INTERNATIONAL TELECOMMUNICATION UNION

ITU-T H.233

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(03/93)

LINE TRANSMISSION OF NON-TELEPHONE SIGNALS

CONFIDENTIALITY SYSTEM FOR AUDIOVISUAL SERVICES

ITU-T Recommendation H.233

(Previously "CCITT Recommendation")

FOREWORD

The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the International Telecommunication Union. The ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Conference (WTSC), which meets every four years, established the topics for study by the ITU-T Study Groups which, in their turn, produce Recommendations on these topics.

ITU-T Recommendation H.233 was prepared by the ITU-T Study Group XV (1988-1993) and was approved by the WTSC (Helsinki, March 1-12, 1993).

NOTES

1 As a consequence of a reform process within the International Telecommunication Union (ITU), the CCITT ceased to exist as of 28 February 1993. In its place, the ITU Telecommunication Standardization Sector (ITU-T) was created as of 1 March 1993. Similarly, in this reform process, the CCIR and the IFRB have been replaced by the Radiocommunication Sector.

In order not to delay publication of this Recommendation, no change has been made in the text to references containing the acronyms "CCITT, CCIR or IFRB" or their associated entities such as Plenary Assembly, Secretariat, etc. Future editions of this Recommendation will contain the proper terminology related to the new ITU structure.

2 In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

CONTENTS

Page

1 Introduction 1

2 Properties of the system specified 1

2.1 Confidentiality 1

2.2 Algorithm specification 1

3 The confidentiality mechanism 1

3.1 Description of operation 1

3.1.1 Controls and indication within the H.221 frame 2

3.1.2 Message formats 3

3.1.3 Unenciphered ECS channel 3

3.2 Transmission encryption method 7

3.3 Procedure for use of the system 7

4 Multilayer protocol encryption 7

Appendix I – Encryption and decryption for 2 × B channels 8

Appendix II – Encryption algorithms and their parameters 10

References 11

Recommendation H.233

CONFIDENTIALITY SYSTEM FOR AUDIOVISUAL SERVICES

(Helsinki, 1993)

1 Introduction

A privacy system consists of two parts, the confidentiality mechanism or encryption process for the data, and a key management subsystem.

This Recommendation describes the confidentiality part of a privacy system suitable for use in narrowband audiovisual services conforming to Recommendations H.221, H.230 and H.242. Although an encryption algorithm is required for such a privacy system, the specification of such an algorithm is not included here: the system caters for more than one specific algorithm.

.

The confidentiality system is applicable to point-to-point links between terminals or between a terminal and a multipoint control unit (MCU); it may be extended to multipoint working in which there is no decryption at the MCU, but this is for further study.

2 Properties of the system specified

2.1 Confidentiality

1) Confidentiality is independent of other privacy services provided by the system; keys are provided by other mechanisms such as that described in the draft Recommendation on Authentication and Key Management, or may be manually entered.

2) It is applicable to audiovisual signals framed according to Recommendation H.221, at transfer rates of $p \times 64$ kbit/s where p takes any one value from 1 to 30. In accordance with Recommendation H.221, the frame structure itself is not encrypted.

3) Confidentiality is given to all user audio, video and data transmissions, these signals being encrypted together under the same key (this currently includes MLP data, according to Annex A/H.221, though this aspect is for further study).

4) The system is independent of the encryption algorithm used; some algorithms are currently provided for, and further algorithms could be added.

5) The confidentiality mechanism is capable of working in point-to-point calls, and also in multipoint calls where decryption is permitted at the MCU (the so-called “trusted MCU”).

2.2 Algorithm specification

The specification of algorithms is not included in this Recommendation, which caters to a wide range of encryption algorithms. The specifications must be available elsewhere (see 3.2) and must contain the following details:

– lengths of initialisation vector and session keys;

– generation of starting variable from initialisation vector.

3 The confidentiality mechanism

3.1 Description of operation

Figure 1 gives a block diagram of a link encryptor. It consists of an encryptor block and a decryptor block. The encryptor takes in user data and enciphers it to form enciphered data. The decryptor takes enciphered data and deciphers it to obtain user data.

Connecting the encryptor and decryptor are two channels. One is used to transmit the enciphered user data. The second is an unenciphered channel known as the encryption control signal (ECS) which is used to pass control information from the encryptor to the decryptor. Although these two channels are shown physically separated in practice they are multiplexed into a single data stream.

Additive-stream encipherment techniques are used (see 3.2).

Keys are provided by other mechanisms and are presented to the confidentiality mechanism as required. They are used by the encryptor and decryptor synchronously with the data, a load new key flag being sent via the control channel.

Data encipherment is controlled from the encryptor: a flag is sent via the control channel to indicate when data is being enciphered. The decryptor responds to this flag and deciphers data when requested.

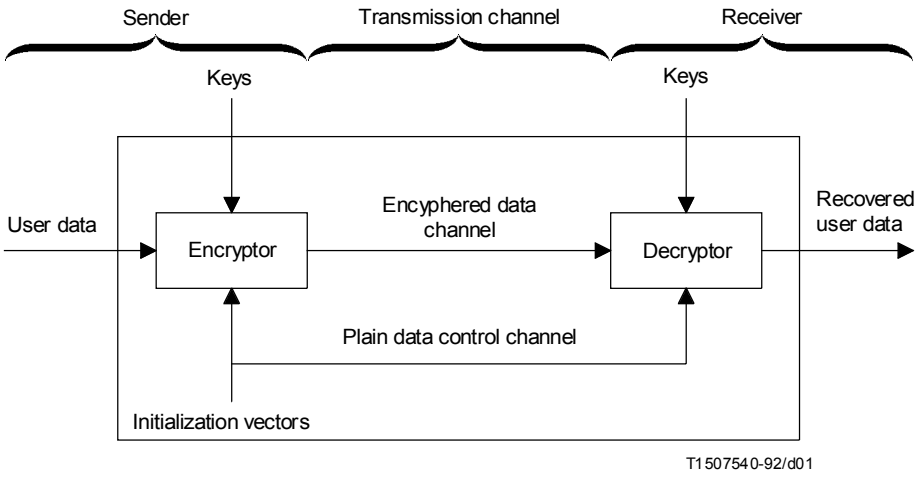


FIGURE 1/H.233

Block diagram of a link encryptor

3.1.1 Controls and indication within the H.221 frame

To indicate the presence of a confidentiality system within a terminal the BAS code "Encryption capability" must be transmitted. If this capability is signalled from both ends of a link, the encryption control signal (ECS) channel may be opened in each direction by use of the encrypt-on BAS command; the ECS channel may be closed using the command encrypt-off, but this must be preceded by the transmission of the encryption-off flag within the channel itself (see below). If a terminal receives the BAS command encrypt-off without first receiving the encryption-off flag, the user should be alerted to a possible intrusion or malfunction of the confidentiality system.

In cases where an H.221-framed signal is in use in one direction only, the ECS channel may be activated without use of the capability mechanism: the mechanism to ensure that the receiving end is able to decrypt the chosen algorithm, etc., is then outside the scope of this Recommendation.

3.1.2 Message formats

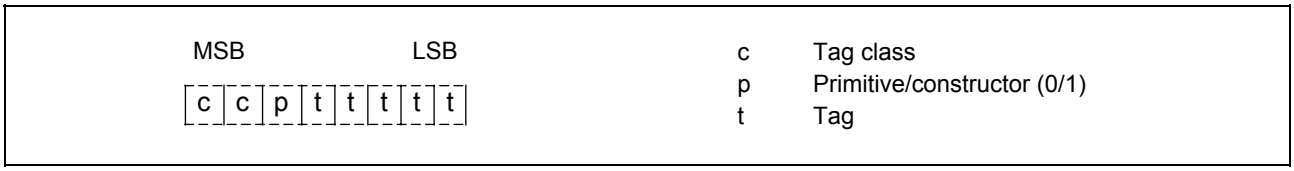
The messages used by the encryption system for key distribution and authentication are formatted in a nested ILC (identifier, length, content) form as described in Recommendation X.409. The length may be encoded in short form or long form. The indefinite form as defined in Recommendation X.409 will not be used.

The messages described in this Recommendation allow the various messages to be identified by the encryption system. The messages used by the encryption system must also be identified by the message system as belonging to the encryption system. The descriptions of the identifiers used by the messaging system for that purpose are beyond the scope of this Recommendation.

A short description of some of the Recommendation X.409 definitions used within this proposal is given below.

3.1.2.1 Identifier

An identifier is an octet with the structure shown next.



The tag class defines the type of identifier which will be 10 or 11 (context specific) for the identifiers defined within this Recommendation.

The primitive/constructor (P) bit indicates whether the content is primitive or whether it is composed of nested elements.

The 5-bit tag uniquely defines the identifier (according to its class).

Thus all identifiers in this Recommendation have the octet form: 10 P t_1 t_2 t_3 t_4 t_5 or 11 P t_1 t_2 t_3 t_4 t_5.

3.1.2.2 Length

The length specifies the length in octets of the contents and is itself variable in length.

The short form is one octet long and shall be used in preference to the long form when L is less than 128. Bit 8 has the value zero and bits 7-1 encode L as an unsigned binary number whose MSB and LSB are bit 7 and bit 1, respectively.

The Long form is from 2 to 127 octets long and is used when L is greater than or equal to 128 and less than 2 to the power 1008. Bit 8 of the first octet has the value one. Bits 7-1 of the first octet encode a number one less than the size of the length in octets as an unsigned binary number whose MSB and LSB are bit 7 and bit 1, respectively. L itself is encoded as an unsigned binary number whose MSB and LSB are bit 8 of the second octet and bit 1 of the last octet, respectively. This binary number shall be encoded in the fewest possible octets, with no leading octets containing the value 0.

3.1.2.3 Bit string

A bit string in primitive form has the bits packed eight to an octet and preceded by an octet that encodes the number of unused bits in the final octet of the contents – from zero to seven – as an unsigned binary number those MSB and LSB are bit 8 and bit 1, respectively.

3.1.3 Unenciphered ECS channel

The confidentiality system requires the use of an unenciphered control channel between encryptor and decryptor. Only one control channel per link encryption system is required. The same control channel is used in association with the encryption of the audio, video and any data that may be present.

The content of the ECS channel is structured in blocks of 128 bits, synchronous with the H.221 multiframe (see Figure 2); thus the first bit of the block is bit 8 of octet 17 of frame number 0 in a multiframe. There are two types of block: session exchange (SE) and initialisation vector (IV). The information contained within an IV block takes effect from the start of the next multiframe, and remains effective until another TV has been sent. The ECS channel must always contain either an IV block or an SE block; during a session the IV may be repeated without change as often as necessary.

	Bit No.														
	0	1	2	3	4	5	6	7	8	9	10	11	|	12-119	| 120-127
SE Type	0	n	n	s	s	s	s	s	e	e	e	e	|	message	| spare
	Bit No.														
	0	1	2	3	4	5	6	7	8	9	10	11	|	12-107	| 108-127
IV Type	1	n	n	A	C	C	L	s	e	e	e	e	|	IV	| spare

FIGURE 2/H.233

Control channel blocks

The block contains the following :

1) Header (12 bits), consisting of:

   – Bit 0 to select type: 0 = SE (session exchange)

   1 = IV (initialisation vector)

   – Bits 1 and 2 to identify the blocks of a multi-block sequence

   00 for a single block, not followed by related blocks

   01 for block #1 of a sequence of several blocks

   10 for an intermediate block in a sequence

   11 for the last block of a sequence

   – Bit 3 of IV-type block to indicate encryption on/off (A):

   1 = ON, 0 = OFF

   – Bits 4 and 5 of IV-type block to give length of IV (CC):

   00 = 64 bits + 32 bits error correction

   01, 10, 11 reserved

   – Bit 6 of IV-type block: reserved for key-loading synchronisation (L)

   – All other bits: spare(s) set to "0"

   – Bits 8-11: error correction for bits 0-7

2) SE Blocks: 108 bits structured as 9 × (8 information bits + 4 error correction bits)

   IV Blocks: System Initialisation Vector or part thereof (64 bits), with error protection (32 bits).

3) SE Blocks: 8 spare bits

   IV Blocks: 20 spare bits – provide an interval for the system to act upon the information received, and may also provide for future enhancement.

3.1.3.1 Session exchange blocks

In SE-type blocks, the 116 bits following the 8 + 4 bit header are structured as $9 \times (8 + 4) + 8$, where the last 8 bits are not used, and the 9 words are each 8 information bits with 4 error-correction bits. At the receiver, the information bits (from more than one block if so indicated in the header) are formed into one stream, consisting of messages on authentication and key management, plus two additional messages P8, P9 defined below for the algorithm capabilities and commands.

All 12 bits of trailing unused words in the SE block must be set to zero.

Algorithm capabilities (P8)

Message name: Here is decryption – algorithms-available information (P8)

Message identifier: 1 1 P t_1 t_2 t_3 t_4 t_5 = 11000000

Content: [number 3-255][more bytes] where the first byte gives the number of following bytes. Each set of three bytes indicates an available decryption mechanism using the values listed under media identifiers, algorithm identifiers, and parameter identifiers listed below. For example, a terminal capable of decoding DES and FEAL would transmit the P8 message {[11000000][00000110][00000000][00000010][00000000][00000000][00000001][00000000]}

Algorithm command (P9)

Message name: Here is algorithm-in-use information (P9)

Message identifier: 1 1 P t_1 t_2 t_3 t_4 t_5 = 11000001

Meaning: when the encryption-ON bit is next set in the IV header, the algorithm used is that specified here in this message.

Content: encryption scheme bytes (same values as in the capability message P8)

Media identifiers

One byte is used for identifying which elements of the audiovisual signal are encrypted. Each bit of this byte corresponds to the following medium;

1st bit (LSB): Audio 0 = encrypted, 1 = unencrypted

2nd bit: Video 0 = encrypted, l = unencrypted

3rd bit: LSD 0 = encrypted, 1 unencrypted

4th bit: HSD 0 = encrypted, 1 unencrypted

5th bit: reserved for MLP, set to "0"

6th bit: reserved for H-MLP, set to "0"

7th bit: reserved for future use, set to "0"

8th bit(MSB): reserved for future use, set to "0"

[00000000] represents that the multiplexed signal (except FAS, BAS and ECS) is encrypted. Procedures for other cases are under study.

Algorithm identifiers

One byte is used for algorithm identification. The definition of the algorithm includes the complete specification as to how the cipher stream is obtained from the current key and IV value. Currently several algorithms have been identified; the following codes should be used:

MSB LSB	
0 0 0 0 0 0 0 0	Not allocated. Reserved for future use
0 0 0 0 0 0 0 1	"FEAL" (see Appendix II.1)
0 0 0 0 0 0 1 0	"DES" (see Appendix II.2), Mode 1
0 0 0 0 0 0 1 1	Reserved for "DES" (see Appendix II.2), Mode 2
0 0 0 0 0 1 0 0	Reserved for "DES" (see Appendix II.2), Mode 3
0 0 0 0 0 1 0 1	Reserved for ISO/IEC 9979 algorithm register, Registration number 000001 (B-CRYPT)
Other values	Not allocated. Reserved for future use

Parameter identifiers

One byte is used for identifying parameters of the encryption algorithms which are defined in 3.2. Default value is [00000000], which may be used when the algorithm does not need parameter values.

Equipment should provide for decryption of at least one of the identified algorithms; if more than one capability is indicated then it may be left to the operator of the system to select the required algorithm for the encryption of the transmitted information.

Other messages

P1 Message Name: Cannot encrypt

Meaning: The sender of this message will not use an encryption system.

Message identifier: 1 0 P t_1 t_2 t_3 t_4 t_5 = 10000001

Content: This message has no content.

P2 Message name: Failure to start encryption system

Meaning: The sender of this message has failed to start its encryption system. This could be due to a key exchange failure, but for security reasons, no indication of the cause of failure is given in the message.

Message identifier: 1 0 P t_1 t_2 t_3 t_4 t_5 = 10000010

Content: This message has no content.

3.1.3.2 Initialisation vectors

The default length of the IV is 64 bits. The length including error correction is 96 bits. Greater IV lengths can be transmitted using more than one block. The most-significant bit is transmitted first, that is, bit 12 of (first) IV-type block.

3.1.3.3 Error protection of control channel information

The information transmitted via the control channel must be error protected. A [12,8] hamming code is used for this. The generator and parity check matrices are given in Figure 3.

The same scheme is used for headers, for session exchange messages and for initialisation vectors. In each case an 8-bit byte is followed by four error correction bits.

The IV is split into 8 bytes, each byte then having 4 parity bits attached making a total IV plus parity length of 96 bits, in the default case.

Generator matrix	Parity check matrix
100000001110 010000000111 001000001010 000100000101 000010001011 000001001100 000000100110 000000010011	1110 0111 1010 0101 1011 1100 0110 0011 1000 0100 0010 0001

T1507550-92/d02

FIGURE 3/H.233

Error correction matrices

3.2 Transmission encryption method

This subclause deals with the encryption of the audio, video and any associated data. Encryption will only take place if H.221 multiframe alignment is established.

The encryption system performs the same functions regardless of the transfer rate. Any or all of the user information streams may be encrypted. The encryption system does not need information as to the allocation of the capacity between these various forms of user information, as it encrypts data after multiplexing and decrypts data before demultiplexing.

The temporal order of encryption follows that of transmission in a serial stream bit by bit. Data must be encrypted before any CRC4 calculation takes place. CRC4 calculations are then performed on encrypted data, ensuring that any associated networks are presented with a valid CRC4 code.

A cipher streams is created at both terminals from the current values of the key and the initialisation vector; at the encryptor this stream is combined with the bits to be encrypted by modulo-2 addition, and at the decryptor the encrypted bits are modulo-2-added to the same cipher stream to recover the clear user information.

Initialisation vectors (lVs) are created in a random way at the encryptor and are sent to the decryptor via the ECS. They are used synchronously with the data to be encrypted or decrypted. They provide a method of re-synchronising the encryptor and decryptor periodically.

NOTE – Attention must be paid to the order of IV bits loaded to the encryptor and decryptor, according to the chosen algorithm.

Should synchronisation be lost data will be corrupted until a new IV is received. The period for IV transmission is determined by the amount of data loss which can be tolerated until re-synchronisation is obtained.

Each bit within the channel is treated by the encryption system in one of the three following ways (see Appendix I):

a) cipher stream is generated and applied: user information (audio, video, data);

b) cipher stream is generated, but not applied: FAS and BAS in initial and additional channels (see Recommendation H.221) and ECS; the cipher stream is not stored or delayed for subsequent use, but is lost, and is not used to encrypt any following information;

c) no cipher stream is generated: if the terminal output to line includes channels not forming part of the transfer rate specified in the relevant BAS command (e.g. TS0 and/or TS16 of a primary rate connection, or other channels not transmitted end to end), no cipher stream is generated for these bits.

For the 56 kbit/s transmission as described in Annex 2/H.221, cipher stream is generated for the eighth sub-channel but only the first 7 bits are used for modulo-2 addition to the septet signal.

For the restricted 128 kbit/s or higher bit rate transmission, the cipher stream is generated but not applied to the stuffed eighth bit in every timeslot.

The parameter identifier is set to [00000000].

For the operational parameters for each encryption method to be used, refer to Appendix II.

3.3 Procedure for use of the system

When a terminal wishes to start encryption, having received the capability “encryp.” (see Recommendation H.221) in the capset of the remote terminal, it opens the ECS channel and transmits message(s) P8. On receipt of message(s) P8 from the remote end it checks whether there are any compatible algorithms/modes: if not, it sends the message Pl; if compatible, it sends a message P9 to identify the algorithm/mode which will be used, and then begins the transmission of IV blocks.

P2 may be used in failure recovery procedures (for further study).

4 Multilayer protocol encryption

For further study.

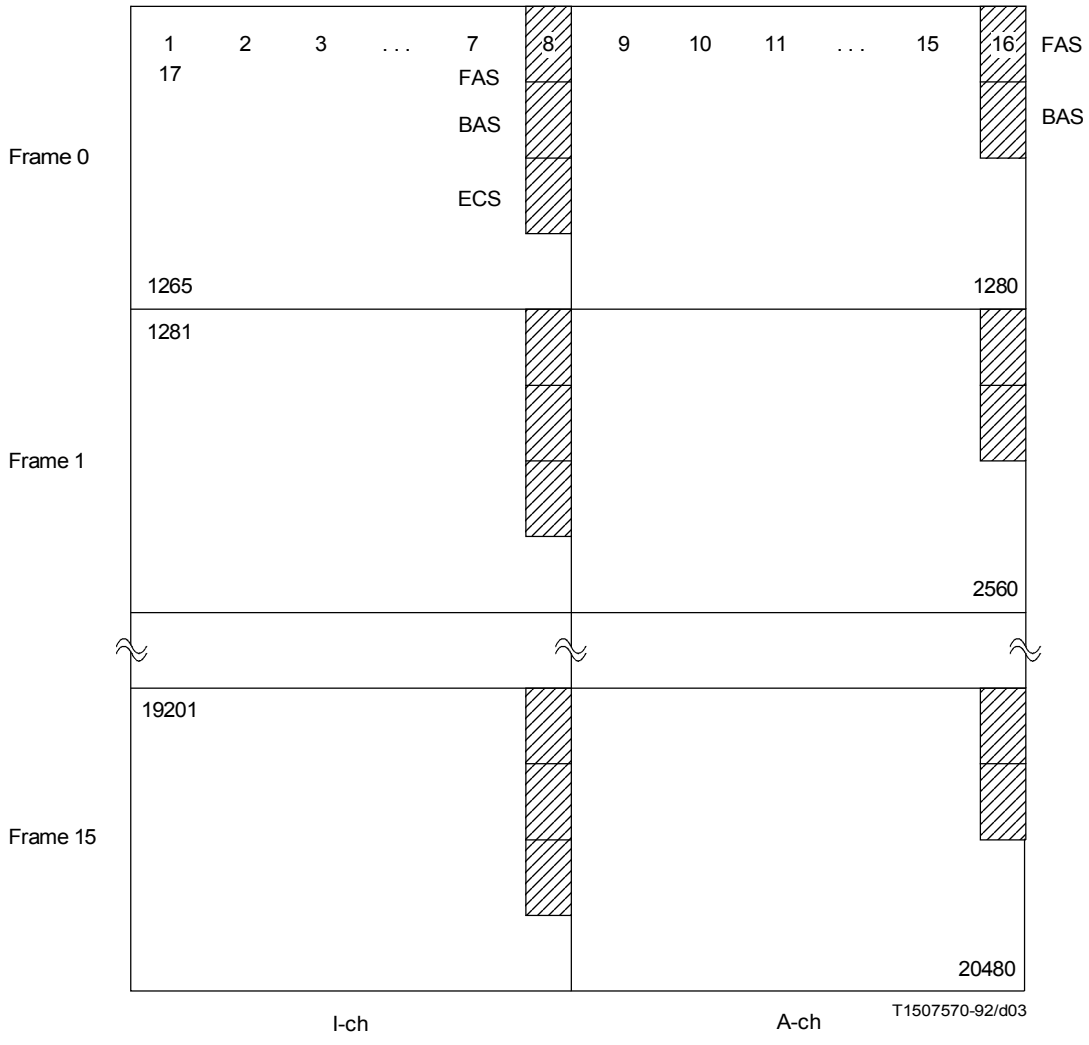
Appendix I

Encryption and decryption for 2 × B channels

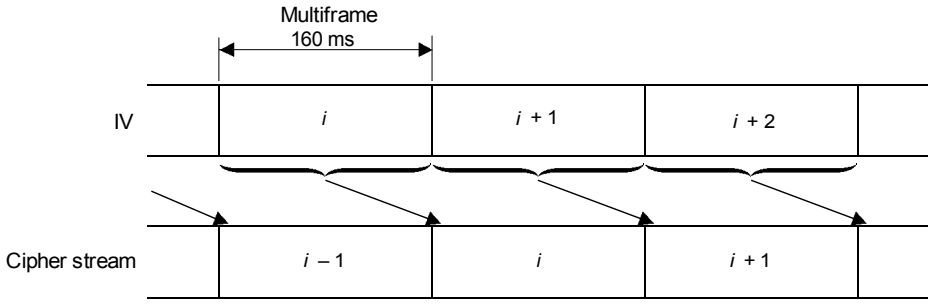
(This appendix does not form an integral part of this Recommendation)

This appendix serves as an illustration for how H.233 encryption/decryption works.

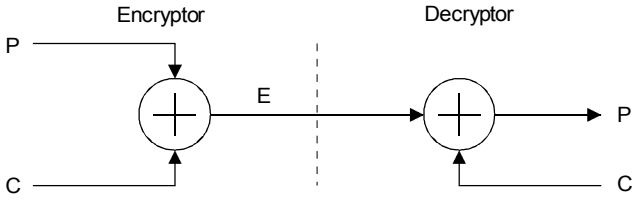
- Cipher stream is generated for all bits;
- Cipher stream is added to all bits except the hatched part.



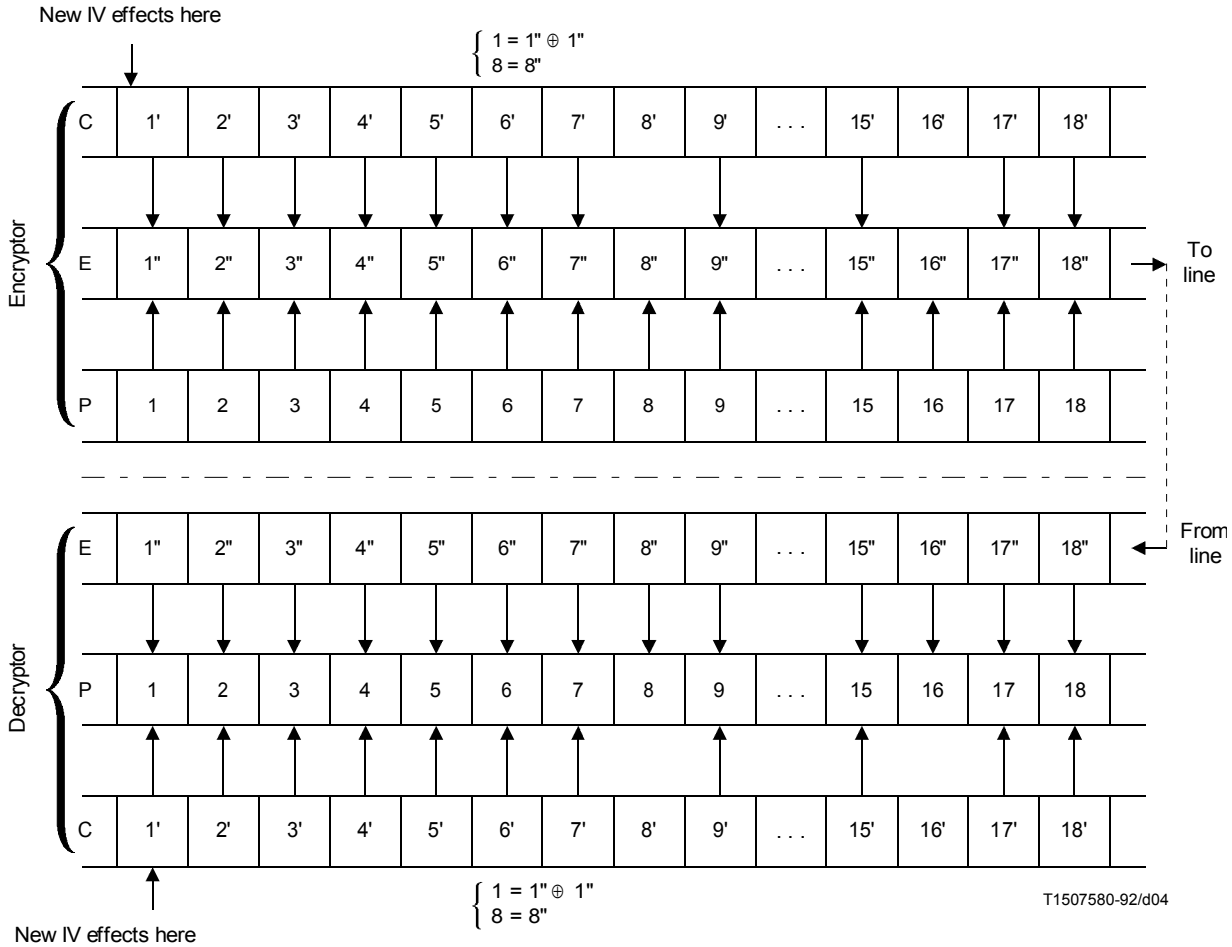
Bit numbering and unenciphered bits in a multiframe for 2 × B channel



Cipher stream generation from new IV



Additive stream cipher



P Plain text
C Cipher stream
E Encrypted text

Appendix II

Encryption algorithms and their parameters

(This appendix does not form an integral part of this Recommendation)

II.1 FEAL

A cipher stream is created at both terminals from the current values of the key and the initialisation vector using FEAL-8 (8 round FEAL with 64-bit key) in the OFB mode defined ISO8372. Details of FEAL algorithm are given in [1]. At the encryptor this stream is combined with the bits to be encrypted by modulo-2 addition, and at the decriptor the encrypted bits are modulo-2 added to the same cipher stream to recover the clear user information. See Figure II.1.

Starting variable (SV) is identical to initialisation vector (IV). IV is loaded at the start of every multiframe.

Out of the 64 bits output from the encipherment algorithm, the first 8 bits of the MSB side are used for bit-by-bit modulo-2 addition to the 8 bits of the audiovisual signal block; the first bit of the cipher block is modulo-2 added to the first bit of the signal block and the resultant bit is transmitted first through the channel, the second bit of the cipher block is modulo-2 added to the second bit of the signal block and the resultant bit is transmitted next through the channel, and so on. If all of the 8 bits are transmitted, the next cycle of the cipher stream is generated and used for encryption.

II.2 DES

The DES algorithm is specified in [2].

The methods of applying the cipher stream to the data stream are described in [3].

DES mode 1 will use the method designated OFB-8, DES mode 2 and DES mode 3 are reserved for further study.

The starting variable (SV) is identical to the initialisation vector (IV).

The parameter identifier is set to [00000000], all other values are reserved for further study.

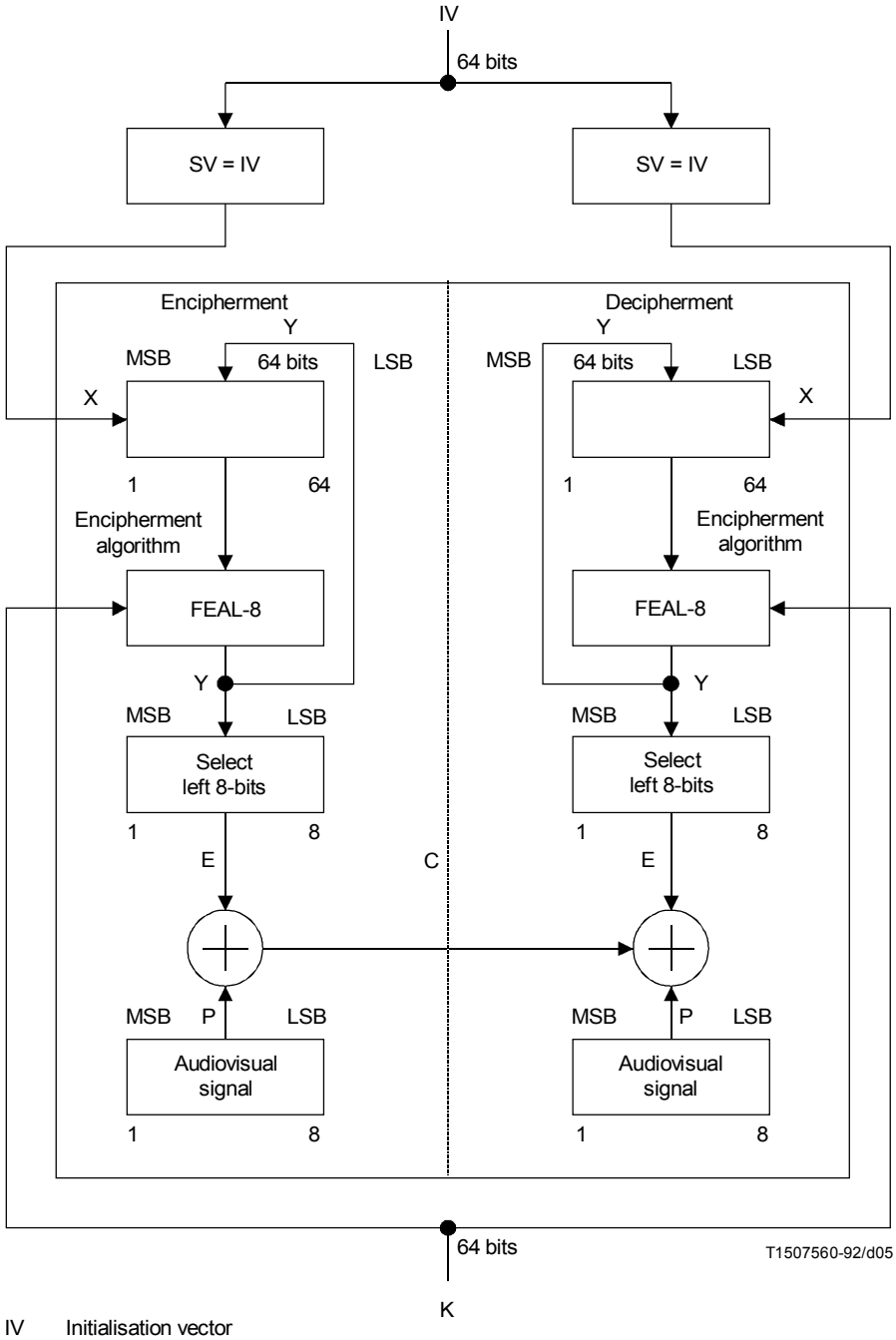


FIGURE II.1/H.233

Output feedback (OFB) mode operation for FEAL

References

[1] MIYAGUCHI (S.), KURIHARA (S.), OHTA (K.), MORITA (H.): Expansion of FEAL Cipher, *NTT Review*, Vol. 2, No. 6, pp.117-127, November 1990.

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

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

Printed in Switzerland

Geneva, 1994