UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T H.233

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(03/93)

UTILISATION DES LIGNES POUR LA TRANSMISSION DES SIGNAUX AUTRES QUE TÉLÉPHONIQUES

SYSTÈME DE CONFIDENTIALITÉ POUR LES SERVICES AUDIOVISUELS

Recommandation UIT-T H.233

(Antérieurement «Recommandation du CCITT»)

AVANT-PROPOS

L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'Union internationale des télécommunications (UIT). Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

La Conférence mondiale de normalisation des télécommunications (CMNT), qui se réunit tous les quatre ans, détermine les thèmes que les Commissions d'études de l'UIT-T doivent examiner et à propos desquels elles doivent émettre des Recommandations.

La Recommandation UIT-T H.233, élaborée par la Commission d'études XV (1988-1993) de l'UIT-T, a été approuvée par la CMNT (Helsinki, 1-12 mars 1993).

NOTES

1 Suite au processus de réforme entrepris au sein de l'Union internationale des télécommunications (UIT), le CCITT n'existe plus depuis le 28 février 1993. Il est remplacé par le Secteur de la normalisation des télécommunications de l'UIT (UIT-T) créé le 1er mars 1993. De même, le CCIR et l'IFRB ont été remplacés par le Secteur des radiocommunications.

Afin de ne pas retarder la publication de la présente Recommandation, aucun changement n'a été apporté aux mentions contenant les sigles CCITT, CCIR et IFRB ou aux entités qui leur sont associées, comme «Assemblée plénière», «Secrétariat», etc. Les futures éditions de la présente Recommandation adopteront la terminologie appropriée reflétant la nouvelle structure de l'UIT.

2 Dans la présente Recommandation, le terme «Administration» désigne indifféremment une administration de télécommunication ou une exploitation reconnue.

TABLE DES MATIÈRES

Recommandation H.233

SYSTÈME DE CONFIDENTIALITÉ POUR LES SERVICES AUDIOVISUELS

(Helsinki, 1993)

1 Introduction

Un système de protection des données privées comprend deux parties, le mécanisme de confidentialité ou processus de chiffrement des données, et un sous-système de gestion de clés.

La présente Recommandation décrit la partie mécanisme de confidentialité d'un système de protection des données privées destiné à être utilisé dans les services audiovisuels à bande étroite conformes aux Recommandations H.221, H.230 et H.242. Bien qu'un tel système de protection des données privées nécessite un algorithme de chiffrement, la spécification de cet algorithme n'est pas incluse ici: le système admet plusieurs algorithmes spécifiques.

Le système de confidentialité est applicable aux liaisons point à point entre terminaux ou entre un terminal et un pont de conférence (MCU) (*multipoint control unit*); son application peut être élargie au fonctionnement multipoint sans chiffrement dans le pont de conférence, mais cette question fera l'objet d'un complément d'étude.

2 Propriétés du système spécifié

2.1 Confidentialité

1) La confidentialité est indépendante des autres services de protection des données privées assurés par le système; les clés sont fournies par d'autres mécanismes tels que celui qui est décrit dans le projet de Recommandation sur l'authentification et la gestion des clés, ou peuvent être introduites manuellement.

2) La confidentialité est applicable aux signaux audiovisuels dont le verrouillage de trame est conforme à la Recommandation H.221, aux débits utiles de $p \times 64$ kbit/s, où p prend une valeur quelconque de 1 à 30. Conformément à la Recommandation H.221, la structure de trame elle-même n'est pas chiffrée.

3) La confidentialité est assurée pour toutes les transmissions audio, vidéo et de données des usagers, ces signaux étant chiffrés ensemble avec la même clé (sont actuellement incluses ici les données MLP, conformément à l'Annexe A/H.221, bien que cet aspect nécessite un complément d'étude).

4) Le système est indépendant de l'algorithme de chiffrement utilisé; certains algorithmes sont actuellement prévus, auxquels d'autres pourront venir s'ajouter.

5) Le mécanisme de confidentialité peut fonctionner dans le cas de communications point à point, mais aussi dans le cas de communications multipoint pour lesquelles le déchiffrement est autorisé dans le pont de conférence (dit «sûr»).

2.2 Spécification des algorithmes

La spécification des algorithmes n'est pas incluse dans la présente Recommandation, qui s'applique à un large éventail d'algorithmes de chiffrement. Les spécifications doivent être recherchées ailleurs (voir 3.2) et devront contenir les précisions suivantes:

- longueurs du vecteur d'initialisation et des clés de session;
- génération de la variable initiale par le vecteur d'initialisation.

3 Le mécanisme de confidentialité

3.1 Description du fonctionnement

La Figure 1 montre le schéma fonctionnel d'un module de chiffrement, avec ses blocs de chiffrement et de déchiffrement. Le module de chiffrement reçoit les données d'usager qu'il convertit en données chiffrées. Le module de déchiffrement reçoit les données chiffrées qu'il déchiffre pour obtenir les données d'usager.

Deux canaux permettent le raccordement du module de chiffrement et du module de déchiffrement. Le premier canal est utilisé pour transmettre les données d'usager chiffrées. Le second est un canal non chiffré appelé signal de commande de chiffrement (ECS) (*encryption control signal*) qui est utilisé pour transmettre les informations de commande du module de chiffrement au module de déchiffrement. Bien que ces deux canaux soient représentés séparément sur la figure, dans la pratique ils sont multiplexés en un train de données unique.

Des techniques de chiffrement série sont utilisées (voir 3.2).

Les clés sont fournies par d'autres mécanismes et sont présentées au mécanisme de confidentialité lorsque besoin est. Elles sont utilisées par les unités de chiffrement et de déchiffrement simultanément avec les données, un changement de clés étant signalé par un drapeau sur le canal de commande.

Le chiffrement des données se fait sous la conduite du module de chiffrement: un drapeau envoyé par l'intermédiaire du canal de commande indique le début du chiffrement des données. Le module de déchiffrement répond à ce drapeau et déchiffre les données lorsque la demande lui en est faite.

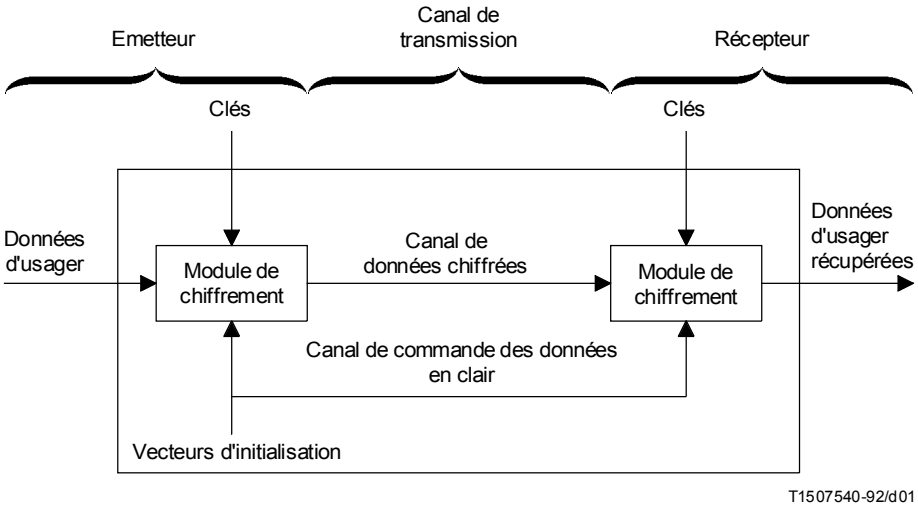


FIGURE 1/H.233

Schéma fonctionnel d'un module de chiffrement de liaison

3.1.1 Commandes et indication dans la trame de la Recommandation H.221

Pour indiquer la présence d'un système de confidentialité dans un terminal, il est nécessaire de transmettre le code «possibilité de chiffrement» du BAS. Si cette possibilité est signalée par les deux extrémités d'une liaison, le canal signal de commande de chiffrement (ECS) peut être ouvert dans chaque direction grâce à l'utilisation de la commande chiffrement en service du BAS; le canal ECS peut être fermé à l'aide de la commande chiffrement hors service, mais cette commande doit être précédée par la transmission du drapeau chiffrement hors service dans le canal même (voir ci-dessous). Si un terminal reçoit la commande chiffrement hors service du BAS sans avoir reçu préalablement le drapeau chiffrement hors service, il convient d'éveiller l'attention de l'usager sur la possibilité d'une intrusion dans le système de confidentialité ou d'un mauvais fonctionnement de celui-ci.

En cas d'utilisation dans une direction seulement d'un signal avec verrouillage de trame conforme à la Recommandation H.221, le canal ECS peut être activé sans que la possibilité de chiffrer soit signalée: le mécanisme qui permet au récepteur de déchiffrer l'algorithme choisi, ou autre, n'entre pas dans le cadre de la présente Recommandation.

3.1.2 Formats des messages

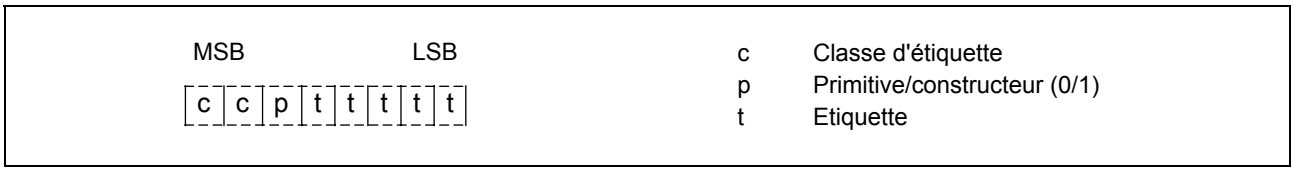
Les messages utilisés par le système de chiffrement pour la distribution des clés et l'authentification ont un format de type identificateur, longueur, contenu (ILC) (*identifier, length, content*) avec entrelacement, comme indiqué dans la Recommandation X.409. Le codage de la longueur peut être de forme courte ou de forme longue. La forme indéfinie spécifiée dans la Recommandation X.409 ne sera pas utilisée.

Les messages décrits dans la présente Recommandation permettent au système de chiffrement d'identifier les différents messages. Les messages utilisés par le système de chiffrement doivent en outre être reconnus par le système de transmission comme appartenant au système de chiffrement. Les descriptions des identificateurs utilisés à cet effet par le système d'échange de messages n'entrent pas dans le cadre de la présente Recommandation.

Un bref rappel de quelques-unes des définitions de la Recommandation X.409 utilisées dans le cadre de la présente proposition est présenté ci-dessous.

3.1.2.1 Identificateur

Un identificateur est un octet dont la structure est la suivante:



La classe d'étiquette définit le type d'identificateur qui aura la valeur 10 ou 11 (en fonction du contexte) pour les identificateurs définis dans la présente Recommandation.

Le bit primitive/constructeur (P) indique si le contenu est une primitive ou s'il est composé d'éléments entrelacés.

L'étiquette de 5 bits définit exceptionnellement l'identificateur (selon sa classe).

Les identificateurs qui figurent dans le présent document se présentent donc tous sous la forme d'un octet du type: 10 P t_1 t_2 t_3 t_4 t_5 ou 11 P t_1 t_2 t_3 t_4 t_5.

3.1.2.2 Longueur

La longueur du contenu, exprimée en nombre d'octets, est elle-même variable.

La forme courte, qui est d'un octet, est à utiliser de préférence à la forme longue lorsque L est inférieur à 128. Le bit 8 a la valeur 0 et les bits 7 à 1 codent L sous forme de nombre binaire sans signe dont le bit de poids fort et le bit de poids faible sont respectivement le bit 7 et le bit 1.

La forme longue, qui varie de 2 à 127 octets, est utilisée lorsque L est supérieur ou égal à 128 et inférieur à 2 à la puissance 1008. Le bit 8 du premier octet a la valeur 1. Les bits 7 à 1 du premier octet servent à coder un nombre inférieur d'une unité à la longueur en octets, sous la forme d'un nombre binaire sans signe dont le bit de poids fort et le bit de poids faible sont respectivement le bit 7 et le bit 1. L lui-même est codé sous la forme d'un nombre binaire sans signe dont le bit de poids fort et le bit de poids faible sont respectivement le bit 8 du deuxième octet et le bit 1 du dernier octet. Ce nombre binaire doit être codé en un nombre aussi faible que possible d'octets, sans octet de gauche contenant la valeur 0.

3.1.2.3 Chaîne binaire

Une chaîne binaire en forme de primitive compte huit bits par octet, précédés d'un octet qui code le nombre de bits inutilisés du dernier octet du contenu – de zéro à sept – sous la forme d'un nombre binaire sans signe dont le bit de poids fort et le bit de poids faible sont respectivement le bit 8 et le bit 1.

3.1.3 Canal ECS non chiffré

Le système de confidentialité nécessite l'utilisation d'un canal de commande non chiffré entre l'unité de chiffrement et l'unité de déchiffrement. Un canal de commande par système de chiffrement de liaison suffit. Ce canal de commande sert aussi au chiffrement des signaux audio et vidéo et, le cas échéant, des données.

Le contenu du canal SCC est structuré en blocs de 128 bits, inclus dans la multitrame de la Recommandation H.221 (voir la Figure 2); le premier bit du bloc est donc le bit 8 de l'octet 17 de la trame numéro 0 de la multitrame. Il existe deux types de blocs: les blocs d'échange de session (SE) (*session exchange*) et les blocs de vecteur d'initialisation (IV) (*initialisation vector*). Les informations contenues dans un bloc IV prennent effet dès le début de la multitrame suivante et restent en vigueur jusqu'à ce qu'un autre bloc IV soit envoyé. Le canal ECS doit toujours contenir un bloc IV ou un bloc SE; pendant une session, le bloc IV peut être répété sans modification aussi souvent que nécessaire.

	Bit numéro													
	0	1	2	3	4	5	6	7	8	9	10	11	12 à 119	120 à 127
Type SE	0	n	n	s	s	s	s	s	e	e	e	e	messages	réserve

	Bit numéro													
	0	1	2	3	4	5	6	7	8	9	10	11	12 à 107	108 à 127
Type IV	1	n	n	A	C	C	L	s	e	e	e	e	IV	réserve

FIGURE 2/H.233

Blocs du canal de commande

Le bloc contient les éléments suivants:

1) en-tête (12 bits), comprenant:
   - bit 0 pour sélectionner le type: 0 = SE (échange de session)

     1 = IV (vecteur d'initialisation)
   - bits 1 et 2 pour identifier les blocs d'une séquence de plusieurs blocs:

     00 pour un bloc isolé non suivi de blocs connexes

     01 pour le bloc n° 1 d'une séquence de plusieurs blocs

     10 pour un bloc intermédiaire d'une séquence

     11 pour le dernier bloc d'une séquence
   - bit 3 du bloc de type IV pour indiquer le chiffrement en service/hors service (A):

     1 = EN SERVICE, 0 = HORS SERVICE
   - bits 4 et 5 du bloc de type IV pour indiquer la longueur de IV (CC):

     00 = 64 bits + 32 bits (correction d'erreur)

     01, 10, 11 réservés
   - bit 6 du bloc de type IV: réservé pour la synchronisation de chargement de clé (L)
   - autres bits: réservé(s) mis à «0»
   - bits 8 à 11: correction d'erreur pour les bits 0 à 7.
2) blocs SE: structurés comme suit: 9 × (8 bits d'information + 4 bits de correction d'erreur)

   blocs IV: vecteur d'initialisation de système ou partie de vecteur d'initialisation de système (64 bits), avec protection contre les erreurs (32 bits).
3) blocs SE: 8 bits de réserve

   blocs IV: 20 bits de réserve – laissent au système un intervalle pour donner suite aux informations reçues; peut aussi permettre une amélioration future.

3.1.3.1 Blocs d'échange de session

Dans les blocs de type SE, les 116 bits qui suivent l'en-tête de 8 + 4 bits sont structurés comme suit: $9 \times (8 + 4) + 8$, les 8 derniers bits n'étant pas utilisés et les 9 mots comportant chacun 8 bits d'information + 4 bits de correction d'erreur. Dans le récepteur, les bits d'information (dont la provenance sera indiquée dans l'en-tête dans le cas où ils proviennent de plusieurs blocs) forment un train constitué des messages sur l'authentification et sur la gestion des clés, ainsi que des messages de possibilité d'algorithme (P8) et de commande d'algorithme (P9) définis ci-dessous.

Les 12 bits des mots inutilisés à la fin du bloc SE doivent être mis à zéro.

Possibilité d'algorithme (P8)

Nom du message: présentation de l'information de disponibilité des algorithmes de chiffrement (P8).

Identificateur du message: 11 P t_1 t_2 t_3 t_4 t_5 = 11000000

Contenu: [numéro 3-255][octets supplémentaires] où le premier octet indique le nombre des octets qui suivent. Chaque ensemble de trois octets indique la disponibilité d'un mécanisme de chiffrement utilisant les valeurs indiquées pour les identificateurs de support d'information, les identificateurs d'algorithme et les identificateurs de paramètre énoncés ci-dessous. Par exemple, un terminal capable de décoder DES et FEAL transmettra le message P8 {[11000000][00000110][00000000][00000010][00000000][00000000][00000001][00000000]}.

Commande d'algorithme (P9)

Nom du message: présentation de l'information d'algorithme en service (P9).

Identificateur du message: 11 P t_1 t_2 t_3 t_4 t_5 = 11000001

Signification: lorsqu'on place ensuite le bit de chiffrement EN SERVICE dans l'en-tête IV, l'algorithme utilisé est celui qui est spécifié ici dans ce message.

Contenu: octets du schéma de chiffrement (mêmes valeurs que dans le message de possibilité P8).

Identificateurs de support d'information

Un octet est utilisé pour déterminer ceux des éléments du système audiovisuel qui sont codés. Chaque bit de cet octet correspond au support d'information suivant:

Premier bit (LSB):	Audio 0 = chiffré, 1 = non chiffré
Deuxième bit:	Vidéo 0 = chiffré, 1 = non chiffré
Troisième bit:	LSD 0 = chiffré, 1 = non chiffré
Quatrième bit:	HSD 0 = chiffré, 1 = non chiffré
Cinquième bit:	réservé pour MLP, mis à «0»
Sixième bit:	réservé pour MLP-H, mis à «0»
Septième bit:	réservé pour utilisation future, mis à «0»
Huitième bit (MSB):	réservé pour utilisation future, mis à «0»

[00000000] indique que le signal multiplexé (sauf FAS, BAS et ECS) est chiffré. Les procédures applicables aux autres cas sont à l'étude:

Identificateurs d'algorithme

Un octet est utilisé pour l'identification de l'algorithme. La définition de l'algorithme indique en outre en détail comment procéder pour obtenir la suite chiffrante à partir de la clé et de la valeur IV en vigueur. Plusieurs algorithmes sont actuellement pris en compte; les codes à utiliser sont les suivants:

MSB LSB	
0 0 0 0 0 0 0 0	Non attribué. Réservé pour utilisation ultérieure
0 0 0 0 0 0 0 1	«FEAL» (voir l'Appendice II.1)
0 0 0 0 0 0 1 0	«DES» (voir l'Appendice II.2), Mode 1
0 0 0 0 0 0 1 1	Réservé pour «DES» (voir l'Appendice II.2), Mode 2
0 0 0 0 0 1 0 0	Réservé pour «DES» (voir l'Appendice II.2), Mode 3
0 0 0 0 0 1 0 1	Réservé pour ISO/IEC, Registre d'algorithme 9979, numéro d'enregistrement 000001 (B-CRYPT)
Autres valeurs	Non attribué. Réservé pour utilisation ultérieure.

Identificateurs de paramètre

Un octet est utilisé pour identifier les paramètres des algorithmes de chiffrement définis en 3.2. La valeur par défaut est [00000000]; elle peut être utilisée lorsque l'algorithme ne nécessite pas de valeurs de paramètre.

L'équipement doit assurer le déchiffrement par au moins un des algorithmes indiqués; si plusieurs possibilités sont indiquées, on peut laisser à l'opérateur du système le soin de choisir l'algorithme nécessaire au chiffrement de l'information transmise.

Autres messages

P1 Nom du message: chiffrement impossible

Signification: l'expéditeur de ce message n'utilisera pas de système de chiffrement

Identificateur du message: 10 P t_1 t_2 t_3 t_4 t_5 = 10000001

Contenu: ce message n'a pas de contenu.

P2 Nom du message: échec du lancement du système de chiffrement

Signification: l'expéditeur de ce message n'a pas réussi à mettre en marche son système de chiffrement. Cet échec peut être dû à une défaillance au stade de l'échange des clés; pour des raisons de sécurité, la cause de l'échec n'est pas indiquée dans le message.

Identificateur du message: 10 P t_1 t_2 t_3 t_4 t_5 = 100000010

Contenu: ce message n'a pas de contenu.

3.1.3.2 Vecteurs d'initialisation

La longueur par défaut d'un IV est de 64 bits. La longueur, correction d'erreur comprise, est de 96 bits. On peut transmettre des longueurs d'IV plus grandes en utilisant plusieurs blocs. Le bit de poids fort, c'est-à-dire le bit 12 du (premier) bloc de type IV, est transmis en premier.

3.1.3.3 Protection contre les erreurs des informations transmises dans le canal de commande

Les informations transmises dans le canal de commande doivent être protégées contre les erreurs. On utilise à cet effet un code de Hamming [12,8]. Les matrices de générateur et de contrôle de parité sont représentées à la Figure 3.

La même structure est utilisée pour les en-têtes, pour les messages d'échange de session et pour les vecteurs d'initialisation. Dans chaque cas, un octet est suivi de quatre bits de correction d'erreur.

Le IV est subdivisé en 8 octets, assortis chacun de 4 bits de parité, ce qui porte la longueur totale du IV, bits de parité compris, à 96 bits, dans le cas par défaut.

Matrice du générateur	Matrice de controle de parité
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

Matrices de correction d'erreur

3.2 Méthode de chiffrement de la transmission

Le présent paragraphe traite du chiffrement des signaux audio, des signaux vidéo, et, le cas échéant, des données associées. Le chiffrement n'aura lieu qu'en cas de verrouillage de multitrame conformément à la Recommandation H.221.

Le système de chiffrement remplit les mêmes fonctions quel que soit le débit utile. Chacun des flux de données d'usager ou leur ensemble peut être chiffré. Le système de chiffrement n'a pas besoin d'être informé de la manière dont se répartissent ces diverses formes d'informations d'usager, puisqu'il chiffre les données après le multiplexage et qu'il les déchiffre avant le démultiplexage.

L'ordre temporel de chiffrement suit l'ordre de transmission dans le train série bit par bit. Il convient de chiffrer les données avant de procéder à un calcul CRC4. Les calculs CRC4 sont ensuite effectués sur des données chiffrées, ce qui garantit la validité du code CRC4 des réseaux associés qui pourront être présents.

Une suite chiffrante est créée dans les deux terminaux à partir des valeurs en cours de la clé et du vecteur d'initialisation; dans le module de chiffrement, cette suite vient s'ajouter en addition modulo 2 aux bits à chiffrer et dans l'unité de déchiffrement, les bits chiffrés sont ajoutés en addition modulo 2 à la même suite chiffrante pour récupérer l'information d'usager en clair.

Les vecteurs d'initialisation (IV) sont créés de manière aléatoire dans le module de chiffrement et sont envoyés au module de déchiffrement par l'intermédiaire du ECS. Ils sont utilisés avec les données à chiffrer ou à déchiffrer. Ils fournissent une méthode de resynchronisation périodique des modules de chiffrement et de déchiffrement.

NOTE – Selon l'algorithme choisi, il convient de prêter attention à l'ordre des bits IV chargés dans les unités de chiffrement et de déchiffrement.

En cas de perte de synchronisation, les données seront altérées jusqu'à l'échange d'un nouveau IV. Le moment auquel le IV doit être transmis est fonction de la tolérance sur la perte de données jusqu'à resynchronisation.

Chaque bit dans le canal est traité par le système de chiffrement de l'une des trois manières suivantes (voir Appendice I):

a) suite chiffrante générée et appliquée: information d'usager (audio, vidéo, données);

b) suite chiffrante générée, mais non appliquée FAS et BAS dans les canaux initial et supplémentaires (voir la Recommandation H.221) et ECS; la suite chiffrante n'est ni stockée ni différée en vue d'une utilisation ultérieure, mais perdue; elle n'est pas utilisée pour chiffrer des informations ultérieures;

c) suite chiffrante non générée: si la sortie du terminal vers la ligne inclut des canaux qui ne font pas partie du débit utile spécifié dans la commande BAS pertinente (TS0 et/ou TS16 d'une liaison à débit primaire, ou autres canaux non transmis de bout en bout, par exemple), aucune suite chiffrante n'est générée pour ces bits.

Dans le cas de la transmission à 56 kbit/s décrite dans l'Annexe 2/H.221, la suite chiffrante est générée pour le huitième sous-canal, mais seuls les sept premiers bits sont utilisés pour l'addition modulo 2 au signal en sept parties.

Dans le cas de la transmission à débit binaire restreint de 128 kbit/s ou supérieur, la suite chiffrante est générée mais pas appliquée au huitième bit inséré par bourrage dans chaque intervalle de temps.

L'identificateur de paramètre est mis à [00000000].

Pour les paramètres opérationnels de chaque méthode de chiffrement, se reporter à l'Appendice II.

3.3 Procédure à suivre pour utiliser le système

Un terminal qui a reçu l'indication que le terminal correspondant dispose du chiffrement (voir Recommandation H.221) et qui souhaite commencer le chiffrement, ouvre le canal ECS et transmet le ou les messages P8. Au reçu du ou des messages P8 provenant du terminal correspondant, il vérifie s'il existe des algorithmes/modes compatibles; s'il n'en existe pas, il envoie le message P1; s'il y a compatibilité, il envoie un message P9 pour identifier l'algorithme/le mode qui sera utilisé, puis commence la transmission des blocs IV.

P2 peut être utilisé dans les procédures de reprise sur incident (nécessite un complément d'étude).

4 Chiffrement du protocole multicouche

Nécessite un complément d'étude.

Appendice I

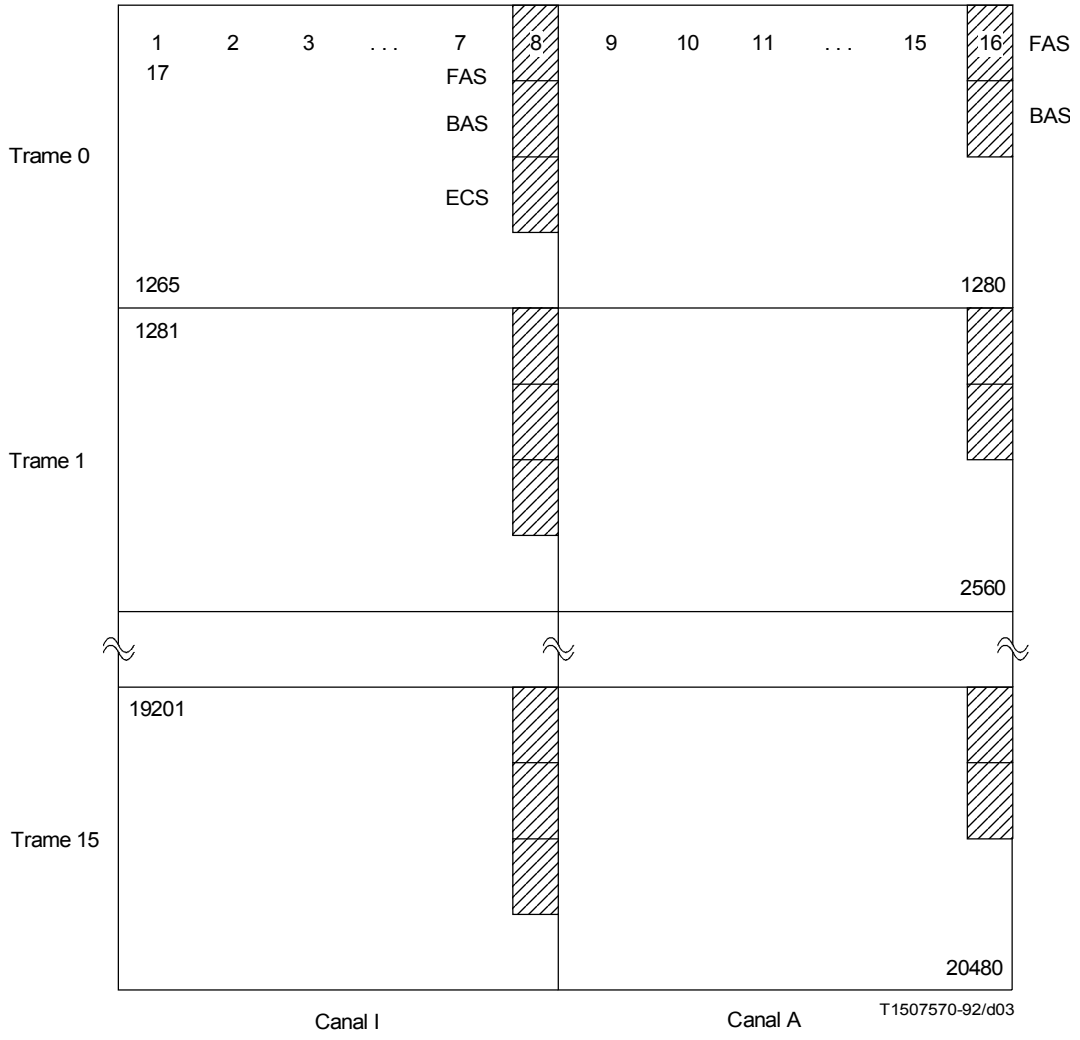
Chiffrement et déchiffrement de 2 × canaux B

(Cet appendice ne fait pas partie intégrante de la présente Recommandation)

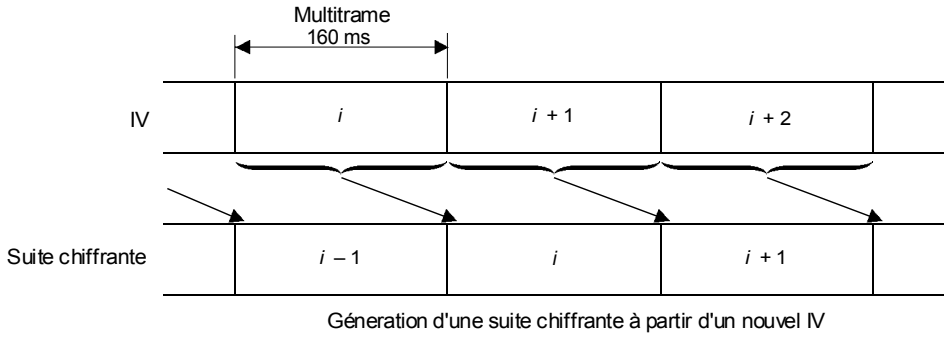
Le présent appendice donne un exemple du mode de fonctionnement du chiffrement/déchiffrement de la Recommandation H.233.

– La suite chiffrante est générée pour tous les bits.

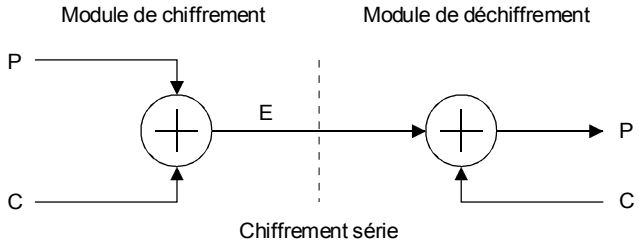
– La suite chiffrante est ajoutée à tous les bits sauf ceux de la partie hachurée.



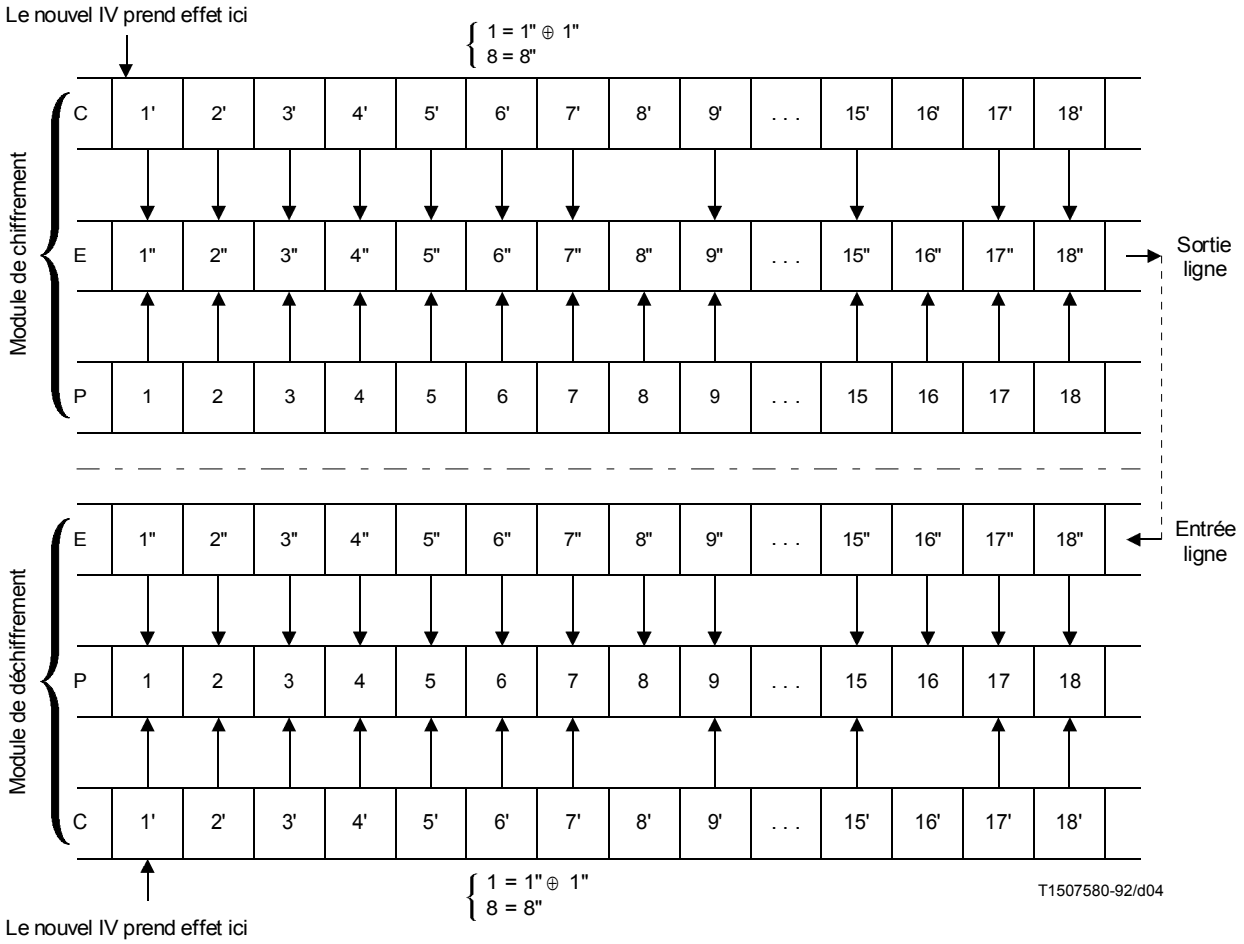
Numérotation des bits et bits non chiffrés d'une multitrame sur 2 canaux B



Géneration d'une suite chiffrante à partir d'un nouvel IV



Chiffrement série



P Texte clair
C Train chiffré
E Texte chiffré

Appendice II

Algorithme de chiffrement et paramètres associés

(Cet appendice ne fait pas partie intégrante de la présente Recommandation)

II.1 FEAL

Une suite chiffrante est créée dans les deux terminaux à partir des valeurs actuelles de la clé et du vecteur d'initialisation à l'aide de l'algorithme FEAL-8 (FEAL à 8 étages avec clé à 64 bits) dans le mode rebouclage de la sortie (OFB) (*output feedback*) défini dans la norme ISO 8372. Des précisions sur l'algorithme FEAL sont données en [1]. Dans l'unité de chiffrement, cette suite vient s'ajouter en mode modulo 2 aux bits à chiffrer et dans l'unité de déchiffrement les bits chiffrés sont ajoutés au modulo 2 à la même suite chiffrée pour récupérer l'information d'usager en clair. Voir la Figure II.1.

La variable initiale (SV) (*starting variable*) est identique au vecteur d'initialisation (IV). IV est chargé au début de chaque multitrame.

Sur les 64 bits sortants de l'algorithme de chiffrement, les huit premiers bits en partant du bit de poids fort sont utilisés pour addition bit par bit aux 8 bits du bloc du signal audiovisuel; le premier bit du bloc chiffrant est ajouté modulo 2 au premier bit du bloc du signal et le bit résultant est transmis au premier dans le canal; le deuxième bit du bloc chiffrant est ajouté modulo 2 au deuxième bit du bloc du signal et le bit résultant est transmis dans le canal, et ainsi de suite. Une fois les 8 bits transmis, le tour suivant de la suite chiffrante est généré et utilisé pour le chiffrement.

II.2 DES

L'algorithme DES est spécifié en [2].

Les méthodes permettant d'appliquer la suite chiffrante au train de données sont décrites en [3].

Le mode 1 DES utilisera la méthode appelée OFB-8; les modes 2 et 3 DES feront l'objet d'un complément d'étude.

La variable initiale (SV) (*starting variable*) est identique au vecteur d'initialisation (IV).

L'identificateur de paramètre est mis à [00000000], les autres valeurs devant faire l'objet d'un complément d'étude.

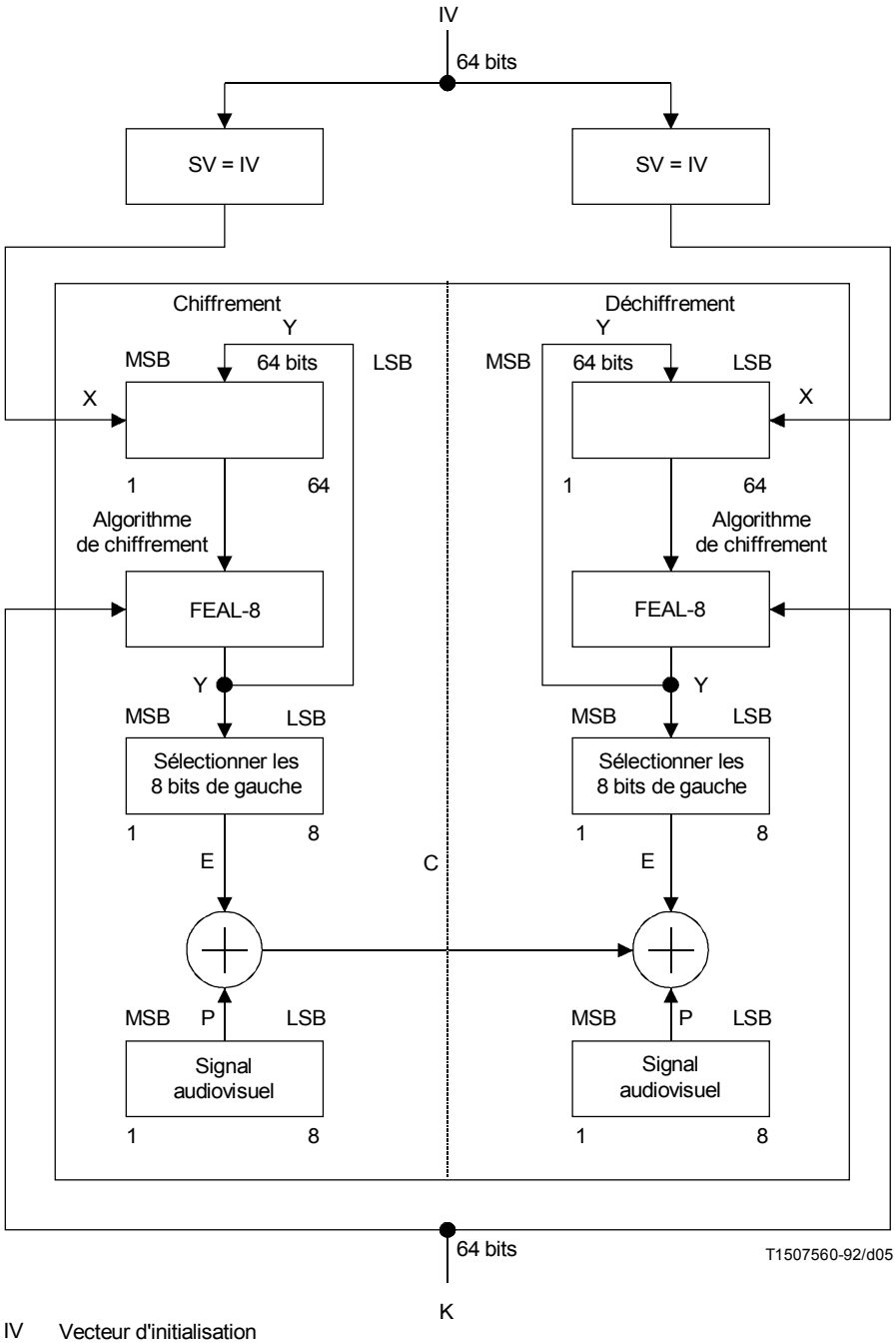


FIGURE II.1/H.233

Mode rebouclage de la sortie pour l'algorithme FEAL

Références

[1] MIYAGUCHI (S.), KURIHARA (S.), OHTA (K.), MORITA (H.): Expansion of FEAL Cipher, *NTT Review*, Vol. 2, n° 6, pages 117 à 127, novembre 1990.

[2] Data encryption standard, *Federal Information Publication Service (FIPS) Publication 46*, 15 janvier 1977.

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

Imprimé en Suisse

Genève, 1994