INFORME 1079-1

CARACTERÍSTICAS GENERALES DE UN SISTEMA DE RADIODIFUSIÓN DE ACCESO CONDICIONAL

(Cuestión 37/11)

(1986-1990)

1. Introducción

Este Informe contiene los principios elaborados por la UER para los sistemas de acceso condicional para su aplicación a la televisión por satélite en Francia y el Reino Unido, donde dichos principios se han aplicado a los servicios de teletexto. Algunos detalles de esas aplicaciones pueden verse en el cuadro I al final del Informe.

Los principios se pueden aplicar también a sistemas terrenales clásicos de televisión y radiodifusión sonora y a otros servicios adicionales distintos del teletexto, enumerados en el Informe 802.

2. Componentes de un sistema de acceso condicional

Esta clase de sistema tiene dos componentes distintos y en muchos casos independientes:

2.1 *Aleatorización**

Proceso por el que un servicio se vuelve inutilizable para los usuarios no autorizados mediante la modificación de algunas de sus características bajo control del sistema de acceso condicional en el extremo transmisor.

2.2 *Control de acceso**

Suministro de información para que los usuarios autorizados puedan desaleatorizar el servicio. La disponibilidad de esta información se controla mediante su transmisión en forma encriptada*.

3. Condiciones que ha de cumplir un sistema de acceso condicional

3.1 *Seguridad*

La seguridad del sistema es el grado de dificultad con que tropieza el usuario no autorizado cuando intenta conseguir el acceso a los servicios.

Las dificultades son de dos clases:

- Desaleatorización de la señal sin referencia al proceso de control de acceso, lo que está en función de la naturaleza del servicio y del método de aleatorización.
- Obtención no autorizada de la clave* de control de acceso, lo que está en función de la seguridad de los algoritmos utilizados y del método de distribución de la clave.

3.2 *Modos de acceso*

Un sistema de acceso condicional será más eficaz si hay varios modos de acceso.

Como ejemplo cabe citar:

- Disponibilidad por un periodo de tiempo – autorización desde un momento de comienzo hasta un momento de fin.
- Programa o parte de un servicio – disponibilidad para una parte concreta de un servicio, se utilice o no completamente.

---

* Véanse las definiciones en el anexo I.

– Tasa por servicio (generalmente llamada «tasación por prestación») – el importe cobrado o adeudado es proporcional a la duración y/o el valor del servicio efectivamente recibido.

Los modos de acceso tienen que ser variables en relación con varios parámetros, por ejemplo:

– tiempo,
– diversos segmentos del servicio,
– grupos de destinatarios.

3.3 *Normalización del equipo*

Para ofrecer una economía de escala máxima en la fabricación del equipo receptor y simplificar así la gestión y el mantenimiento:

– hay que normalizar un equipo común que pueda absorber la mayor cantidad posible de opciones de servicio;
– los componentes «secretos» deben estar dentro de un módulo seguro con un interfaz normalizado* .

3.4 *Gestión del acceso*

La definición de acceso condicional se funda en el concepto formal de *derecho* al acceso, que se puede aplicar de diversas formas. Un derecho confiere a su titular la *autorización* de acceder al correspondiente servicio.

3.5 *Manera de evitar la degradación del servicio*

Hay tres tipos de degradación importantes:

– degradación del servicio finalmente disponible a causa de los procesos de aleatorización/desaleatorización;
– degradación debida a la adquisición deficiente o insegura de los datos de control de acceso;
– utilización antieconómica de los recursos a causa de los gastos generales de gestión o transmisión.

3.6 *Interacción con el proceso digital*

Se señala que algunos procesos de aleatorización pueden entrar en conflicto con algunas operaciones de los métodos de proceso digital de la señal, por ejemplo, la reducción de la velocidad binaria.

4. Descripción general de un sistema de acceso condicional

4.1 *Consideraciones generales*

El acceso condicional exige la *aleatorización* de la información antes de su radiodifusión. Este proceso está controlado por una secuencia de aleatorización obtenida de un *generador seudoaleatorio.*

El proceso de desaleatorización en el extremo receptor requiere la misma secuencia (en este caso, la secuencia de desaleatorización) para recuperar la señal original.

Para proporcionar esta secuencia y para garantizar el sincronismo de los procesos de transmisión y recepción, la activación del tren de bits del generador seudoaleatorio está controlada por una *palabra de inicialización.*

Para la seguridad del proceso, la información relacionada con el acceso que permite la recuperación de la palabra de inicialización se transmite en forma encriptada, según el modo de acceso utilizado (véase la fig. 1). La fig. 2 contiene la estructura detallada de este proceso, que se desribe en los puntos siguientes.

---

* Este tema ha sido examinado ya en la UER en relación con las especificaciones de un sistema de acceso condicional para el servicio de radiodifusión por satélite (véase el Informe 1073).

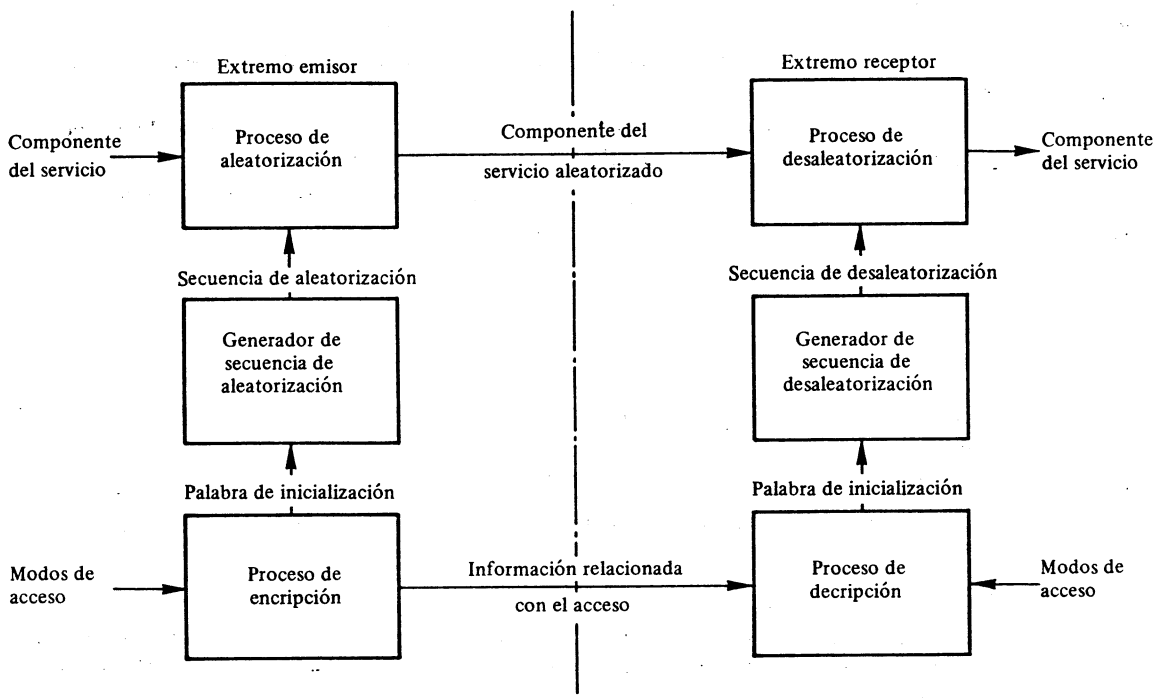


FIGURA 1 – *Sistema básico de acceso condicional*

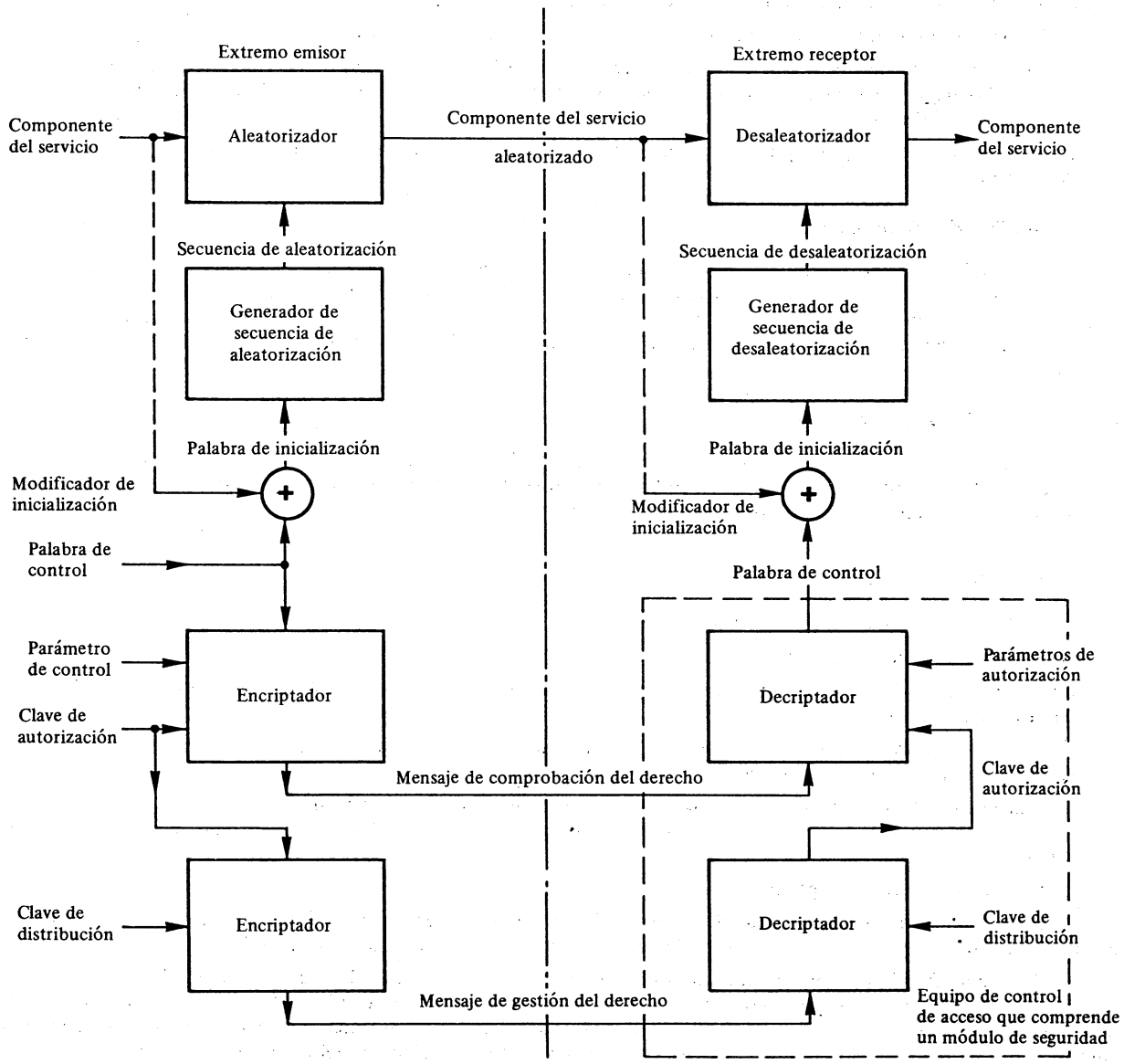


FIGURA 2 – *Descripción funcional de un sistema de acceso condicional*

Nota. – Para mayor claridad, en esta figura se presentan dos encriptadores y decriptadores. En la práctica se puede necesitar solamente uno de cada si el algoritmo de encripción controlado por la clave de autorización y el controlado por la clave de distribución son iguales.

4.2 *Palabra de inicialización*

El acceso condicional a un componente del servicio es pues el acceso condicional a la palabra de inicialización, que tiene dos elementos: la *palabra de control* y el *modificador de inicialización.*

4.3 *Palabra de control*

La palabra de control es el elemento básico de la seguridad. Su valor se elige arbitrariamente y se puede modificar durante el funcionamiento del servicio para aumentar la seguridad.

La palabra de control se comunica al receptor de la siguiente manera:

- En el extremo transmisor, según el modo de acceso utilizado, un algoritmo de encripción suministra versiones encriptadas de la palabra de control, que se transmiten en mensajes especiales. Se trata de los *mensajes de verificación del derecho al acceso.*
- En el extremo receptor, el equipo de control de acceso aplica el algoritmo inverso para regenerar la palabra de control.

4.4 *Modificador de inicialización*

El modificador de inicialización se utiliza para imponer secuencias de aleatorización suficientemente breves, con objeto de proporcionar seguridad y evitar al mismo tiempo la necesidad de un cálculo demasiado frecuente de la palabra de control. Así, la utilización de modificadores de inicialización diferentes para cada unidad estructurada de información aleatorizada hace que la palabra de inicialización cambie con suficiente frecuencia.

4.5 *Índice de palabra de control*

Para explotar un servicio segmentado, es necesario disponer de varias palabras de control relacionadas. Estas palabras se identifican por medio de *índices.* El índice de palabras de control utilizado para acceder a una unidad de información aleatorizada debe poderse obtener a partir de la señal transmitida.

5. Mensajes de comprobación del derecho al acceso

Cada uno de estos mensajes comprende:

- el índice de palabras de control;
- una señalización de modificación de la palabra de control; un cambio de estado indica un cambio de valor de la palabra de control;
- un *indicador de autorización* que identifica la clave de autorización situada en el módulo de seguridad del receptor a que se dirige el mensaje;
- un *parámetro de control* que suministra el valor (por ejemplo: fecha, precio, etc.) para los límites de comparación fijados a esos valores en el módulo de seguridad del receptor llamados *parámetros de autorización*;
- la palabra de control encriptada.

Para desaleatorizar una unidad de información, el receptor debe haber adquirido previamente la palabra de control a partir de un mensaje de comprobación del derecho de acceso que lleve el índice adecuado.

Para una eficacia óptima, los mensajes de comprobación del derecho de acceso relacionados con la misma palabra de control pero correspondientes a diferentes grupos de usuarios o a diferentes tipos de equipo de control de acceso deben estar agrupados en el mismo índice. Aunque ésta no es su única aplicación, el sistema de índices antes descrito permite la transmisión anticipada de mensajes de comprobación del derecho de acceso.

El equipo de acceso condicional crea un cuadro de palabras de control activo, que es actualizado por los mensajes de comprobación del derecho de acceso independientemente de los datos aleatorizados. Para identificar la palabra de control correcta, el dispositivo desaleatorizador suministra al equipo de control de acceso el índice correspondiente. La gestión de este cuadro forma parte de las facilidades proporcionadas en el interfaz entre el desaleatorizador y el equipo de control de acceso.

6. Mensajes de gestión del derecho de acceso

El proceso de un mensaje de gestión del derecho de acceso convalida o confiere el derecho. Este proceso se lleva a cabo dentro del módulo de seguridad asociado con un cálculo criptográfico que comprende una *clave de distribución.* Esta clave de distribución se utiliza para encriptar y descriptar mensajes y/o claves de autorización dirigidos a receptores individuales. Los criptogramas correspondientes constituyen la señal de validación y se transportan como parte del mensaje de gestión del derecho de acceso.

En los sistemas de radiodifusión con acceso condicional, los mensajes de gestión del acceso se pueden radiodifundir. Esta operación se conoce con el nombre de «distribución por las ondas». Los mensajes de gestión de acceso se pueden, sin embargo, distribuir también por otros medios.

En los sistemas de radiodifusión con acceso condicional, los mensajes de gestión del acceso se pueden radiodifundir. Esto se conoce como "direccionamiento radiotransmitido". El tiempo asociado con la distribución de las claves radiotransmitidas puede reducirse en forma significativa aplicando los principios del cifrado de claves compartidas (véase el punto 2 del anexo II). Los mensajes de gestión del acceso también pueden distribuirse por otros medios.

En el caso del pago cifrado por unidad de tiempo o por programa, los mensajes de gestión incluyen un código de costo, transmitido como parte del servicio. El crédito del receptor puede tomar la forma de fichas de dinero cifradas es que se transmiten como parte de un servicio de direccionamiento radiotransmitido (véase el punto 3 del anexo II). Alternativamente, el crédito puede tomar la forma de fichas de dinero almacenadas distribuidas por otros medios. El pago consiste en una disminución del crédito almacenado, según el código de costo recibido.

7. Equipo de control de acceso

Este equipo comprende un módulo de seguridad que se suministra con los mensajes de comprobación del derecho de acceso. Este módulo puede ser fijo o móvil (por ejemplo, la tarjeta inteligente (smart card)). El equipo de control de acceso comunica con el desaleatorizador a través de un interfaz físico y circuitos lógicos. La normalización de este interfaz es importante para permitir:

- la independencia del módulo de seguridad y la función de desaleatorización incorporada al receptor;
- el desarrollo ulterior del equipo de control de acceso.

Si el módulo de seguridad contiene una autorización con el mismo identificador que el indicador de autorización del mensaje de comprobación del derecho de acceso, suministra una palabra de control si, además, los parámetros de control cumplen las condiciones de los parámetros de autorización recibidos. Estas condiciones comprenden:

- una exigencia de fecha, de modo que la fecha del parámetro de control esté comprendida entre las fechas de comienzo y expiración en el parámetro de autorización;
- una exigencia de precio, de modo que sólo se pueda dar una autorización si el módulo de seguridad acepta un cargo.

Una transacción en la que intervenga el módulo de seguridad puede comprender tres fases distintas:

- instrucciones preliminares, en caso de presencia (por ejemplo: contraseña, aceptación del usuario, etc.);
- instrucciones de funcionamiento utilizando el módulo de seguridad;
- proceso de resultados (por ejemplo: entrega de la palabra de control).

Como se pueden utilizar varios módulos de seguridad, sería aconsejable que el equipo de control de acceso no dependiese de transacciones concretas. Esta independencia es posible si el equipo de control de acceso puede interpretar una secuencia de instrucciones dispuestas en un lenguaje específico y transmitida dentro de mensajes específicos.

8. Aplicaciones

Las técnicas de acceso condicional se han aplicado a algunos sistemas de teletexto organizado por páginas y al uso de sistemas de radiodifusión de datos independientes (véase la Recomendación 653), sistemas de radiodifusión por satélite, (véase el Informe 1073), y sistemas de radiodifusión terrenal (véase el Informe 802). En el cuadro I se dan algunos ejemplos.

CUADRO I - Ejemplos de realización de un sistema de acceso condicional

Referencia en el presente Informe	Sistemas de teletexto organizado por páginas		Sistemas de radiodifusión de datos		Familia MAC paquetes (Informe 1073, C-MAC/paquetes y D2-MAC/paquetes)
	Teletexto sistema A [CCIR, 1982-86, parte I, capítulo 5]	Teletexto sistema B [CCIR, 1982-86, parte II]	Líneas de datos independientes sistema de teletexto B	Capas 1 a 4 del sistema de teletexto C adoptado en Francia	
Proceso de aleatorización. Véase el § 4.1	Combinación «O exclusiva» de octetos de datos con el octeto de un generador seudoaleatorio. Un octeto de interpretación en el encabezamiento indica si el mensaje está aleatorizado o no. Véase el § 3.1	Combinación «O exclusiva» de octetos de datos con los octetos de un generador seudoaleatorio. Los enlaces del paquete 27 designan la página aleatorizada. Véase el § 20.1	Combinación "O exclusiva" de octetos de datos con los octetos de un generador embrollador. La presencia regular de bloques de datos claves de usuario designa el servicio aleatorizado	Combinación "O exclusiva" de octetos de datos con los octetos de un generador aleatorio. Un octeto del modificador de inicialización indica si el grupo de datos se aleatoriza o no. Los grupos de datos con GT = 0 ó 1 no se aleatorizan.	*Imagen:* Rotación de componentes de doble corte o rotación de línea de corte sencillo bajo control de un generador seudoaleatorio *Sonido:* Combinación «O exclusiva» bit por bit de los bits de datos con los bits de un generador seudoaleatorio en funcionamiento continuo
Generador seudoaleatorio. Véase el § 4.1	Combinación de tres registros de desplazamiento multietapa con realimentación lineal. Véase el Anexo I	Uso de una función unidireccional que emplea un algoritmo de cifrado con realimentación. Véanse las notas al § 20	El generador embrollador usa un algoritmo de descifrado conectado en el modo realimentado de salida (ISO DIS 8372)	Combinación de tres registros de desplazamiento multietapas con realimentación lineal	*Imagen:* dos registros de desplazamiento multietapas con realimentación lineal *Sonido:* dos registros de desplazamiento de pasos múltiples con realimentación lineal que inicializan un nuevo registro de desplazamiento de pasos múltiples con realimentación lineal
Sincronización del generador seudoaleatorio. Véase el § 4.1	Primer octeto que sigue la primera secuencia US-X-Y del mensaje. Véase el § 2.3	Primer octeto de datos del paquete 0 de una página designada. Véase el § 20	Primer octeto de datos de usuario en los bloques de datos de usuario	Primer octeto después del modificador de inicialización	Iniciación de cada trama de imagen
Palabra de inicialización. Véase el § 4.2	12 octetos. Véase el § 2.3	Clave de página de 56 bits. Véase el § 20.1	La variable embrolladora inicial es un solo octeto al principio del bloque de datos de usuario repetido 8 veces	12 octetos	60 bits
Palabra de control. Véase el § 4.3	8 octetos aleatorios. Véase el § 2.1	56 bits que constituyen la clave del sistema corriente. Véase el § 20.1.3	Clave de usuario de 64 bit	8 octetos aleatorios	60 bits que pueden ser escogidos al azar o un criptograma del contador de 256 tramas
Modificador de inicialización. Véase el § 4.4	4 octetos que siguen al encabezamiento del mensaje. Véase el § 2.3	No aplicable	No aplicable	4 octetos que siguen al encabezamiento de grupo de datos	El contador de trama de 8 bits
Mensajes de comprobación del derecho de acceso. Véase el § 5	Mensajes designados con número de clasificación FFF e $Y_{11} = 1$; el octeto Y_{12} da el índice de la palabra de control. Cada mensaje es introducido por la secuencia US-3/F-3/F y comprende: - 3 octetos para el indicador de autorización - 3 octetos para el parámetro de control - 16 octetos para la palabra encriptada de control Véase el § 3.2	Los paquetes designados incluyen 22 bits de autorización y parámetros de control, 112 bits de la palabra encriptada de control. Véase el § 20.1.3	Un tipo de bloque de control lleva una clave de datos de usuario a todos los usuarios que tienen una clave de sistema válida que les permite descifrarlo	Grupos de datos para los que GT (tipo de grupo de datos, véase el punto 4.1 del cuadro 1a de la Rc. 653) es igual a 14. Los grupos de datos están constituidos por instrucciones de control, cada una de las cuales se identifica por un identificador de instrucción de control y un identificador de longitud de instrucción de control, y está compuesto de parámetros identificados por identificadores de parámetro e identificadores de longitud de parámetro. Se definen dos tipos de instrucciones de control: Cl=0, referencia al módulo de seguridad que hay que utilizar Cl ≠0: instrucción de control de comprobación del derecho de acceso donde cada parámetro lleva un mensaje de comprobación de derecho de acceso y comprende: - 3 octetos para el indicador de autorización - 3 octetos para el parámetro de control - 16 octetos para la palabra cifrada de control	En el sistema de acceso condicional para el sistema D2-MAC/paquete utilizado entre otros por el sistema francés de radiodifusión directa por satélite TDF1-TDF2, la codificación se ajusta a las disposiciones de la especificación "Sistema de acceso condicional para la familia MAC/paquetes EUROCRYPT - marzo de 1989 [CCIR, 1986-90a] En el Reino Unido, donde se ha adoptado el sistema D-MAC/paquete, Britihs Satellite Broadcasting iniciará las operaciones en el servicio de radiodifusión por satélite utilizando el sistema de acceso condicional Eurocypher para emplearlo con los formatos de transmisión de la familia MAC/paquetes [CCIR, 1986-90b]

CUADRO I (continuación)

Referencia en el presente Informe	Sistemas de teletexto organizado por páginas		Sistemas de radiodifusión de datos		Familia MAC paquetes (Informe 1073, C-MAC/paquetes y D2-MAC/paquetes)
	Teletexto sistema A [CCIR, 1982-86, parte I, capítulo 5]	Teletexto sistema B [CCIR, 1982-86, parte II]	Líneas de datos independientes sistema de teletexto B	Capas 1 a 4 del sistema de teletexto C adoptado en Francia	
Índice de la palabra de control. Véase el § 4.5	Octeto Y_{16} de mensaje aleatorizado para desaleatorización y octeto Y_{12} de comprobación del derecho de acceso para actualización. Véanse los § 3.1 y 3.2	No aplicable	No aplicable		No aplicable
Cambio de la palabra de control y del iniciador. Véase el § 5	Bit b_8 del octeto Y_{12} de comprobación del derecho de acceso. Véase el § 3.2	Palabras clave corrientes y nuevas incluidas en un paquete designado del direccionamiento del usuario. Véase el § 20.2	Las versiones correctas de las claves se identifican comparando las etiquetas de las claves enviadas con las claves y con los bloques de datos requeridos para esas claves	Bit b_8 del identificador de parámetro de la instrucción de control de comprobación del derecho de acceso	Una nueva palabra de control se transmite cada 256 tramas y se convierte en la palabra de control corriente cuando el cómputo de trama es igual a 0
Mensaje de gestión del derecho de acceso. Véase el § 6	El derecho de acceso está corrientemente gestionado por un sistema videotexto en una red de telecomunicación. Véase el § 1.3	El derecho de acceso está gestionado por el direccionamiento radiotransmitido del equipo de recepción utilizando paquetes de direcciones de usuario únicos y compartidos. Véase el § 20.2	El derecho de acceso está gestionado por el direccionamiento radiotransmitido del módulo de control de acceso utilizando bloques de datos compartidos y direccionados unívocamente. Los bloques de datos para el direccionamiento radiotransmitido son multiplexados en el mismo canal que los datos del mensaje	Todavía sin normalizar El derecho de acceso puede gestionarse por un sistema de videotex en una red de telecomunicaciones	En el sistema de acceso condicional para el sistema D2-MAC/paquete utilizado entre otros por el sistema francés de radiodifusión directa por satélite TDF1-TDF2, la codificación se ajusta a las disposiciones de la especificación "Sistema de acceso condicional para la familia MAC/paquetes EUROCRYPT - marzo de 1989 [CCIR, 1986-90a] En el Reino Unido, donde se ha adoptado el sistema D-MAC/paquete, Britbh Satellite Broadcasting iniciará las operaciones en el servicio de radiodifusión por satélite utilizando el sistema de acceso condicional Eurocypher para emplearlo con los formatos de transmisión de la familia MAC/paquetes [CCIR, 1986-90b]
Equipo de control de acceso. Véase el § 7	Incorporado en el receptor, incluye un lector de tarjetas inteligentes. Véase el § 1.3	Incorporado en el receptor o funcionalmente separado, a elección de quien proporciona el servicio	Completamente contenido en el módulo de seguridad. Acepta datos en serie del decodificador de paquetes y suministra al usuario datos serie descrifrados	Incorporado en el receptor, incluye un lector de tarjetas inteligentes	Funcionalmente separado de otras partes del receptor por medio de un interfaz que se normalizará
Módulo de seguridad. Véase el § 7	Tarjeta inteligente con interfaz propuesto para normalización por la ISO [ISO, 1986]	Módulo incorporado o separado o tarjeta inteligente	Unidad basada en el microprocesador cargada con el soporte lógico de aplicación para manejar todos los protocolos de datos y realizar los algoritmos de descifrado	Tarjeta inteligente con interfaz propuesto para normalización por la ISO	Se proponen dos soluciones: – la tarjeta inteligente – un módulo incorporado

REFERENCIAS BIBLIOGRÁFICAS

ISO [1986] TC/97/SC17/WG4/N97 Integrated circuit card with contacts, part III. Electronic signals and exchange protocols.

Documentos del CCIR

[1982-86] 11/422(Rev.1) (Especificación de los sistemas de teletexto, Fascículo descriptivo y provisional).

[1986-90]: a: GITM 10-11/3-116 (Francia),
b: GITM 10-11/3-117 (Reino Unido-IBA).

BIBLIOGRAFÍA

BECKER, H. y PIPER, F. *Cypher Systems. The Protection of Communications.* Northwood Books, ISBN 719825717.

BRADSHAW, D.J. y WRIGTH, D.T. [1986] - BBC Datacast - Conditional Access Operation, IERE Publication No. 69, pp 99-105, Londres, 16th-17th Septiembre, 1986.

DENNING, D. *Cryptography and Data Security.* Addison Wesley. ISBN 0-201-101-50-5.

GUILLOU, L. [noviembre de 1980] Radiodiffusion à péage pour application au télétexte Antiope. Congrès international sur les systèmes et services nouveaux de télécommunications, Liège, Bélgica.

GUILLOU, L. [abril de 1984] Smart card and conditional access. Eurocrypt 1984, La Sorbonne, París, Francia.

ISO [1987] TC97/SC17/WG4. Identification cards. Integrated circuits with contact ISO Dis 7816.

MASON, A. G. [1985] A pay-per-view over-air addressing system specified for direct broadcasting by satellite. IERE Publication No. 62.

WRIGT, D.T. y EDWARDSON, S.M. [1986] - Key Management in Broadcast Conditional Access Systems, IEE Conf. Pub. 269, pp. 104-109, Londres, 27th-28th Octubre, 1986.

Documentos del CCIR

[1982-86]: 11/139 (UER); 11/307 (Francia); 11/308 (Francia); 11/379 (Canadá).

[1986-90]: 11/35 (Reino Unido); 11/36 (Reino Unido); 11/40 (Reino Unido), 11/122 (Francia).

ANEXO I

ALGUNOS TÉRMINOS Y DEFINICIONES RELACIONADOS CON LOS SISTEMAS DE RADIODIFUSIÓN DE ACCESO CONDICIONAL

Aleatorización [en radiodifusión] (scrambling, embrouillage)

Alteración de las características de una señal radiodifundida de imagen, sonido o datos difundida a fin de impedir la recepción no autorizada de la información en forma clara. Esta alteración es un proceso bien definido, controlado por el sistema de acceso condicional en la emisión.

Desaleatorización [en radiodifusión] (descrambling, désembrouillage).

Restablecimiento de las características de una señal radiodifundida de imagen, sonido o datos a fin de permitir la recepción de la información en forma clara. Este restablecimiento es un proceso bien definido, controlado por el sistema de acceso condicional en la recepción.

Nota 1. – Los términos aleatorización y desaleatorización son aplicables tanto a las señales analógicas como a las digitales.

Nota 2. – Estos términos no deben utilizarse para describir procesos tales como la dispersión de energía en un sistema de satélites.

Control de acceso condicional

La función del control de acceso condicional en la emisión es generar las señales de control de la aleatorización y las «claves» correspondientes al servicio.

La función del control del acceso condicional en la recepción es producir las señales de control de la desaleatorización, al mismo tiempo que las «claves» correspondientes al servicio.

Nota. – La palabra «clave» se utiliza en las precedentes definiciones con un sentido general equivalente al utilizado en la Cuestión 37/11.

Las palabras «*encriptado*» y «*decriptado*» se aplican a los métodos utilizados para proteger e interpretar algunas informaciones contenidas en los mensajes relativos al acceso que deben difundirse del extremo de emisión al extremo de recepción de las funciones de control de acceso condicional.

BIBLIOGRAFÍA

Documentos del CCIR

[1982-86]: 11/228 (Grupo de Trabajo sobre Terminología); 11/139 (UER).

ANEXO II

Sistemas de radiodifusión de acceso condicional: ejemplos de los principios de los sistemas de cifrado con clave compartida para servicios de radiodifusión directa por satéliet y radiodifusión de datos, incluido el teletexto

1. Descripción del sistema de acceso condicional que emplea el direccionamiento radiotransmitido utilizado en el Reino Unido

1.1 Sistemas de acceso condicional con direccionamiento radiotransmitido

En la fig. 3 se muestran las funciones básicas de un sistema de cifrado para radiodifusión directa de televisión por satélite con direccionamiento radiotransmitido. Se utiliza una palabra de control (CW) que varía, típicamente cada 10 segundos, para controlar el proceso de aleatorización de la señal de televisión A. Se obtiene así la señal aleatorizada CW(A). La palabra de control se transmite al receptor después de su cifrado con la clave suplementaria S. Este criptograma, que contiene también datos relacionados con el programa, por ejemplo el precio, se transmite en un paquete de mensaje de comprobación del derecho de acceso (ECM) [UER, 1986]. La clave suplementaria S es común a todos los abonados, pero contrariamente a la palabra de control, cambia con poca frecuencia, por ejemplo, una vez por mes. Estos largos intervalos entre los cambios de la clave S permiten transmitirla a cada abonado por medio del proceso de direccionamiento radiotransmitido. La clave S, junto con los mensajes de derecho de acceso del abonado (M) son cifrados con la la clave de distribución, D, de cada abonado. Estos criptogramas son enviados en paquetes de mensajes de gestión del derecho de acceso (EMM), y direccionados individualmente a receptores separados. En [Mason, 1986] figura una descripción completa.

1.2 Reducción de la duración del ciclo de validación - El criptograma compartido

La fig. 4 muestra el formato de un criptograma compartido que reduce el número total de bits que es necesario transmitir en el ciclo de validación del abonado. El criptograma de la Figura 4 comprende veintitrés abonados, que representan un grupo de abonados. Todos los miembros del grupo comparten la misma dirección principal, que se utiliza para tener acceso al criptograma, y la misma clave de distribución que sirve para descifrar el criptograma. Como cada uno de los miembros del grupo necesita la clave suplementaria de 56 bits para recuperar la señal de televisión, el "excedente" en bits se distribuye entre los 23 abonados. Lo mismo es válido para la palabra de modo de 4 bits y para la dirección principal de 24 bits. El total de 84 bits es transmitido a todo el grupo en vez de a cada abonado individualmente. De este modo, para un grupo de 23 miembros sólo hay que transmitir 3,65 bits por abonado. Este presupuesto permite obtener una palabra de abonado de 12 bits que puede proporcionar 12 servicios de abono básicos independientes, 6 servicios superpuestos independientes o fichas para tasación por prestación. Estas últimas pueden utilizarse para cualesquiera servicios, a condición de que todos éstos sean administrados por un operador de servicios común. La palabra de modo identifica qué opción se está transmitiendo. Pueden utilizarse menos bits para la palabra de abonado: por ejemplo, un sistema de abono a un solo servicio básico sólo requerirá un bit. Lo que permitirá reducir la duración del ciclo de validación de abonado en una proporción mucho mayor, por ejemplo, la utilización de una palabra de abonado de 12 bits reduce normalmente la duración del ciclo por un factor de 6,5, mientras que la utilización de una palabra de abonado de 1 bit la reduce por un factor de 20.

1.2.1 Estrategia para eliminar las claves de distribución robadas

Si se determina que un abonado se ha convertido en pirata, debe suprimirse esa clave. Se requiere un método para evitar la neutralización de los otros abonados que comparten la misma clave.

Esto se logra almacenando dos claves secretas en el dispositivo de seguridad del receptor, en vez de sólo una. La primera clave es la clave de distribución compartida y la segunda es una clave única (U), que no es compartida sino que es diferente para cada abonado. Cuando se detecta un pirata, se envía individualmente una nueva clave de distribución compartida (D_{new}) a cada uno de los miembros restantes de buena fe, cifrándola con su clave única (U), véase la fig. 5. Veamos un ejemplo: X, Y y Z son los abonados de un grupo dado que comparten la clave de distribución (D_{old}) y se determina que X es un pirata. Se envía la clave (D_{new}) a los abonados Y y Z transmitiendo UY (D_{new}) y UZ (D_{new}). Evidentemente, el formato para la transmisión de U(D) es mucho menos eficaz que la clave compartida, pero esto no es importante puesto que sólo incumbe a un pequeño número de abonados. La entidad radiodifusora puede estar segura de que los abonados de buena fe han recibido la nueva clave de distribución compartida (D), transmitiendo U(D) hasta que los abonados hayan hecho dos pagos de abono. Como la duración del ciclo es probablemente inferior a un minuto, la entidad radiodifusora puede tener la certeza de que se ha recibido la nueva clave compartida. Esta certeza se basa en la hipótesis de que cada abonado del grupo mira los programas durante más de un minuto en el transcurso del periodo de abono que ha comprado.

1.3 Transmisión de crédito radiotransmitido y de precio del programa para tasación por prestación

Debe proporcionarse un alto grado de seguridad para la transmisión de de crédito radiotransmitido para un servicio completo con tasación por prestación. Esto puede lograrse de manera fiable si se siguen los siguientes principios.

1.3.1 Información de crédito radiotransmitido

El valor de una suma de dinero no puede radiotransmitirse cifrado con una clave K en la forma K(MONEY). Esto es muy inseguro porque el mensaje MONEY no es único. Supóngase que MONEY es un código transmitido que representa una suma de dinero que aumenta monótonamente y que la transmisión del valor "todos ceros" para el código representa un crédito nulo para un abonado. El cifrado de este código con la clave K produce algunas secuencias de bits para K(MONEY). Un pirata puede añadir dinero al crédito almacenado en el receptor sin conocer la clave K, alterando sencillamente la secuencia de bits de K(MONEY). Cuando el receptor descifra este nuevo mensaje mediante la clave secreta K el texto claro debe ser distinto de cero. Esto se debe a que sólo puede haber una relación de correspondencia del texto cifrado con el texto claro. Como el texto cifrado original significaba "crédito nulo" cualquier cambio debe significar "crédito no nulo". De este modo el pirata puede añadir crédito, pero ignora el importe.

Este problema se evita adjuntando una clave al valor del dinero, que no será aceptada por el receptor sino la reconoce. Para ello, se envía la señal D(M,S) donde D es la clave de distribución y S la clave suplementaria. Para que el receptor valide los bits de "dinero" (M) mediante la clave S, debe estar seguro de que la clave suplementaria S ha sido correctamente recibida. A este fin, se transmite la señal S(P,CW,S), véase el punto 1.3.4.

1.3.2 Transmisión de fichas de dinero

Como el ciclo de validación se repite, para transmitir las fichas de dinero, debe utilizarse un método que permita que el receptor acepte un nuevo pago pero que le impida acumular continuamente el mismo pago en cada repetición del ciclo. Asimismo, las "repeticiones" locales del antiguo texto cifrado no deben engañar al dispositivo de seguridad del receptor para que acepte pagos anteriores más de una vez. Como el canal de radiodifusión sólo permite la comunicación unidireccional, deben cumplirse estos requisitos cuando la velocidad con que se hacen los pagos no concuerda con la velocidad a la cual el dispositivo de seguridad los recibe.

El único método conocido para satisfacer estos criterios esenciales consiste en transmitir la suma total de todos los pagos enviados a la entidad radiodifusora en la señal (M_T). El dispositivo de seguridad almacena en memoria la suma total de todos los pagos que ha recibido (M_R) y el valor del pago (M_P) separadamente en sus memorias de dinero. M_P es la diferencia entre M_T y M_R:

pago efectuado $M_P = M_T - M_R$ para $M_P >$ a cero.

De esta manera, los pagos nunca pueden "fallar" y las repeticiones de pago anteriores no aumentarán M_P porque cada vez que se acepta un pago M_R se pone al valor recibido, M_T. De este modo, un pago sólo se acepta si $M_T - M_R > 0$. Para que la duración del ciclo, sea corta debe imponerse un límite al número de bits utilizado para transmitir el valor M_T. La especificación del sistema MAC/paquetes [UER, 1986] utiliza 12 bits para M_T que proporciona hasta 4.096 fichas.

1.3.3 Precio del programa

Los datos relacionados con el programa (P) pueden representar el precio de un programa. Un método para indicar el precio es que el importe de la memoria de dinero disminuya cada 10 segundos por un valor dado a medida que se recibe el programa. Otra posibilidad es solicitar un solo pago al comienzo del programa para su adquisición completa. Si se utiliza el segundo método, se almacena en memoria un número de identificación cuando se compra el programa a fin de evitar una doble compra si por ejemplo, el receptor es desconectado durante la transmisión.

Los datos relacionados con el programa (P) están "firmados" como correctos por la clave suplementaria (S) de la misma manera que los bits "de dinero" del abonado. Esta "firma" se obtiene incluyendo la clave S en el texto claro de la señal S(P,CW,S). Sólo se requiere que el receptor compruebe que la clave S se ha recibido correctamente para verificar tanto los datos relacionados con el programa (precio) como los mensajes de abonado (dinero), véase el punto 1.3.4.

1.3.4 Conocimiento de la clave suplementaria correcta

El control de seguridad en la clave suplementaria (S) se realiza por medio de la señal S(P,CW,S). Esta señal tiene la propiedad de que la clave S está contenida en el texto claro y que se utiliza también para cifrarlo. El control de seguridad en el receptor obtiene en primer lugar la clave que parece ser la clave suplementaria correcta S descifrando la señal de validación D(M,S). Utiliza después esta clave S recibida para descifrar la señal S(P,CW,S). En la medida en que el dispositivo de seguridad pueda descifrar la señal S(P,CW,S) y obtener el mismo valor para la clave suplementaria S en el texto claro, existe un alto grado de certidumbre de que se ha recibido la clave suplementaria correcta S.

La probabilidad de que el dispositivo de seguridad dé una información errónea es aproximadamente de 2^{-n}, donde n es el número de bits utilizados para la clave S. El sistema de [UER,1986] utiliza 56 bits para la clave S, lo que da una probabilidad de detección falsa de 10^{-17}.

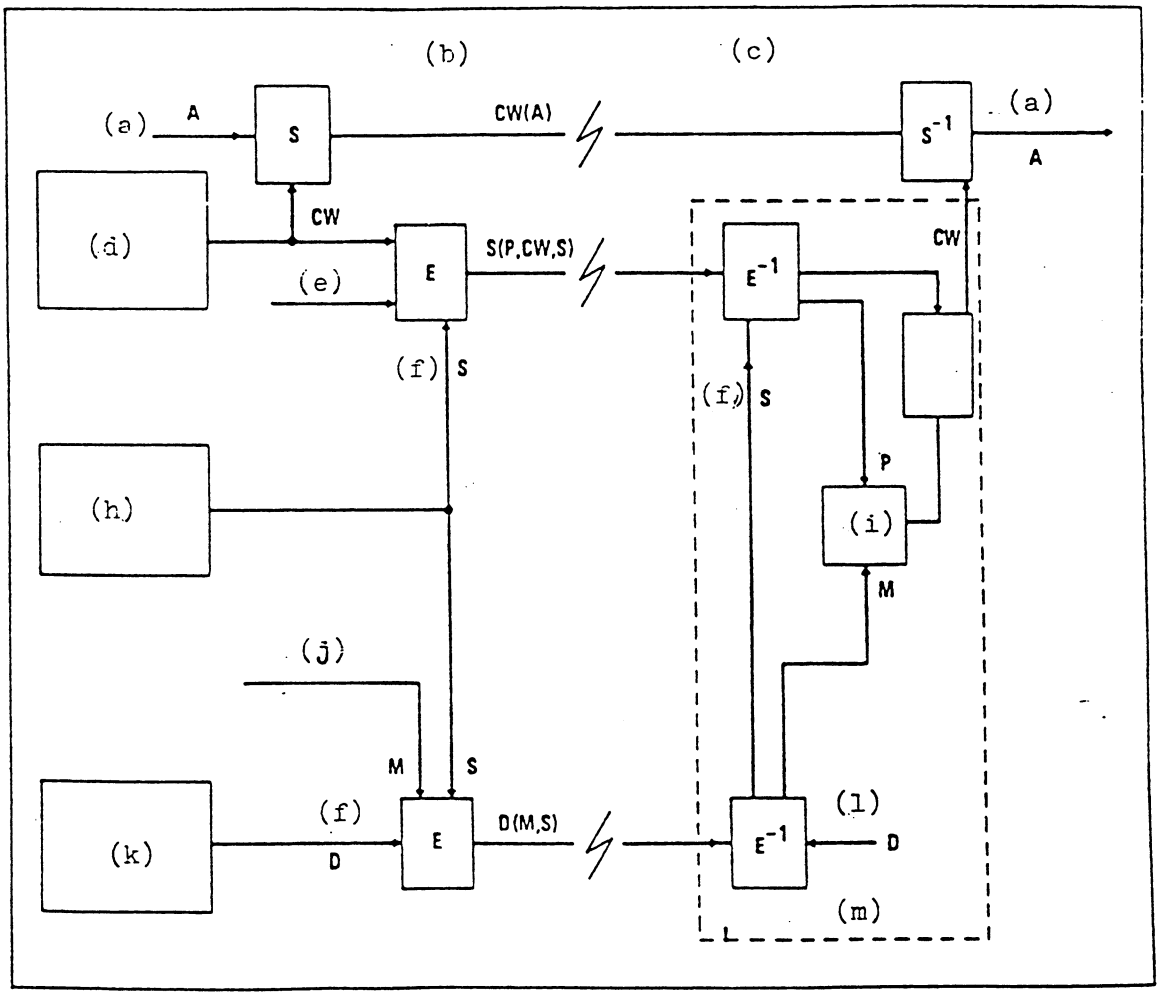


FIGURA 3

Sistema de cifrado básico

(a) señal de televisión
(b) transmisor
(c) receptor
(d) palabra de control, CW, que se cambia cada 10 segundos
(e) datos de programa, P
(f) clave
(g) puerta
(h) clave suplementaria S, que se cambia, digamos, cada mes
(i) memoria
(j) mensaje de cliente
(k) clave de distribución del cliente, D
(l) clave secreta del cliente
(m) dispositivos de seguridad

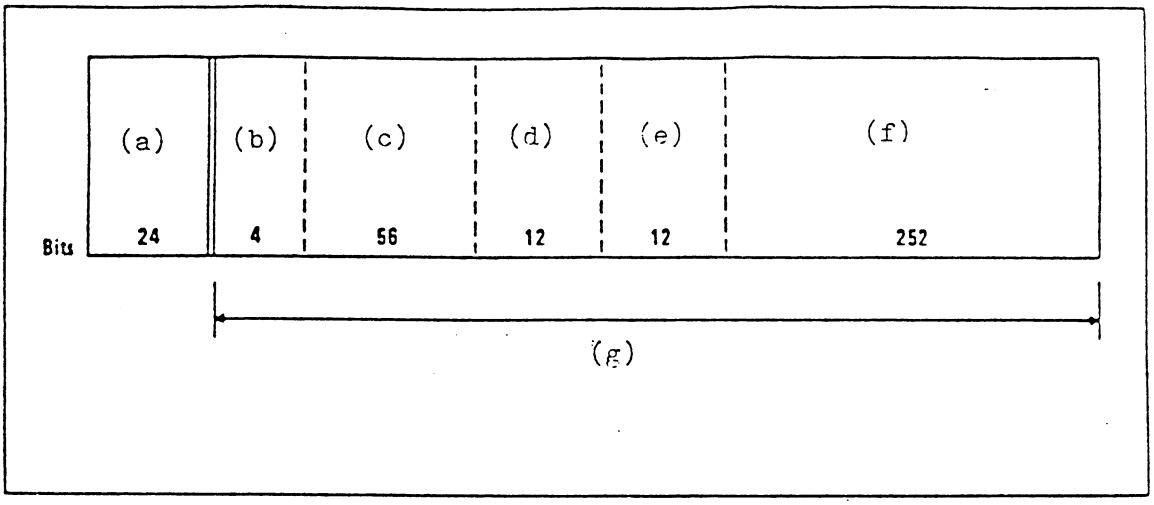


FIGURA 4

Bloque de validación compartido

(a) dirección compartida
(b) modo
(c) clave suplementaria, S
(d) cliente Nº 1
(e) cliente Nº 2
(f) clientes Nº 3 a 23
(g) bloque compartido cifrado con la misma clave de distribución compartida, D

Nota.- Protección contra errores (no mostrada) - treinta (24, 12) palabras de código de Golay.

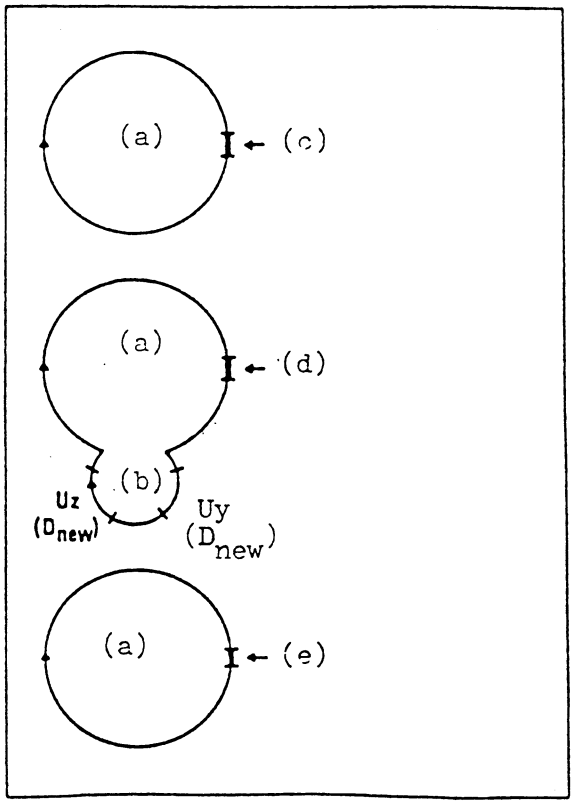


FIGURA 5

Sustitución de la clave compartida D

(a) ciclo D
(b) ciclo U
(c) D_{old}: los clientes X, Y, Z comparten la clave D_{old}
(X,Y,Z)
(d) D_{new}: X se convierte en pirata y es eliminado
(Y,Z)
(e) D_{new}: la entidad radiodifusora está segura de que Y y Z han recibido D_{new}
(Y,Z) porque cada uno ha enviado dos pagos de abono.

2. Descripción de un sistema de acceso condicional con direccionamiento radiotransmitido. El sistema Eurocrypt

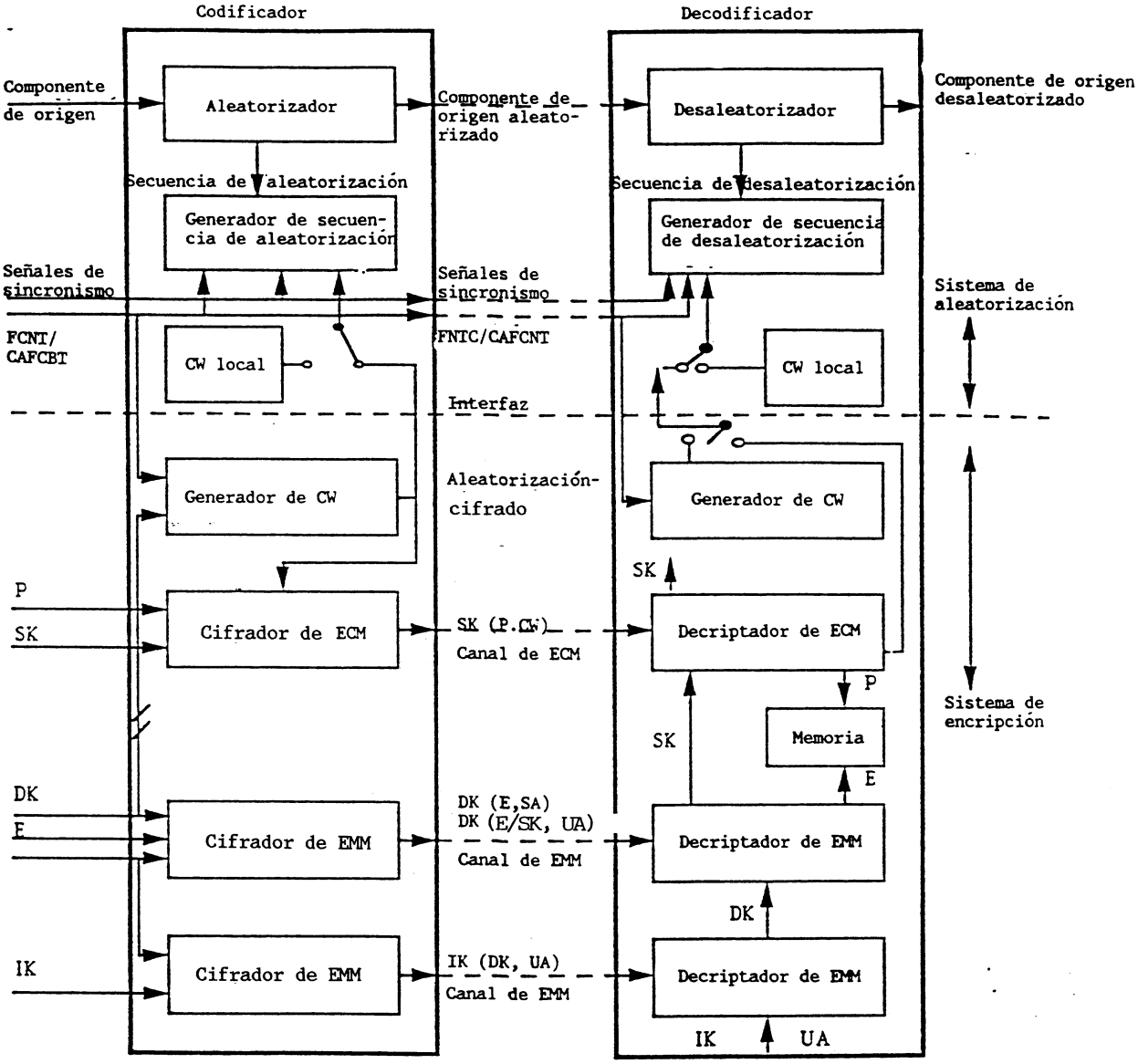
2.1 Sistemas de aleatorización y encripción

En relación con la Figura 6, se utiliza una palabra de control (CW) para inicializar el generador de secuencia de aleatorización/desaleatorización.

La palabra de control se transmite, cifrada con la clave de explotación, en los mensajes de comprobación de los derechos de acceso (ECM). En los ECM también están presentes los datos relativos al modo de acceso condicional del programa. El contenido de los ECM se protege contra la falsificación por un procedimiento de firma. La clave de explotación (SK) es una información secreta contenida en un procesador de seguridad. Si el procesador de seguridad comprueba que los parámetros de autorización (derechos de acceso) del receptor coinciden con los parámetros de acceso condicional del programa, puede utilizarse la clave de explotación para descifrar la palabra de control.

La clave de explotación es común a todos los usuarios. Los derechos de acceso son actualizados periódicamente (por ejemplo, cada mes); la clave de explotación puede modificarse en circunstancias excepcionales. Es posible transmitir a los usuarios tanto los derechos de acceso como las claves de explotación, utilizando técnicas de direccionamiento radiotransmitido, en los mensajes de gestión de los derechos de acceso (EMM). Las claves de explotación se transmiten cifrados con una clave de distribución propia del suministrador del programa. El contenido de los EMM se protege (al igual que los ECM) utilizando un procedimiento de firma. La clave de distribución puede ser específica de cada uno de los usuarios de un grupo de utilizadores (o incluso de toda la audiencia). Si la clave de distribución es específica del usuario, no puede servir más que para enviar derechos de acceso o claves a un usuario único, identificado por su dirección individual (UA) en un EMM individual (EMM-U). Si la clave de distribución es común a un grupo de usuarios, se utiliza para enviar derechos de acceso a un grupo de usuarios mediante un EMM común compartido (llamado EMM-S). Esta técnica se utiliza con preferencia a la primera en la medida en que permite reducir la velocidad de transmisión de los EMM. El primer método se adapta mejor a los raros casos en que es necesario cambiar la clave de distribución compartida.

La primera clave de distribución de un suministrador de programas se envía igualmente en un EMM, cifrada con la clave del transmisor IK. Esta clave tiene total prioridad en el sistema de claves y es la única que puede dar acceso al procesador de seguridad a un nuevo suministrador de programa. La clave del transmisor es específica de cada usuario y se utiliza en los EMM-U.



EMM: Mensaje de gestión de derechos de acceso
CW: Palabra de control
SK: Clave de servicio (o clave de explotación)
FNCT: Contador de tramas (procedente de la línea 625)
CAFCNT: Cómputo de tramas para acceso condicional (procedente de la línea 625)
E: Derecho de acceso del cliente
IK: Clave del transmisor
UA: Dirección única del receptor
P: Datos de programa
SK (P; CW) : P y CW encriptados con SK
DK (E; S): E y S encriptados con DK
IK (SK; UA): SK encriptado con IK
DK: Clave de distribución
SA: Dirección compartida de receptor

FIGURA 6

Diagrama de bloques general que ilustra la jerarquía de claves de un sistema de acceso condicional

2.2 Jerarquía y actualización de las claves

En la Figura 7 se muestra la utilización funcional de las diferentes claves:

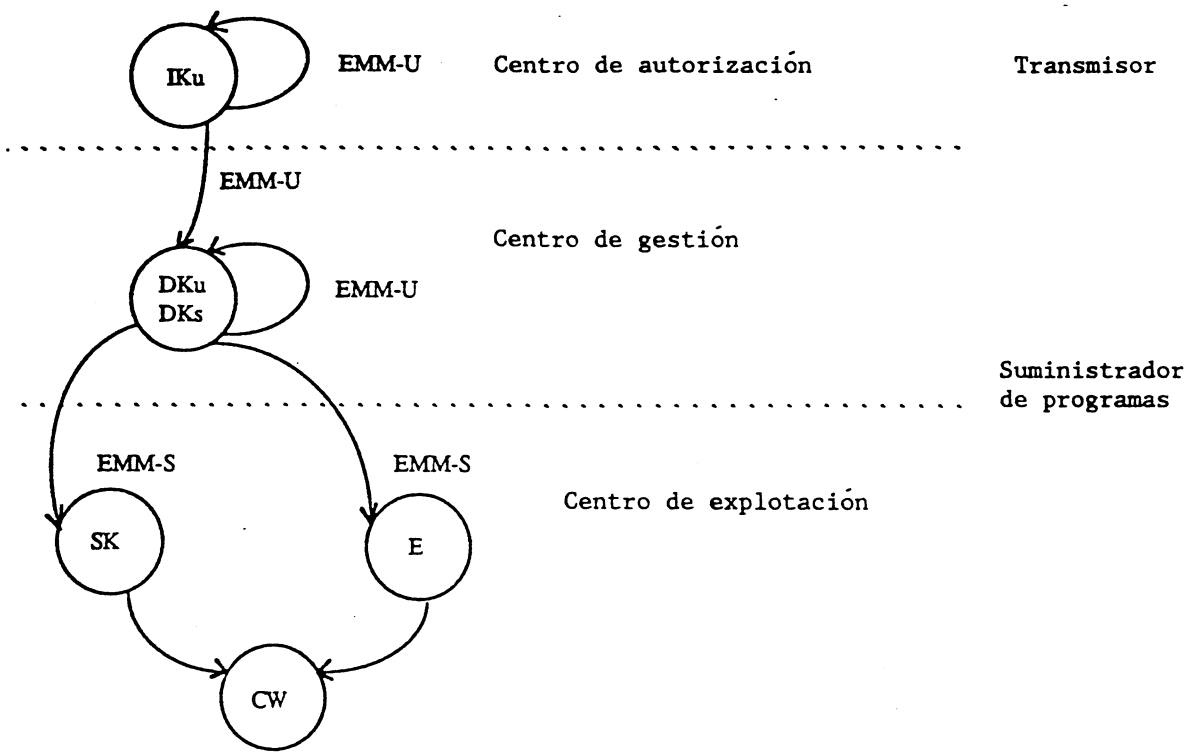


FIGURA 7

Jerarquía de las claves

2.2.1 Clave del transmisor

La clave del transmisor introduce y actualiza todo tipo de claves secretas (DKu, DKs, SK, IKu).

La clave del transmisor es la única capaz de dar acceso a un nuevo suministrador de programas al procesador de seguridad, cargando la primera clave de distribución.

La clave del transmisor se utiliza solamente en mensajes individuales (EMM-U).

2.2.2 Clave de distribución

La clave de distribución única DKu puede actualizar las DKs del servicio a través de los EMM-U.

Las claves de distribución compartidas introducen o actualizan las claves de explotación y de derechos de acceso a través de EMM-S; para esto puede también utilizarse la DKu con un EMM-U, pero este método es menos ventajosos debido al aumento de la velocidad de transmisión de datos.

2.2.3 Clave de explotación

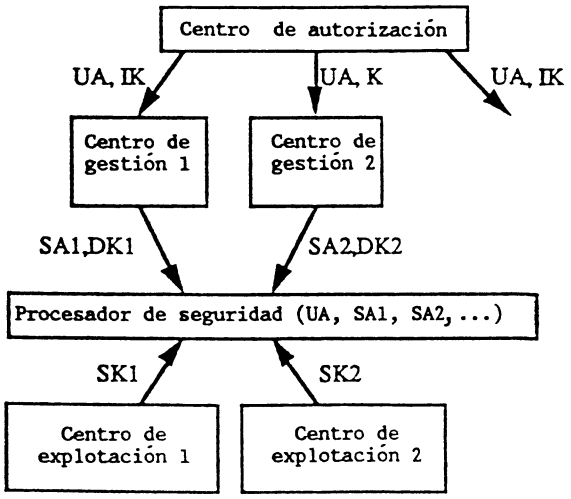
La SK se utiliza para firmar un ECM y para cifrar una palabra de control.

2.2.4 Organización de la jerarquía de claves

Pueden contemplarse dos escenarios principales:

- el centro de autorización se encarga de la gestión de las claves secretas (introducción y actualización);
  - el transmisor introduce y actualiza DKs y SK con IKu;
  - el suministrador de programas actualiza los derechos de acceso E con DKs;
- el centro de autorización se encarga de la inicialización del suministrador de programas pero delega a continuación la gestión de las claves pertenecientes al servicio:
  - el transmisor introduce DKu (utilizando IKu);
  - el suministrador de programas introduce y actualiza DKs, SK y E.

El organigrama de las operaciones se puede representar de la siguiente manera:



Introducción de las claves de distribución

Introducción de la clave de sesión, actualización de los derechos de acceso (y, rara vez, actualización de las claves de distribución y explotación)

Almacenamiento en memoria de las claves de explotación SK1, SK2, ... y de los derechos de acceso

Cálculo de CW

2.3 Seguridad del sistema

2.3.1 Integridad de ECM y EMM

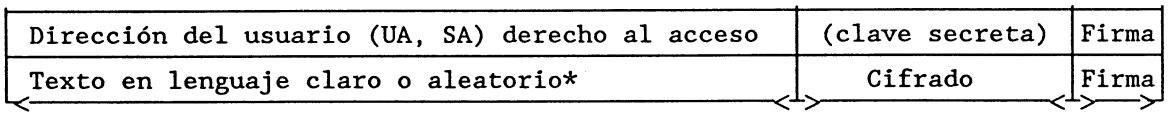
En ECM y EMM se transmiten los dos niveles de datos siguientes:

- datos secretos, transmitidos en forma cifrada (CW, claves secretas),
- datos no secretos cuyo contenido debe gozar de un alto grado de protección (parámetros de acceso condicional, derechos de acceso, dirección única o compartida), y que utilizan un procedimiento de firma.

Es posible que, por razones de reglamentación nacional, haya que enviar los derechos de acceso de manera confidencial, en cuyo caso son aleatorizados. Esta funcionalidad es facultativa.

La estructura de los mensajes es en este caso un texto en lenguaje claro, seguido, llegado el caso, por un campo aleatorizado y terminado por un campo de firma que avala la totalidad del mensaje.

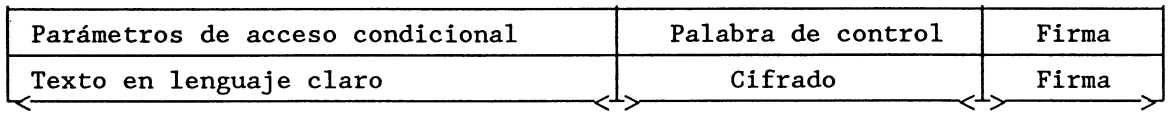
Estructura del EMM:



(clave secreta): facultativa

* El texto aleatorizado es facultativo y no vale más que para la descripción de los derechos de acceso; se puede elegir esta opción por razones de reglamentación nacional.

Estructura de los ECM:



El control de la firma hace imposible la modificación de un campo cualquiera.

2.3.2 Seguridad ofrecida por la jerarquía de claves

La seguridad del sistema se obtiene introduciendo dos niveles diferentes de claves: las claves únicas y las claves compartidas. La posesión de las claves de un servicio es la primera condición para acceder al mismo; la segunda condición es que los derechos de acceso (suscripción, tasación por prestación ...) correspondan a las condiciones de acceso del programa para autorizar la utilización de la clave de explotación SK. Cuando se suprime un abonado, no es necesario cambiar las claves, ya que basta con no actualizar más

los derechos de acceso. Las DKs se utilizan para actualización solamente cuando las claves de explotación han sido descubiertas por piratas. La utilización de claves únicas (IKu o DKu) es excepcional y se reserva para la actualización de las DKs. La actualización de las DKs requiere más capacidad porque hace falta transmitir EMM-U para direccionar individualmente a todos los miembros del grupo. Aunque el uso fraudulento de una clave única no reviste interés, ya que se aplica a un solo usuario, también puede actualizarse este tipo de claves.

2.3.3 Seguridad ofrecida por el procesador de seguridad

El procesador de seguridad debe proporcionar una capacidad de memorización de datos secretos, incluyendo un algorítmo para decodificar los campos cifrados y para controlar la integridad de los datos. El sistema es lo bastante flexible como para permitir la mejora del procesador de seguridad cambiando el algorítmo, aumentando la capacidad de tratamiento (introducción de nuevas condiciones de acceso), etc. sin necesidad de cambiar los receptores. Esta funcionalidad se realiza más fácilmente si el procesador de seguridad es de tipo enchufable (tarjeta inteligente, etc.). El procesador debe estar concebido de manera tal que impida toda utilización del mecanismo de seguridad distinta de aquellas para las que ha sido realizado.

2.3.4 Seguridad de la transmisión

La integridad de la transmisión de todos los parámetros que describen un derecho de acceso (tema/nivel, fechas, crédito, número de programa, etc.) queda asegurada por el método de firma. Este hace imposible modificar con éxito uno o varios bits del mensaje, porque fallaría el control.

Para la transmisión de un crédito se dispone de dos métodos:

- transmisión del monto total de crédito adquirido para un elemento de programa. Ese monto se memoriza en el procesador de seguridad. La compra de cualquier otro programa nuevo sólo es posible si el crédito residual (monto total del crédito, monto total del coste) es superior o igual al coste del programa. El monto total se transmite con una fecha de acreditación;

- transmisión de un suplemento de crédito para un elemento de servicio. El suplemento de crédito se añade al monto total en la tarjeta. Está asociado a una fecha de acreditación para asegurar que no se añada el mismo crédito varias veces en el procesador de seguridad.

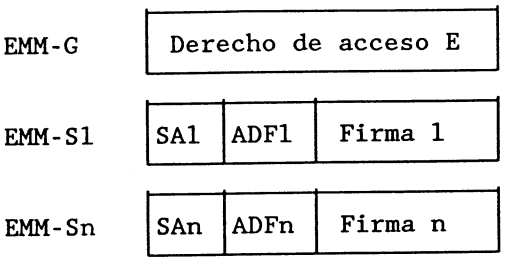
2.4 Mensajes compartidos EMM-S

El objeto de los EMM-S es reducir consiguientemente la velocidad de transmisión de datos de los mensajes de gestión. Los usuarios de un mismo grupo reciben la misma actualización de sus derechos de acceso.

Suponiendo que haya que enviar un derecho de acceso E para actualizar la suscripción de los usuarios, el mensaje puede ser:

- un EMM general (EMM-G), interpretado por todos los receptores, para describir el derecho de acceso común;

- varios EMM-S para direccionar a grupos de usuarios.



en donde:

E : es el derecho de acceso que hay que renovar

SA1 : es la dirección compartida de un grupo de 256 usuarios

ADF1 : es el campo de dirección (256 bits), en el que se atribuye un bit a cada usuario (si el bit es igual a 1, se actualiza el derecho de acceso, si el bit es igual a 0, no se actualiza)

Firma: es la firma de E, SA1, ADF1 utilizando con tal fin la clave de distribución DK1.

Este método permite una consiguiente reducción de la velocidad de transmisión de datos, ya que 256 usuarios comparten un mismo mensaje (lo que contrasta con un EMM-U, donde se utiliza un mensaje por cada usuario).

REFERENCIAS BIBLIOGRÁFICAS

MASON, A. [1986] The principles of the over air addressed pay-per view encryption system for direct broadcasting by satellite and teletext. IERE Conference Publication Nº 69, septiembre de 1986.

UER [1986] Specification of the systems of the MAC/packet family UER Tech.3258.

BIBLIOGRAFÍA

U.K. Department of Trade and Industry, London [1987] World system teletext and data broadcasting specification.