Smart cards can be Contact, Contactless or a combination of both.

List the key points of each.

Contact

Contactless
The Harmony Agreement

The Harmony agreement exists among set-top vendors to provide a common interface to allow operators to build systems with inter-working components from different vendors.

Motorola and Scientific-Atlanta have agreed to manufacture products based on a set of five open standards.

List each standard.
Role of the Technician

In analog systems, filters and interdiction are used to block premium channels.

In digital systems, the digital encryption/decryption processes are built into the cable system.

From a field perspective, digital conditional access is a relatively quiet area.

The technician’s main responsibilities will occur during and after installation. List these responsibilities.
Workbook Exercise # 3

Testing Your Knowledge

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.

2. What is the difference between a code and a cipher?

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

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

5. What is DES?
6. What characteristics must be part of a digital signature?

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

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

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?
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.

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 instructor will have access to a video source, video encoder, channel modulator, set-top decoder and television to facilitate the laboratory exercises below).
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 interfaces 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.

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.
Glossary

CA0 interface – In the DVB specification for conditional access, the interface between the conditional access device (PC card) and the set-top unit.

CA1 interface – In the DVB specification for conditional access, the interface between the conditional access device (PC card) and a smart card.

Certificate – Documentation that verifies the validity and integrity of published public keys.

Cipher – Process that uses a mathematical formula to change a stream of message bits into an unintelligible cryptogram.

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 service.


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

DVB – Digital Video Broadcasting Group

Electronic commerce – Secure exchange of funds for goods and services over an electronic network between parties who may not have a prior relationship.

FIPS – Federal Information Processing Standard

PC card – Circuit card originally developed to be inserted into a personal computer in a special slot, and which provided functions such as modem, hard drive, etc. Originally called a PCMCIA card.
Plaintext – Content of an unencrypted message.

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

Renewable security – Part of a conditional access system which is easily changed.

RSA – Public key algorithm. Also the name of the firm which owns the algorithm.

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.