UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T H.233

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

(03/93)

TRANSMISIÓN EN LÍNEA DE SEÑALES NO TELEFÓNICAS

SISTEMAS CON CONFIDENCIALIDAD PARA SERVICIOS AUDIOVISUALES

Recomendación UIT-T H.233

(Anteriormente «Recomendación del CCITT»)

PREFACIO

El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la Unión Internacional de Telecomunicaciones. El UIT-T tiene a su cargo el estudio de las cuestiones técnicas, de explotación y de tarificación y la formulación de Recomendaciones al respecto con objeto de normalizar las telecomunicaciones sobre una base mundial.

La Conferencia Mundial de Normalización de las Telecomunicaciones (CMNT), que se reúne cada cuatro años, establece los temas que habrán de abordar las Comisiones de Estudio del UIT-T, que preparan luego Recomendaciones sobre esos temas.

La Recomendación UIT-T H.233, preparada por la Comisión de Estudio XV (1988-1993) del UIT-T, fue aprobada por la CMNT (Helsinki, 1-12 de marzo de 1993).

NOTAS

1 Como consecuencia del proceso de reforma de la Unión Internacional de Telecomunicaciones (UIT), el CCITT dejó de existir el 28 de febrero de 1993. En su lugar se creó el 1 de marzo de 1993 el Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T). Igualmente en este proceso de reforma, la IFRB y el CCIR han sido sustituidos por el Sector de Radiocomunicaciones.

Para no retrasar la publicación de la presente Recomendación, no se han modificado en el texto las referencias que contienen los acrónimos «CCITT», «CCIR» o «IFRB» o el nombre de sus órganos correspondientes, como la Asamblea Plenaria, la Secretaría, etc. Las ediciones futuras en la presente Recomendación contendrán la terminología adecuada en relación con la nueva estructura de la UIT.

2 Por razones de concisión, el término «Administración» se utiliza en la presente Recomendación para designar a una administración de telecomunicaciones y a una empresa de explotación reconocida.

ÍNDICE

Recomendación H.233

SISTEMAS CON CONFIDENCIALIDAD PARA SERVICIOS AUDIOVISUALES

(Helsinki, 1993)

1 Introducción

Un sistema de privacidad consta de dos partes, el mecanismo de confidencialidad o proceso de criptación de los datos, y un subsistema de gestión de claves.

Esta Recomendación describe la parte de confidencialidad de un sistema de privacidad adecuado para su utilización en los servicios audiovisuales de banda estrecha conformes con las Recomendaciones H.221, H.230, y H.242. Aunque en un sistema de privacidad así se necesita un algoritmo de criptación, la especificación de dicho algoritmo no se incluye aquí: el sistema prevé más de un algoritmo específico.

El sistema de confidencialidad es aplicable a los enlaces punto a punto entre terminales o entre un terminal y una unidad de control multipunto (MCU, *multipoint control unit*); puede extenderse al funcionamiento multipunto, en el que no existe descriptación en el MCU, pero este punto será objeto de estudio ulterior.

2 Propiedades del sistema especificado

2.1 Confidencialidad

1) La confidencialidad es independiente de otros servicios de privacidad proporcionados por el sistema; las claves se proporcionan por otros mecanismos tales como el descrito en el proyecto de Recomendación sobre autenticación y gestión de claves, o pueden introducirse manualmente.

2) Es aplicable a las señales audiovisuales entramadas según la Recomendación H.221, a velocidades de transferencia de $p \times 64$ kbit/s, donde p toma cualquier valor de 1 a 30. De acuerdo con la Recomendación H.221, la propia estructura de trama no está criptada.

3) Se da confidencialidad a todas las transmisiones de audio, vídeo y datos, criptándose estas señales juntas bajo la misma clave (Esto incluye actualmente datos MLP, de acuerdo con el Anexo A/H.221, aunque este aspecto queda en estudio).

4) El sistema es independiente del algoritmo de criptación utilizado; algunos algoritmos han sido proporcionados, y podrían añadirse más algoritmos.

5) El mecanismo de confidencialidad es capaz de funcionar en llamadas punto a punto, y también en llamadas multipunto en las que se permite descriptación en la MCU (la denominada «MCU encargada»).

2.2 Especificación de algoritmos

La especificación de algoritmos no se incluye en esta Recomendación, que prevé una amplia gama de algoritmos de criptación. Las especificaciones deben hallarse en otro lugar (véase 3.2) y contener los siguientes detalles:

- longitudes del vector de inicialización y de las claves de sesión;
- generación de la variable de partida a partir del vector de inicialización.

3 El mecanismo de confidencialidad

3.1 Descripción de la operación

La Figura 1 da un diagrama de bloques de un criptador de enlace. Consta de un bloque criptador y un bloque descriptador. El criptador toma los datos de usuario y los cifra para formar datos cifrados. El descriptador toma los datos cifrados y los descifra para obtener los datos de usuario.

Conectando el criptador y el descriptador hay dos canales. Uno se utiliza para transmitir los datos de usuario cifrados. El segundo es un canal no cifrado conocido como señal de control de criptación (ECS, *encryption control signal*) que se utiliza para transmitir información de control del criptador al descriptador. Aunque estos dos canales se muestran físicamente por separado, en la práctica se multiplexan en un único tren de datos.

Se utilizan técnicas de cifrado de tren aditivo (véase 3.2).

Las claves son proporcionadas por otros mecanismos y se presentan al mecanismo de confidencialidad a medida que se requieren. Son utilizadas por el criptador y el descriptador de manera síncrona con los datos, enviándose vía el canal de control una bandera de claves de nueva carga.

El cifrado de datos es controlado desde el criptador: se envía una bandera vía el canal de control para indicar cuándo se cifran los datos. El descriptador responde a esta bandera y descifra los datos cuando se le solicite.

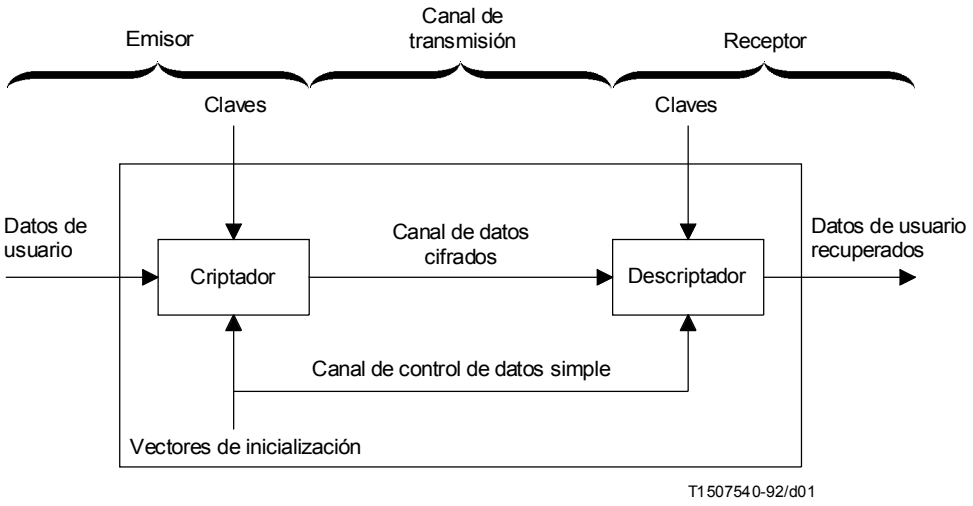


FIGURA 1/H.233

Diagrama de bloques de un criptador de enlace

3.1.1 Control e indicación dentro de la trama Rec. H.221

Para indicar la presencia de un sistema de confidencialidad dentro de un terminal, debe transmitirse el código BAS «Capacidad de criptación». Si esta capacidad es señalizada desde ambos extremos de un enlace, puede abrirse el canal de señal de control criptación (ECS, *encryption control signal*) en cada sentido mediante el comando BAS Encryp-on; el canal ECS puede cerrarse utilizando el comando Encryp-off, pero debe ir precedido por la transmisión de una bandera Encryption-off dentro del propio canal (ver a continuación). Si un terminal recibe la instrucción BAS Encryp-off sin recibir primero la bandera Encryption-off, debe avisarse al usuario de una posible intrusión o funcionamiento incorrecto del sistema de confidencialidad.

En los casos en que se utilice una señal entramada Rec. H.221 en un sentido solamente, el canal ECS puede ser activado sin utilizar el mecanismo de capacidad: el mecanismo para asegurar que el extremo receptor puede descriptar el algoritmo elegido, etc., cae entonces fuera del alcance de esta Recomendación.

3.1.2 Formatos de mensaje

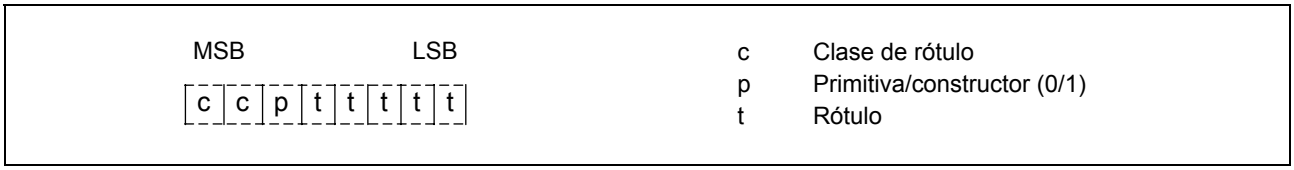
Los mensajes utilizados por el sistema de criptación para la distribución y autenticación de claves se formatan en una forma identificador, longitud, contenido (ILC, *identifier, length content*) nidificada que se describe en la Recomendación X.409. La longitud puede codificarse en forma corta o forma larga. No se utilizará la forma indefinida indicada en la Recomendación X.409.

Los mensajes descritos en esta Recomendación permiten a los diversos mensajes ser identificados por el sistema de criptación. Los mensajes utilizados por el sistema de criptación deben también ser identificados por el sistema de mensajes como pertenecientes al sistema de criptación. Las descripciones de los identificadores utilizados por el sistema de mensajería a tal fin caen fuera del alcance de esta Recomendación.

A continuación figura una breve descripción de algunas de las definiciones de la Recomendación X.409 utilizadas en esta propuesta.

3.1.2.1 Identificador

Un identificador es un octeto cuya estructura es la que se presenta a continuación.



La clase de rótulo define el tipo de identificador que será 10 u 11 (específico del contexto) para los identificadores definidos en esta Recomendación.

El bit de primitiva/constructor (P) indica si el contenido es una primitiva o si se compone de elementos nidificados.

El rótulo de 5 bits define unívocamente el identificador (según su clase).

Por tanto, todos los identificadores de esta Recomendación tienen la forma de octeto: 10 P $t_1\,t_2\,t_3\,t_4\,t_5$ o 11 P $t_1\,t_2\,t_3\,t_4\,t_5$.

3.1.2.2 Longitud

La longitud especifica la longitud de octetos del contenido y es de naturaleza variable.

La forma corta tiene un octeto de longitud y se utilizará con preferencia a la forma larga cuando L es menor que 128. El bit 8 tiene el valor cero y los bits 7-1 codifican L como un número binario sin signo cuyos MSB y LSB son el bit 7 y el bit 1, respectivamente.

La forma larga tiene una longitud de 2 a 127 octetos si se utiliza cuando L es superior o igual a 128 y menor que 2 a la potencia 1008. El bit 8 del primer octeto tiene el valor uno. Los bits 7-1 del primer octeto codifican un número inferior en una unidad al tamaño de la longitud en octetos, como número binario sin signo cuyos MSB y LSB son el bit 7 y el bit 1, respectivamente. El propio L se codifica como un número binario sin signo cuyos MSB y LSB son el bit 8 del segundo octeto y el bit 1 del último octeto, respectivamente. Este número binario será codificado en el menor número posible de octetos, sin octetos delanteros que contengan el valor 0.

3.1.2.3 Cadena de bits

Una cadena de bits en forma primitiva tiene los bits empacados a ocho en un octeto y va precedida por un octeto que codifica el número de bits no utilizados en el octeto final del contenido – de cero a siete – como número binario sin signo. Estos MSB y LSB son el bit 8 y el bit 1, respectivamente.

3.1.3 Canal ECS no cifrado

El sistema de confidencialidad exige la utilización de un canal de control no cifrado entre el criptador y el descriptador. Sólo se necesita un canal de control por sistema de criptación de enlace. El mismo canal de control se utiliza en asociación con la criptación del audio, vídeo y cualesquiera datos que puedan estar presentes.

El contenido del canal ECS se estructura en bloques de 128 bits, síncronos con la multitrama H.221 (véase la Figura 2); por tanto, el primer bit del bloque es el bit 8 del octeto 17 de la trama número 0 en una multitrama. Existen dos tipos de bloques: intercambio de sesión (SE, *session exchange*) y vector de inicialización (IV, *initialisation vector*). La información contenida dentro de un bloque IV surte efecto desde el comienzo de la siguiente multitrama, y sigue siendo efectivo hasta que se ha enviado otro IV. El canal ECS debe siempre contener sea un bloque IV o un bloque SE; durante una sesión, el IV puede repetirse sin variación tan a menudo como sea necesario.

	Bit N.°														
	0	1	2	3	4	5	6	7	8	9	10	11	12-119	120-127
Tipo de SE	0	n	n	s	s	s	s	s	e	e	e	e	mensaje	de reserva
	Bit N.°														
	0	1	2	3	4	5	6	7	8	9	10	11	12-107	108-127
Tipo IV	1	n	n	A	C	C	L	s	e	e	e	e	IV	de reserva

FIGURA 2/H.233

Bloques de canales de control

El bloque contiene lo siguiente:

1) Encabezamiento (12 bits), compuesto por:

   – Bit 0 para seleccionar el tipo: 0 = SE (intercambio de sesión)

   1 = IV (vector de inicialización)

   – Bits 1 y 2 para identificar los bloques de una secuencia multibloque

   00 para una sola frecuencia, no seguida por los bloques correspondientes

   01 para el bloque N.º 1 de una secuencia

   10 para un bloque intermedio de una secuencia

   11 para el último bloque de una secuencia

   – Bit 3 del bloque tipo IV para indicar criptación on/off (A): 1 = ON, 0 = OFF

   – Bits 4 y 5 del bloque de tipo IV para dar la longitud de IV (CC):

   00 = 64 bits + 32 bits de corrección de errores

   01, 10, 11 reservados

   – Bit 6 del bloque tipo IV: reservado para sincronización de carga de claves (L)

   – Todos los demás bits: de reserva puestos a «0»

   – Bits 8-11: corrección de errores para los bits 0-7

2) Bloques SE: 108 bits estructurados como 9 × (8 bits de información + 4 bits de corrección de errores)

   Bloques IV: vector de inicialización del sistema o parte del mismo (64 bits), con protección contra errores (32 bits).

3) Bloques SE: 8 bits de reserva

   Bloques IV: 20 bits de reserva – proporcionan un intervalo para que el sistema actúe sobre la información recibida, y pueden también proporcionar mejora futura.

3.1.3.1 Bloques de intercambio de sesión

En los bloques de tipo SE, los 116 bits que siguen al encabezamiento de bits 8 + 4 están estructurados como $9 \times (8 + 4) + 8$, donde los últimos 8 bits no se utilizan, y las 9 palabras son cada una 8 bits de información con 4 bits de corrección de errores. En el receptor, los bits de información (procedentes de más de un bloque si así se indica en el encabezamiento) se forman para componer un tren, compuesto de mensajes sobre autenticación y gestión de claves, más dos mensajes adicionales P8, P9 definidos a continuación para las capacidades y comandos de algoritmo.

Los 12 bits de las palabras no utilizadas traseras del bloque SE deben ponerse a cero.

Capacidades de algoritmo (P8)

Nombre del mensaje: esta es la información disponible sobre los algoritmos de descriptación (P8).

Identificado del mensaje: 1 1 P t_1 t_2 t_3 t_4 t_5 = 11000000.

Contenido: [número 3-255] [más bytes] en el que el primer byte da el número de los bytes siguientes. Cada conjunto de tres bytes indica un mecanismo de descriptación disponible utilizando los valores listados a continuación como identificadores de medios, identificadores de algoritmo e identificadores de parámetro. Por ejemplo, un terminal capaz de decodificar DES y FEAL transmitiría el mensaje P8 {[11000000][00000110][00000000][00000010][00000000] [00000000][00000001][00000000]}.

Comando de algoritmo (P9)

Nombre del mensaje: esta es la información del algoritmo en uso (P9).

Identificador del mensaje: 1 1 P t_1 t_2 t_3 t_4 t_5 = 11000001.

Significado: cuando el bit encryption-ON es el próximo conjunto en el encabezamiento IV, el algoritmo utilizado es el especificado aquí en este mensaje.

Contenido: bytes del esquema de criptación (mismos valores que en el mensaje de capacidad P8).

Identificadores de medios

Se utiliza un byte para identificar qué elementos del sistema audiovisual son criptados. Cada bit de este byte corresponde al medio siguiente;

1er	bit (LSB):	audio	0 = criptado, 1 = no criptado
2º	bit:	vídeo	0 = criptado, 1 = no criptado
3er	bit:	LSD	0 = criptado, 1 = no criptado
4º	bit:	HSD	0 = criptado, 1 = no criptado
5º	bit:	reservado para MLP, puesto a «0»	
6º	bit:	reservado para H-MLP, puesto a «0»	
7º	bit:	reservado para uso futuro, puesto a «0»	
8º	bit (MSB):	reservado para uso futuro, puesto a «0»	

[00000000] indica que la señal multiplexada (excepto FAS, BAS y ECS) está criptada. Los procedimientos para otros casos quedan en estudio.

Identificadores de algoritmo

Se utiliza un byte para identificación de algoritmo. La definición del algoritmo incluye la especificación completa sobre cómo se obtiene el tren de cifrado a partir de la clave vigente y el valor IV. Actualmente hay identificados varios algoritmos; deben utilizarse los siguientes códigos:

MSB LSB	
0 0 0 0 0 0 0 0	No asignado. Reservado para uso futuro
0 0 0 0 0 0 0 1	«FEAL» (véase el apéndice II.1)
0 0 0 0 0 0 1 0	«DES» (véase el apéndice II.2), modo 1
0 0 0 0 0 0 1 1	Reservado para «DES» (véase el apéndice II.2), modo 2
0 0 0 0 0 1 0 0	Reservado para «DES» (véase el apéndice II.2), modo 3
0 0 0 0 0 1 0 1	Reservado para ISO/CEI Algorithm Register 9979, registration number 000001 (B-CRYPT)
Otros valores	No asignados. Reservados para uso futuro

Identificadores de parámetro

Se utiliza un byte para identificar los parámetros de los algoritmos de criptación que se definen en 3.2. El valor por defecto es [00000000], que puede utilizarse cuando el algoritmo no necesita valores de parámetros.

El equipo debe proporcionar la descriptación de al menos uno de los algoritmos identificados; si se indica más de una capacidad, puede entonces dejarse al operador del sistema la selección del algoritmo necesario para la criptación de la información transmitida.

Otros mensajes

P1 Nombre del mensaje: no se puede criptar.

Significado: el enviador de este mensaje no utilizará un sistema de criptación.

Identificador del mensaje: 1 0 P t_1 t_2 t_3 t_4 t_5 = 10000001.

Contenido: este mensaje no tiene contenido.

P2 Nombre del mensaje: Falla el arranque del sistema de criptación.

Significado: el enviador de este mensaje no ha podido hacer arrancar su sistema de criptación. Esto podría deberse a un fallo en el intercambio de claves, pero por razones de seguridad, no se da ninguna indicación en el mensaje de la causa del fallo.

Identificador del mensaje: 1 0 P t_1 t_2 t_3 t_4 t_5 = 10000010

Contenido: este mensaje no tiene contenido.

3.1.3.2 Vectores de inicialización

La longitud por defecto del IV es 64 bits. La longitud, incluida corrección de errores, es de 96 bits. Pueden transmitirse longitudes IV mayores utilizando más de un bloque. El bit más significativo se transmite primero, es decir, el bit 12 del (primer) bloque de tipo IV.

3.1.3.3 Protección contra errores de la información del canal de control

La información transmitida vía el canal de control debe protegerse contra los errores. Se utiliza para ello un código Hamming [12,8]. Las matrices generadora y de comprobación de paridad se dan en la Figura 3.

El mismo esquema se utiliza para los encabezamientos, para los mensajes de intercambio de sesión y para los vectores de inicialización. En cada caso, un byte de 8 bits va seguido por cuatro bits de corrección de errores.

El IV se divide en 8 bytes, cada uno de los cuales tiene 4 bits de paridad asignados, lo que hace una longitud total IV más paridad de 96 bits, en el caso por defecto.

Matriz generada	Matriz de comprobación de paridad
100000001110 010000000111 001000001010 000100000101 000010001011 000001001100 000000100110 000000010011	1110 0111 1010 0101 1011 1100 0110 0011 1000 0100 0010 0001

T1507550-92/d02

FIGURA 3/H.233

Matrices de corrección de errores

3.2 Método de criptación de la transmisión

Esta cláusula trata de la criptación del audio, vídeo y cualesquiera datos asociados. La criptación sólo tendrá lugar si se establece la alineación de multitrama H.221.

El sistema de criptación realiza las mismas funciones independientemente de la velocidad de transferencia. Pueden criptarse cualquier tren de información de usuario o la totalidad de esos trenes. El sistema de criptación no necesita información sobre la capacidad entre estas diversas formas de información de usuario, ya que cripta los datos después de la multiplexación y descripta los datos antes de la demultiplexación.

El orden temporal de criptación sigue el de la transmisión en un tren serie bit a bit. Los datos deben criptarse antes de que tenga lugar ningún cálculo CRC4. Los cálculos CRC4 se efectúan entonces en los datos criptados, asegurándose de que a cualesquiera redes asociadas se les presente un código CRC4 válido.

Se crea en ambos terminales un tren de cifrado a partir de los valores vigentes de la clave y del vector de inicialización; en el criptador este tren se combina con los bits que han de criptarse por adición en módulo 2, y en el descriptador los bytes criptados se añaden en módulo 2 al mismo tren de cifrado para recuperar la información de liberación del usuario.

Los vectores de inicialización (IV) se crean en forma aleatoria en el criptador y se envían al descriptador a través del ECS. Se utilizan síncronamente con los datos que han de criptarse o descriptarse. Proporcionan un método para resincronizar el criptador y el descriptador periódicamente.

NOTA – Debe prestarse atención al orden de los bits IV cargados en el criptador y el descriptador, según el algoritmo elegido.

Si se perdiera la sincronización, los datos se corromperán hasta que se reciba un nuevo IV. El periodo para la transmisión IV viene determinado por la magnitud de la pérdida de datos que puede ser tolerada hasta que se obtiene resincronización.

Cada bit dentro del canal se trata por el sistema de criptación de una de las tres maneras siguientes (véase el Apéndice I):

a) se genera y se aplica tren de cifrado: información de usuario (audio, vídeo, datos);

b) se genera tren de cifrado, pero no se aplica: FAS y BAS en los canales iniciales y adicionales (véase la Recomendación H.221) y ECS; el tren de cifrado no es almacenado ni retardado para uso posterior, pero se pierde, y no se utiliza para criptar ninguna información siguiente;

c) no se genera ningún tren de cifrado: si la salida de terminal a línea incluye canales que no forman parte de la velocidad de transferencia especificada en el comando BAS pertinente (por ejemplo, TS0 y/o TS16 de una conexión a velocidad primaria, u otros canales no transmitidos extremo a extremo), no se genera para estos bits ningún tren de cifrado.

En la transmisión a 56 kbit/s descrita en el Anexo 2/H.221, se genera tren de cifrado para el octavo subcanal, pero solamente se utilizan los primeros 7 bits para la adición en módulo 2 a la señal de septeto.

En la transmisión restringida a 128 kbit/s o a velocidad superior, se genera tren de cifrado, pero no se aplica al octavo bit de relleno en cada intervalo de tiempo.

El Identificador de Parámetro se pone a [00000000].

Los parámetros operacionales y el método de criptación a utilizar pueden verse en el Apéndice II.

3.3 Procedimiento para la utilización del sistema

Cuando un terminal desea empezar la criptación, habiendo recibido la capacidad «encryp» (véase la Recomendación H.221) en el juego de capacidades del terminal distante, abre el canal ECS y transmite el mensaje (o mensajes) P8. Al recibir el mensaje (o mensajes) P8 desde el extremo distante, comprueba si hay algunos algoritmos/modos compatibles: si no, envía el mensaje P1; si es compatible, envía un mensaje P9 para identificar el algoritmo/modo que será utilizado, e inicia entonces la transmisión de bloques IV.

P2 puede ser utilizado en procedimientos de recuperación de fallo (queda en estudio).

4 Criptación de protocolo multicapa

Queda en estudio.

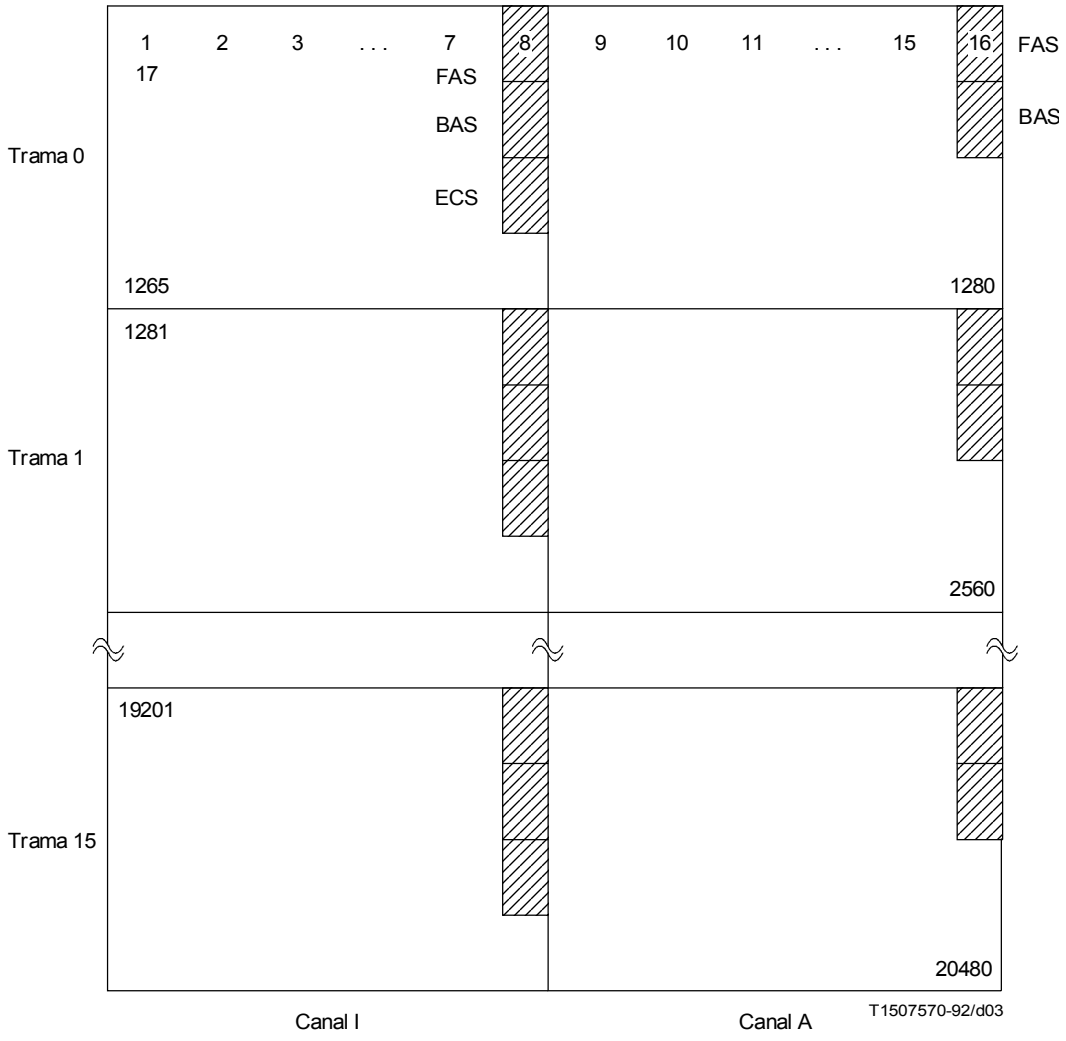
Apéndice I

Criptación y descriptación para dos canales B

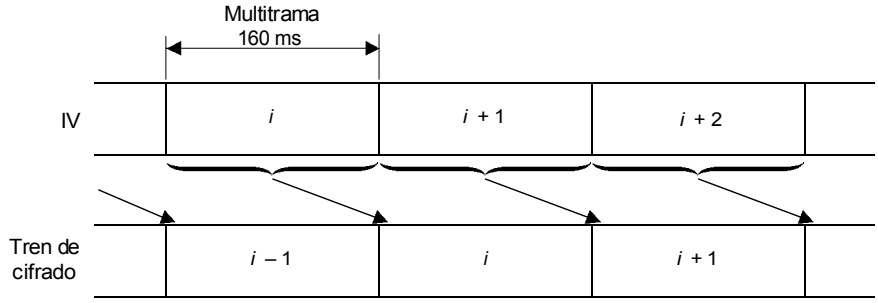
(Este apéndice no es parte integrante de esta Recomendación)

Este apéndice ilustra el modo de funcionar la criptación/descriptación H.233.

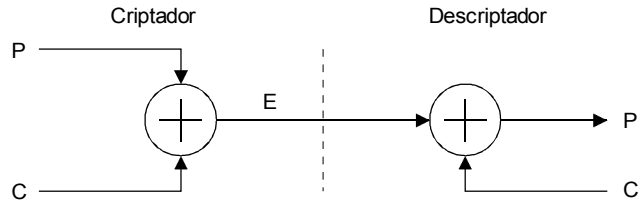
- Se genera un tren de cifrado para todos los bits.
- Se añade un tren de cifrado a todos los bits, salvo a la parte rayada.



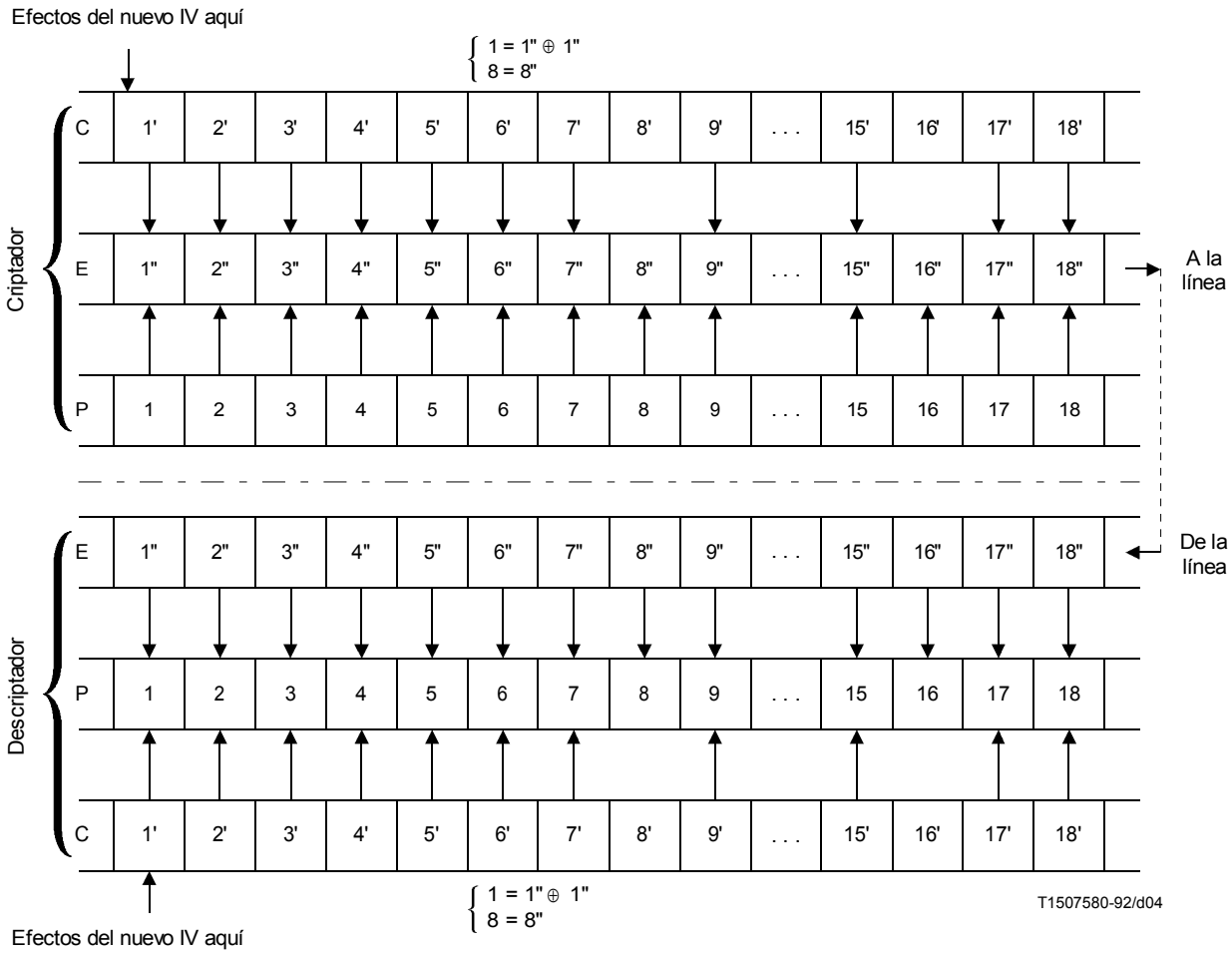
Numeración de bits y bits no cifrados en una multitrama para dos canales B



Generación de tren de cifrado a partir de un nuevo IV



Tren de cifrado aditivo



P Texto claro
C Tren de cifrado
E Texto criptado

Apéndice II

Algoritmos de criptación y parámetros asociados

(Este apéndice no es parte integrante de esta Recomendación)

II.1 FEAL

Se crea un tren de cifrado en ambos terminales a partir de los valores vigentes de la clave y del vector de inicialización utilizando FEAL-8 (FEAL de 8 rondas con clave de 64 bits) del modo realimentación de salaida (OFB, *output feeback*) definido en ISO 8372. En [1] se dan detalles del algoritmo FEAL. En el criptador este tren se combina con los bits que han de criptarse por adición en módulo 2, y en el descriptador, los bits criptados se añaden en módulo 2 al mismo tren de cifrado para recobrar la información de liberación de usuario (véase la Figura II.1).

Variable de partida (SV, *starting variable*) es idéntico al vector de inicialización (IV, *initialization vector*). IV se carga al comienzo de cada multitrama.

De los 64 bits de salida del algoritmo de cifrado, los 8 primeros bits del lado MSB se utilizan para adición en módulo 2 bit a bit a los 8 bits del bloque de señal audiovisual; el primer bit del bloque de cifrado se añade en módulo 2 al primer bit del bloque de señal, y el bit resultante se transmite primero a través del canal, el segundo bit del bloque de cifrado se añade en módulo 2 al segundo bit del bloque de señal y el bit resultante se transmite a continuación a través del canal, y así sucesivamente. Si se transmiten los 8 bits, se genera y utiliza para criptación el siguiente ciclo del tren de cifrado.

II.2 DES

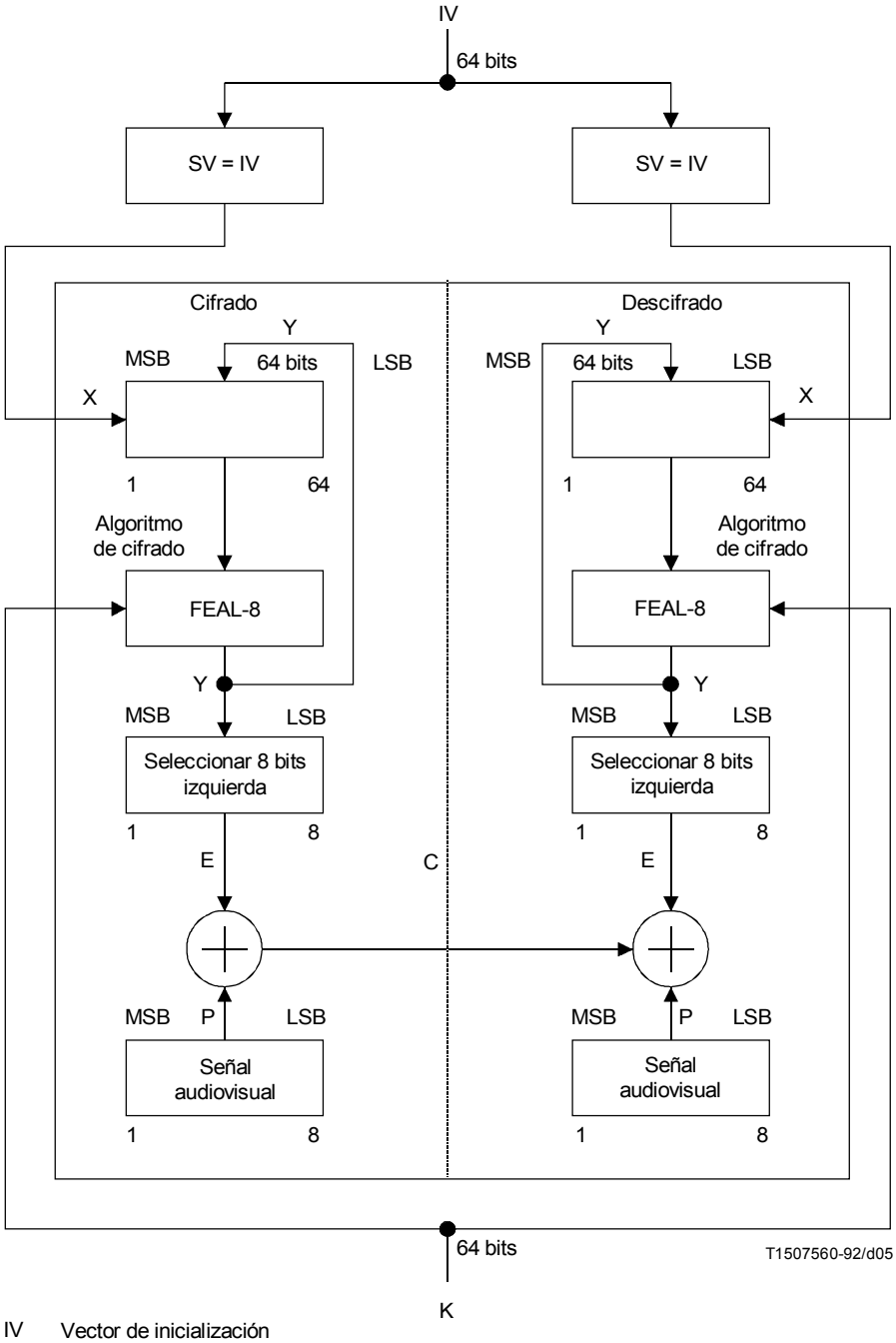
El algoritmo DES se especifica en [2].

Los métodos para aplicar el tren de cifrado al tren de datos se describen en [3].

DES modo 1 utilizará el método designado OFB-8. DES modo 2 y DES modo 3 se reservan para ulterior estudio.

La variable de partida (SV) es idéntica al vector de inicialización (IV).

El identificador de parámetro se pone a [00000000]; todos los demás valores se reservan para ulterior estudio.



IV Vector de inicialización
K Clave
SV Vector de partida

FIGURA II.1/H.233

Operación en modo realimentación de salida para FEAL

Referencias

[1] MIYAGUCHI (S.), KURIHARA (S.), OHTA (K.), MORITA (H.): Expansion of FEAL Cipher, *NTT Review*, Vol. 2, N.° 6, pp.117-127, noviembre de 1990.

[2] Data Encryption Standard, *Federal Information Publication Service (FIPS) Publication 46*, 15 de enero de 1977.

[3] DES Modes of Operation, *FIPS Publication 81*, 2 de diciembre 1980.

Impreso en Suiza

Ginebra, 1994