

REPORT 1079-1

GENERAL CHARACTERISTICS OF A CONDITIONAL-ACCESS BROADCASTING SYSTEM

(Question 37/11)

(1986-1990)

1. Introduction

The present Report presents principles for conditional-access systems worked out by the EBU for application to satellite television by France and the United Kingdom, where the principles have been applied to teletext services. Some details of these applications are given in Table I at the end of the Report.

The principles may also be applied to conventional television and sound broadcasting systems as well as to additional services other than the teletext services listed in Report 802.

2. Components of a conditional access system

There are two distinct and in many cases independent components:

2.1 Scrambling*

This is the process of rendering a service of no value to unauthorized users by changing certain of its characteristics under the control of the conditional access system at the sending end.

2.2 Access control*

This is the provision of information to enable authorized users to descramble the service. The availability of this information is controlled by transmitting it in encrypted* form.

3. The requirements to be satisfied by a conditional access system**3.1 Security**

The security of the system is the degree of difficulty encountered by an unauthorized user in attempting to gain access to the service.

There are two aspects:

- descrambling the signal without reference to the access control process. This is a function of the nature of the services and the scrambling method;
- obtaining the access control key* in an unauthorized manner. This is a function of the security of the algorithms used and the method of key distribution.

3.2 Access modes

A conditional access system will be more effective if there is a range of access modes.

Examples are:

- period availability – authorization runs from a starting time to a finishing time;
- programme or service item – availability is for a specific service item, whether or not it is completely used;
- service charge (commonly called “pay per view”) – the charge or use of credit is proportional to the duration of use and/or the value of the service involved.

* See Annex I for definitions.

The access modes need to be variable with respect to several parameters, for example:

- time;
- various segments of the service;
- groups of intended users.

3.3 *Equipment standardization*

To provide maximum economy of manufacturing scale for receiving equipment and to simplify management and maintenance:

- common equipment should be standardized so that it can cater for as many service options as possible;
- the “secret” components should be within a secure module with a standardized interface**.

3.4 *Access management*

The definition of conditional access is based on the formal concept of *entitlement* to access, which can be implemented in various forms. An entitlement gives to its holder an *authorization* to access the related service.

3.5 *Avoidance of impairments to the service*

Three types of impairment are significant:

- impairment to the finally available service due to the scrambling/descrambling process;
- impairments due to faulty or unreliable acquisition of the access control data;
- uneconomic use of the resources due to the management or transmission overheads involved.

3.6 *Interaction with digital processing*

It should be noted that certain scrambling processes may conflict with some operations of digital signal processing techniques, for instance bit-rate reduction.

4. **General description of a conditional access system**

4.1 *General*

Conditional access requires that the information must be *scrambled* before it is broadcast. This process is under the control of a scrambling sequence obtained from a *pseudo-random generator*.

The descrambling process at the receiving end requires the same sequence (in this case the descrambling sequence) to recover the original signal.

To provide this sequence and to ensure synchronism between the sending and receiving processes, the starting condition of the pseudo-random bit stream generator is controlled by an *initialization word*.

** This subject has already been discussed in the EBU in connection with the specifications for conditional access for the broadcasting-satellite service (BSS) (see Report 1073).

To achieve security, access-related information permitting recovery of the initialization word is transmitted in an encrypted form, according to the access modes in use (see Fig. 1). The detailed structure of this process is given in Fig. 2 and in the following sections.

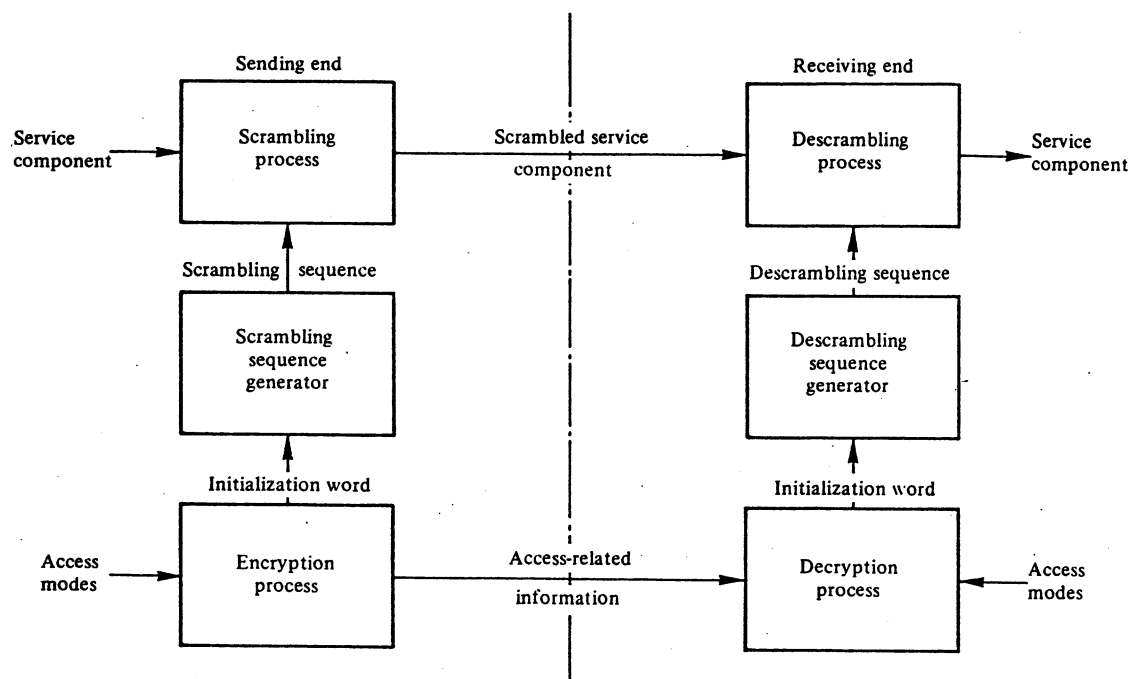


FIGURE 1 – Basic conditional access system

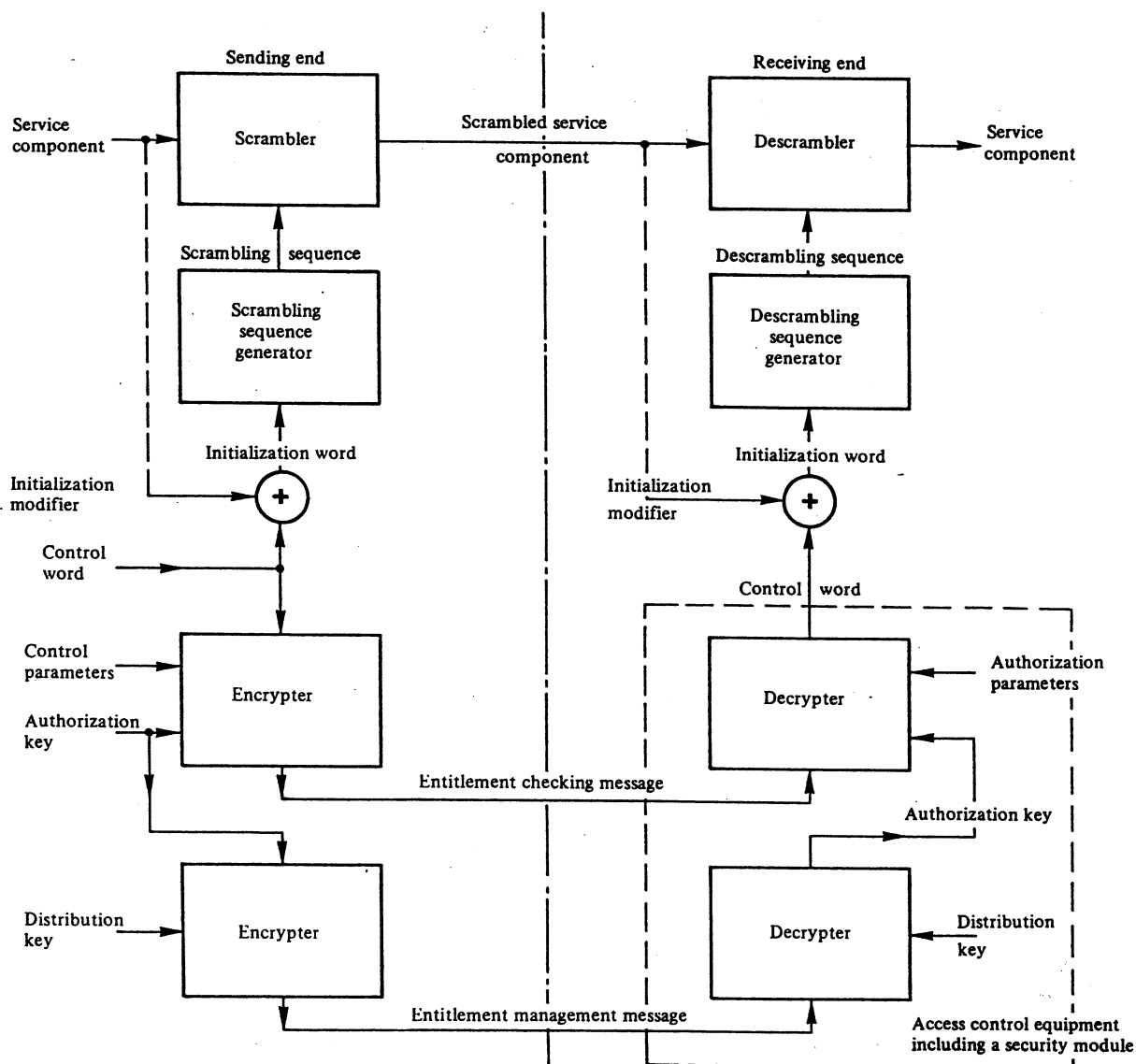


FIGURE 2 – Functional description of a conditional access system

Note. – Two encrypters and decrypters are shown in this figure for clarity. In practice, only one of each may be necessary if the encryption algorithm controlled by the authorization key and the one controlled by the distribution key are the same.

4.2 Initialization word

Conditional access to a service component is in fact equivalent to conditional access to the initialization word, which has two components: the *control word* and the *initialization modifier*.

4.3 Control word

The control word is the basic element of security. Its value is chosen arbitrarily and it may be changed during the service operation to enhance security.

The control word is communicated to the receiver as follows:

- at the sending end, according to the access mode in use, an encryption algorithm supplies encrypted versions of the control word, which are transmitted in special records. These are the *access entitlement checking messages*;
- at the receiving end, the access control equipment applies the inverse algorithm to regenerate the control word.

4.4 Initialization modifier

The initialization modifier is used in order to impose sufficiently short scrambling sequences to provide security, while avoiding the need for too frequent calculation of the control word. Thus, the use of different initialization modifiers for each structural unit of scrambled information causes the initialization word to change sufficiently frequently.

4.5 Control word index

To operate a segmented service, it is necessary to manage several related control words. These are identified by means of *indices*. The control word index used to access a unit of scrambled information must be obtainable from the transmitted signal.

5. Access entitlement checking messages

Each of these messages comprises:

- the control word index;
- a control word change flag: a change of state indicates a change of value of the control word;
- an *authorization pointer* which identifies the authorization key located in the receiver security module to which the message is addressed;
- a *control parameter* which supplies value (e.g. date, price, etc.) for comparison limits set to these values, in the receiver security module, called the *authorization parameters*;
- the encrypted control word.

In order to descramble a unit of information, the receiver must previously have acquired the control word from an access entitlement checking message bearing the appropriate index.

For optimum efficiency, access entitlement checking messages relating to the same control word but corresponding either to different user groups or to different types of access control equipment should be grouped under the same index. Although this is not its only application, the indexing system described above enables the advance transmission of entitlement checking messages.

The conditional access equipment creates a table of active control words which is updated by the access entitlement checking messages independently of the scrambled data. To identify the correct control word, the descrambling device supplies the access control equipment with the corresponding index. The management of this table is a part of the facilities provided at the interface between the descrambler and the access control equipment.

6. Access entitlement management messages

The processing of an access entitlement management message validates or provides the entitlement. This process takes place within the security module associated with a cryptographic calculation involving a *distribution key*. This distribution key is used to encrypt and decrypt messages and/or authorization keys addressed to individual receivers. The corresponding cryptograms constitute the validation signal and are carried as part of the access entitlement management message.

In conditional access broadcasting systems, the access management messages may be broadcast. This is known as "over-air addressing". The cycle time associated with the distribution of over-air keys may be significantly reduced by the application of the principles of shared key encryption (see section 2 of Annex II). The access management messages may also be distributed by other media.

In the case of payment, per unit of time or per programme, the management messages convey an encrypted cost code, transmitted as part of the service. The credit held in the receiver may take the form of encrypted money tokens which are transmitted as part of an over-air addressing service (see section 3 of Annex II). Alternatively credit may take the form of stored money tokens distributed by other means. Payment consists of decrementing the stored credit according to the received cost code.

7. Access control equipment

This equipment includes a security module that is supplied with entitlement checking messages. This module may be buried or detachable (for example, smart card). The access control equipment communicates with the descrambler through a physical interface and logic circuits. The standardization of this interface is important in order to permit:

- the independence of the security module and the descrambling function built into the receiver;
- further development of the access control equipment.

If the security module contains an authorization with the same identifier as the authorization pointer in the entitlement checking message, it provides a control word if, in addition, the control parameters fulfil the conditions of the received authorization parameters. These may include:

- a date requirement, with the date in the control parameter falling between the starting and expiry dates in the authorization parameter;
- a price requirement by which an authorization may be provided only if a charge is accepted by the security module.

A transaction involving the security module may include three distinct stages:

- preliminary instructions, if present (e.g. password, user acceptance, etc.);
- operating instructions using the security module;
- result processing (e.g. delivery of control word).

Because a variety of security modules may be used, it would be desirable for the access control equipment to be independent of specific transactions. This independence can be provided if the access control equipment can interpret a sequence of instructions arranged in a specific language and transmitted within specific messages.

8. Applications

Conditional access techniques have been applied to some page organized teletext systems, to the use of independent data broadcasting systems (see Recommendation 653), satellite-broadcasting systems (see Report 1073) and terrestrial broadcasting systems (see Report 802). Some examples are given in Table I.

TABLE I

Examples of implementation of a conditional-access system

Reference in this Report	Page organized teletext systems		Data broadcasting systems		MAC/packet family (Report 1073, C-MAC/packet and D2-MAC/packet)
	Teletext system A (CCIR, 1982-86, Part I, Chapter 5)	Teletext system B (CCIR, 1982-86, Part II)	Independent data lines in teletext system B	Layers 1 to 4 of teletext system C adopted in France	
Scrambling process § 4.1	Exclusive-OR combination of the data bytes with the bytes of a pseudo-random generator. An interpretation byte in the header indicates whether the record is scrambled or not. See § 3.1	Exclusive-OR combination of the data bytes with the bytes of a pseudo-random generator. Packet 27 links designate the page as scrambled. See § 20.1	Exclusive -OR combination of the data bytes with bytes from a scrambling stream generator. Regular occurrence of user-data-key blocks designates the service as being scrambled.	Exclusive -OR combination of the data bytes with the bytes of pseudo-random generator. A byte in the initialization modifier indicates whether the data group is scrambled or not. Data groups with GT-0 or 1 are not scrambled.	<i>Picture:</i> double cut component rotation or single cut line rotation under the control of a pseudo-random generator <i>Sound:</i> exclusive-OR combination bit by bit of the data bits with the bits of a continuously running pseudo-random generator
Pseudo-random generator § 4.1	Combination of three multi-stage linear feedback shift register. See Annex 1	Use of one-way function employing cipher feedback algorithm. See Notes to § 20	Scrambling stream generator uses deciphering algorithm connected in output feedback mode (ISO DIS 8372).	Combination of three multi-stage linear feedback shift register.	<i>Picture:</i> two multi-stage linear feedback shift registers <i>Sound:</i> two multi-stage linear feedback shift registers initializing a further multi-stage linear feedback shift register
Pseudo-random generator synchronization § 4.1	First byte following the first US-X-Y sequence of the record. See § 2.3	First data byte of packet 0 of a designated page. See § 20	First byte of user data in user data block.	First byte following the initialization modifier.	Start of each picture frame
Initialization word § 4.2	12 bytes, see § 2.3	56 bits page key. See § 20.1	Scrambling stream initial variable is single byte at start of data block replicated eight times.	12 bytes	60 bits
Control word § 4.3	8 random bytes, see § 2.1	56 bits current system key. See § 20.1.3	64-bit user key	8 random bytes	60 bits being either randomly chosen or a cryptogram of the 256 frames counter
Initialization modifier § 4.4	4 bytes following the record header. See § 2.3	Not applicable	Not applicable.	4 bytes following the data group header.	The 8 bits frame-count

Entitlement checking messages (ECM) § 5	Designated records with classification numbers FFF and $Y_{11} = 1$; byte Y_{12} gives the index of the control word. Each message is introduced by the sequence US-J/F-J/F and comprises: - 3 bytes for the authorization pointer - 3 bytes for the control parameter - 16 bytes for the encrypted control word. See § 3.2	Designated packets include 22 bits authorization and control parameters, 112 bits encrypted control word. See § 20.1.3	One type of control block carries a user-data-key to all users who have a valid system key which enables them to decipher it.	Data groups for which GT (data group type, see Recommendation 653, Table Ia point 4.1) is equal to 14. The data groups are constituted of commands, each command identified by a command identifier and a command length identifier and composed of parameters identified by parameter identifier and parameter length identifier; two types of commands are defined: CI - Reference to the security module to use; CI $\neq 0$: entitlement checking command where each parameter carries an ECM and comprises: - 3 bytes for the authorization pointer - 3 bytes for the control parameter - 16 bytes for encrypted control word	Packets designated in the service identification channel. In the conditional access system for D2-MAC/packet used among others, on the French direct broadcasting satellite system TDF1-TDF2, packet coding is in accordance with the provisions of the specifications in "EUROCRYPT conditional access system for the MAC/packet family" (March 1989) [CCIR, 1986-90a] In the United Kingdom where D-MAC/packet has been adopted, British Satellite Broadcasting will commence BSS operations using the "EuroCypher a conditional access system for use with the MAC/packet family of transmission formats" [CCIR, 1986-90b]
Control word index § 4.5	Byte Y_{14} of scrambled record for descrambling and byte Y_{12} of ECM for updating. See § 3.1 and 3.2	Not applicable	Not applicable.		Not applicable
Change of control word and flag § 5	Bit b_8 of byte Y_{12} of ECM. See § 3.2	Current and new key words included in a designated packet of the user addressing. See § 20.2	The correct versions of keys are identified by matching table keys sent with the keys and the data blocks requiring these keys	Bit b_8 of parameter identifier of entitlement checking command	A new control word is transmitted every 256 frames and becomes the current control word when the frame count equals 0