UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T J.96

(07/2002)

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

SÉRIE J: RÉSEAUX CÂBLÉS ET TRANSMISSION DES SIGNAUX RADIOPHONIQUES, TÉLÉVISUELS ET AUTRES SIGNAUX MULTIMÉDIAS

Services numériques auxiliaires propres aux transmissions télévisuelles

Méthode technique permettant de garantir la confidentialité des transmissions internationales longue distance de télévision MPEG-2 conformes à la Recommandation UIT-T J.89

Recommandation UIT-T J.96

RECOMMANDATIONS UIT-T DE LA SÉRIE J

RÉSEAUX CÂBLÉS ET TRANSMISSION DES SIGNAUX RADIOPHONIQUES, TÉLÉVISUELS ET AUTRES SIGNAUX MULTIMÉDIAS

Recommandations générales	J.1–J.9
Spécifications générales des transmissions radiophoniques analogiques	J.10–J.19
Caractéristiques de fonctionnement des circuits radiophoniques analogiques	J.20–J.29
Equipements et lignes utilisés pour les circuits radiophoniques analogiques	J.30–J.39
Codeurs numériques pour les signaux radiophoniques analogiques	J.40–J.49
Transmission numérique de signaux radiophoniques	J.50–J.59
Circuits de transmission télévisuelle analogique	J.60–J.69
Transmission télévisuelle analogique sur lignes métalliques et interconnexion avec les faisceaux hertziens	J.70–J.79
Transmission numérique des signaux de télévision	J.80–J.89
Services numériques auxiliaires propres aux transmissions télévisuelles	**J.90–J.99**
Prescriptions et méthodes opérationnelles de transmission télévisuelle	J.100–J.109
Services interactifs pour la distribution de télévision numérique	J.110–J.129
Transport des signaux MPEG-2 sur les réseaux par paquets	J.130–J.139
Mesure de la qualité de service	J.140–J.149
Distribution de la télévision numérique sur les réseaux locaux d'abonnés	J.150–J.159
IPCablecom	J.160–J.179
Divers	J.180–J.199
Application à la télévision numérique interactive	J.200–J.209

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T J.96

Méthode technique permettant de garantir la confidentialité des transmissions internationales longue distance de télévision MPEG-2 conformes à la Recommandation UIT-T J.89

Résumé

La présente Recommandation UIT-T décrit un système d'embrouillage de base compatible (BISS-E, *basic interoperable scrambling system*) destiné à être utilisé sur des circuits de contribution numériques (satellite, reportage d'actualités par satellite numérique, etc.) conformes à la Rec. UIT-T J.89, c'est-à-dire utilisant des clés fixes. Le système BISS-E, qui utilise des mots de session cryptés, permet un accès conditionnel à gestion centralisée.

Source

La Recommandation J.96 de l'UIT-T, révisée par la Commission d'études 9 (2001-2004) de l'UIT-T, a été approuvée le 29 juillet 2002 selon la procédure définie dans la Résolution 1 de l'AMNT.

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'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.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un Membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

TABLE DES MATIÈRES

Recommandation UIT-T J.96

Méthode technique permettant de garantir la confidentialité des transmissions internationales longue distance de télévision MPEG-2 conformes à la Recommandation UIT-T J.89

1 Domaine d'application

La présente Recommandation constitue une norme commune relative à un système à accès conditionnel pour la transmission internationale longue distance de télévision numérique conformément au profil professionnel MPEG (4:2:2).

L'essor rapide de la technologie DSNG (reportage d'actualités par satellite numérique, *digital satellite news gathering*) a conduit un certain nombre de constructeurs à mettre sur le marché des codecs numériques. Parallèlement, l'absence de méthodes normalisées de sécurisation et d'embrouillage des données diffusées a favorisé l'éclosion de mécanismes de sécurité propres à chacun de ces constructeurs.

L'adoption généralisée des normes de radiodiffusion vidéonumérique (DVB) permet aujourd'hui d'envisager de mettre au point un mécanisme de sécurité qui rende compatibles les équipements de différents constructeurs. Tout en permettant aux radiodiffuseurs d'interconnecter des équipements de plusieurs constructeurs, un tel mécanisme constituerait aussi pour les systèmes un gage de plus grande durabilité.

Fondé sur la spécification DVB-CSA (*radiodiffusion vidéonumérique-algorithme commun d'embrouillage*) [1] le système d'embrouillage de base compatible (BISS, *basic interoperable scrambling system*) utilise des clés fixes en langage clair appelées mots de session (SW, *session word*). Le mode 1 de la spécification BISS est utilisé pour le reportage DSNG.

Le mode E de la spécification BISS (BISS avec clés cryptées – appelé BISS-E) utilise un mécanisme supplémentaire permettant l'insertion de mots de session cryptés (ESWs, *encrypted session words*), tout en conservant, parallèlement, l'interopérabilité (compatibilité des équipements). Ce mécanisme est rétrocompatible avec le mode 1 de la spécification BISS.

2 Références informatives

– UER, document technique 3292 rév.2 (2002), *BISS-E – Basic Interoperable Scrambling System with Encrypted keys* (*Système d'embrouillage de base compatible avec clés cryptées*).

3 Définitions

La présente Recommandation définit les termes suivants:

3.1 embrouilleur: ensemble des mécanismes nécessaires pour satisfaire à la spécification DVB-CSA.

3.2 mot de session: mot attribué pendant une transmission par le centre de gestion.

3.3 unité: dispositif auquel la présente Recommandation est susceptible de s'appliquer.

3.4 centre de gestion: organisation assurant la commande ou la gestion du système à accès conditionnel.

3.5 fonction de décryptage: fonction logique utilisée pour décrypter les mots de session cryptés au moyen d'une clé.

3.6 fonction interopérable: fonction de décryptage qui sera intégrée dans toutes les unités.

Les bits des nombres et des séquences binaires sont numérotés de gauche à droite, conformément à la notation technique. Le bit 0, placé à droite, est le bit de plus faible poids; le bit de gauche est celui de plus fort poids.

Voici un exemple de notation technique pour un nombre de n bits:

$$b_{n-1}b_{n-2} \ldots b_1b_0$$

4 Abréviations

La présente Recommandation utilise les abréviations suivantes:

BISS système d'embrouillage de base compatible (*basic interoperable scrambling system*)

bslbf chaîne binaire, bit de gauche en premier (*bit string, left bit first*)

CA accès conditionnel (*conditional access*)

CAT table d'accès conditionnels (*conditional access table*)

CSA (DVB) algorithme commun d'embrouillage (*common scrambling algorithm*)

CW mot de contrôle (*control word*)

DES algorithme normalisé de cryptage de données (*data encryption standard*)

DSNG reportage d'actualités par satellite numérique (*digital satellite news gathering*)

DVB radiodiffusion vidéonumérique (*digital video broadcasting*)

ECB répertoire de codes électroniques (*electronic codebook*)

ECM message de contrôle des titres d'accès (*entitlement control message*)

EMM message de gestion des titres d'accès (*entitlement management message*)

ESW mot de session crypté (*encrypted session word*)

lsb bit de plus faible poids (*least significant bit*)

LSB octet de plus faible poids (*least significant byte*)

MC centre de gestion (*management centre*)

msb bit de plus fort poids (*most significant bit*)

MSB octet de plus fort poids (*most significant byte*)

PID numéro d'identification de paquet (*packet identification number*)

PMT table de mappage de programmes (*programme map table*)

SW mot de session (*session word*)

uimsbf entier non signé, bit de plus fort poids en premier (*unsigned integer, most significant bit first*)

5 Prescriptions de sécurité

Le modèle de reportage DSNG nécessite la saisie directe d'un mot de session au niveau de l'émetteur et au niveau du récepteur pour contrôler l'accès à la transmission. L'émetteur et le ou les récepteurs de la transmission partagent le mot de session, ainsi seules les parties voulues recevront la transmission, selon le processus ci-dessous:

1) le mot de session est saisi au niveau de l'unité DSNG dans le champ, ou au niveau de la station terrienne d'émission;

2) le mot de session est saisi au niveau des IRD de réception;

3) si les mots de session sont identiques, les IRD sont capables de décrypter les données diffusées;

4) si les mots de session sont différents, les données diffusées ne sont pas reçues.

Les prescriptions de sécurité pour les systèmes de contribution fixes sont quelque peu différentes de celles du modèle DSNG. La sécurité de l'échange des mots de session est fondamentale pour ces systèmes et elle peut être assurée moyennant le cryptage des mots de session.

6 Modes de fonctionnement

L'embrouilleur doit être capable de prendre en charge les trois modes de fonctionnement suivants:

– **Mode 0**: pas d'embrouillage.

– **Mode 1**: toutes les composantes sont embrouillées avec un mot de contrôle (CW, *control word*), dérivé d'un mot de session (SW) en langage clair.

– **Mode E**: toutes les composantes sont embrouillées avec un mot de contrôle fixe, dérivé d'un mot de session crypté (ESW, *encrypted session word*).

Le mécanisme d'embrouillage, tel que défini dans la spécification DVB-CSA, ne sera appliqué qu'au niveau transport.

Une table d'accès conditionnels (CAT, *conditional access table*) doit être présente dans le multiplex pour les modes 1 et E du système BISS-E, même si elle doit être vide, car aucun flux de message de gestion des titres d'accès (EMM, *entitlement management message*) ne sera présent.

NOTE – Un embrouilleur qui ne prend en charge qu'un sous-ensemble des modes de fonctionnement définis doit procéder conformément à une hiérarchie imposée. Un embrouilleur prenant en charge le mode E doit aussi prendre en charge les modes 0 et 1.

7 Mode 0

L'embrouilleur doit être capable de désactiver l'opération d'embrouillage. Dans ce mode, il n'y aura pas de descripteur *CA_descriptor* dans la table de mappage de programmes (PMT, *programme map table*) et il n'y aura pas de flux message de contrôle des titres d'accès (ECM, *entitlement control message*). Les bits *Transport_Scrambling_Control* des paquets de transport seront mis à "00".

8 Système BISS, mode 1 – Prescriptions fonctionnelles

8.1 Aperçu général

Ce mode a été conçu expressément pour les applications de reportage DSNG, les opérations délicates, les situations d'urgence, etc. Il peut aussi constituer une solution de repli en cas d'utilisation du système BISS-E dans son intégralité. Dans le mode 1, un mot de session fixe de 12 caractères est inséré dans l'embrouilleur. Le mot de contrôle de 64 bits est dérivé du mot de session, conformément à la spécification DVB-CSA.

La saisie manuelle du mot de session doit se faire en notation hexadécimale, les chiffres de plus fort poids étant saisis en premier, c'est-à-dire de gauche à droite du point de vue de la notation hexadécimale.

Par exemple, `0xA13DBC42908F` serait saisi dans la séquence suivante:

`A,1,3,D,B,C,4,2,9,0,8,F`

La saisie à distance du mot de session doit aussi être possible, même si la spécification de cette interface n'entre pas dans le cadre de la présente Recommandation.

L'embrouilleur doit faire en sorte que le mot de session utilisé ne puisse pas être modifié plus de dix fois par période de 5 minutes et qu'il y ait au moins 10 secondes entre deux modifications consécutives.

Dans ce mode, il y aura un descripteur *CA_descriptor* dans la table PMT, présent au niveau programme, mais il n'y aura pas de flux ECM. Un seul identificateur *CA_System_ID* unique est assigné pour identifier le système BISS.

Les bits *Transport_Scrambling_Control* des paquets de transport sont mis à "10".

8.2 Descripteur CA_descriptor

Le descripteur *CA_descriptor* qui doit être présent dans la table PMT pour prendre en charge le système BISS est défini dans le Tableau 1.

Tableau 1/J.96 – Descripteur d'accès conditionnel – Mode 1

Syntaxe	Nombre de bits	Identificateur
CA_descriptor() {		
descriptor_tag	8	uimsbf
descriptor_length	8	uimsbf
CA_system_ID	16	uimsbf
reserved	3	bslbf
CA_PID	13	uimsbf
}		

Sémantique

CA_system_ID: champ de 16 bits indiquant le type de système à accès conditionnel applicable pour les flux ECM associés. Pour le système BISS, ce champ vaut `0x2600`. Voir [2].

CA_PID: champ de 13 bits indiquant l'identificateur PID des paquets de flux de transport devant contenir l'information ECM. Pour le système BISS, aucune information ECM n'est nécessaire, ce champ doit donc contenir la valeur `0x1FFF`.

9 Système BISS, mode E – Prescriptions fonctionnelles

9.1 Mot de session en langage clair

L'unité utilisée doit être compatible avec le mode 1 du système BISS. On doit pouvoir y insérer un mot de session en langage clair de 12 caractères depuis son panneau avant ou via une interface de télécommande. Elle doit utiliser le mot de session spécifié au § 8 (système BISS, mode 1).

Une fois saisi via l'interface utilisateur ou le port de télécommande, le mot de session en langage clair ne doit pas pouvoir être lu au moyen d'une quelconque interface avec une autre unité.

9.2 Mot de session crypté

On doit pouvoir insérer dans l'unité des mots de session cryptés (ESW) depuis son panneau avant ou via une interface de télécommande. La définition du port de télécommande n'entre pas dans le cadre de la présente Recommandation.

On entend par mot ESW un numéro de 16 caractères qui est transformé par l'unité en un mot de session en langage clair de 12 caractères. Le mot de session en langage clair est ensuite utilisé par l'unité pour décrypter les données diffusées conformément au § 8 (système BISS, mode 1).

Une fois qu'il a été saisi depuis le panneau avant de l'unité ou via l'interface de télécommande, le mot ESW ne doit pas pouvoir être lu au moyen d'une quelconque interface avec une autre unité.

La saisie manuelle du mot ESW doit se faire sous forme hexadécimale, le quartet de plus fort poids parmi les 16 chiffres étant saisi en premier (c'est-à-dire le quartet de gauche).

Par exemple, à supposer qu'il soit égal à `0xF76EE249BE01A286`, le mot ESW doit être saisi dans la séquence suivante:

`F,7,6,E,E,2,4,9,B,E,0,1,A,2,8` et `6`

9.3 Système de décryptage

9.3.1 Aperçu général

L'équipement doit inclure les éléments suivants:

– un **identificateur**, désigné par l'abréviation ***ID***, constitué d'un mot hexadécimal de 14 caractères, qui doit être *injecté* par l'utilisateur et utilisé par défaut. L'identificateur ID injecté est obligatoire. A titre facultatif, le fournisseur peut aussi prévoir un identificateur ID *implicite*. Dans ce cas, il appartient à l'utilisateur de sélectionner cet identificateur implicite;

– une **fonction de décryptage DES**, désignée par ***f( )***, telle que décrite au § 9.3.3. D'autres fonctions peuvent être offertes, qui toutefois n'entrent pas dans le cadre de la présente Recommandation;

– une **fonction de post-traitement simple**, désignée par ***P( )***, telle que décrite au § 9.3.4.

Le traitement appliqué au mot ESW dans l'unité pour obtenir le mot de session en langage clair est représenté sur la Figure 1. La spécification détaillée de l'algorithme normalisé de cryptage de données (DES) n'entre pas dans le cadre de la présente Recommandation.

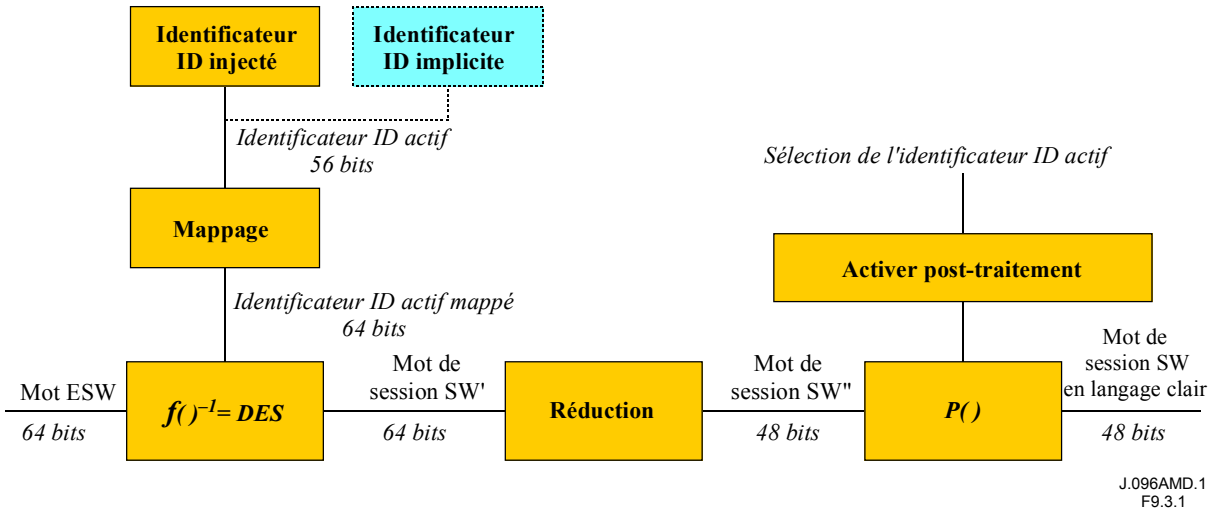

Figure 1/J.96 – Le traitement du signal nécessaire à la production d'un mot de session en langage clair

Le mappage de l'identificateur ID consiste simplement à passer de 56 à 64 bits, moyennant l'adjonction d'un bit d'imparité tous les 7 bits. La suppression des premier et dernier bits de chaque octet permet de ramener le mot de session décrypté de 64 à 48 bits.

L'application de la fonction de post-traitement ***P( )***, permet d'obtenir le mot de session en langage clair à injecter dans l'équipement BISS comme dans le mode 1.

9.3.2 Identificateurs d'unité

La présente Recommandation spécifie deux types d'identificateurs pour chaque unité.

1) Un **identificateur injecté** (ID_i), à savoir une clé secrète intégrée dans l'unité. Cet identificateur est ***obligatoire***.

2) En outre, le constructeur peut prévoir un **identificateur implicite** (ID_b), défini par ses soins et associé en propre à chaque unité. Bien que n'étant pas obligatoire, cet identificateur, s'il est implémenté, devra être conforme aux prescriptions de la présente Recommandation.

Un utilisateur doit pouvoir sélectionner l'identificateur de son choix depuis le panneau avant de l'unité et via l'interface de télécommande. L'identificateur sélectionné fait office de clé active pour décrypter le mot de session crypté (ESW).

a) Identificateur ID injecté – obligatoire

Constitué de 14 caractères, l'identificateur ID injecté peut être saisi dans l'unité BISS par l'utilisateur à tout moment.

L'identificateur ID injecté doit pouvoir être inséré dans l'unité depuis le panneau avant de celle-ci ou via son interface de télécommande. Aucun mécanisme ne doit permettre de relire en partie ou en totalité l'identificateur ID injecté via une quelconque interface avec une autre unité.

Le même identificateur ID peut être injecté dans plusieurs équipements à des fins de gestion par redondance, par exemple.

La saisie manuelle ou à distance de l'identificateur ID injecté doit se faire sous forme hexadécimale; parmi les 14 chiffres, le quartet de plus fort poids (c'est-à-dire le quartet de gauche) est saisi en premier.

Par exemple, à supposer qu'il soit égal à `0xF09A423F56738A`, l'identificateur ID injecté doit être saisi dans la séquence suivante:

`F,0,9,A,4,2,3,F,5,6,7,3,8` et `A`

b) Identificateur ID implicite – facultatif pour le fournisseur

Constitué de 14 caractères, l'identificateur ID implicite est associé en propre à une unité donnée. Les identificateurs ID implicites sont facultatifs.

Deux unités différentes doivent avoir un identificateur ID implicite différent, du moins s'il s'agit d'équipements produits par le même constructeur. Des unités produites par des constructeurs différents pourraient, de manière purement fortuite, avoir le même identificateur ID implicite.

Le constructeur doit faire en sorte que personne ne puisse modifier l'identificateur ID implicite sans son consentement.

9.3.3 Fonction de décryptage

Les unités doivent être dotées de la fonction d'interopérabilité spécifiée au point b) ci-dessous. D'autres fonctions de décryptage peuvent être implémentées, à titre facultatif. En pareil cas, on doit pouvoir sélectionner la fonction de décryptage depuis le panneau avant de l'unité et via l'interface de télécommande. La définition de ces fonctions supplémentaires n'entre pas dans le cadre de la présente Recommandation.

La fonction d'interopérabilité est obligatoire sur toutes les unités. Elle utilise le mot de session crypté (ESW) de 64 bits et l'identificateur ID actif mappé de 64 bits pour calculer un mot de session de 12 caractères appelé SW".

a) *Mappage*

L'identificateur ID actif mappé est obtenu à partir de l'identificateur ID actif de 56 bits par mappage des 56 bits de l'identificateur ID actif sur les 7 bits de plus fort poids d'une séquence de 8 octets, le bit de plus faible poids (lsb) de chaque octet étant ensuite mis à une valeur telle que l'octet ainsi obtenu soit de parité impaire (voir Tableau 2).

Tableau 2/J.96 – Mappage identificateur ID actif – identificateur ID actif mappé

Bit de clé actif	Octet/bit mappé	Bit de clé mappé
55	0/7	63
54	0/6	62
53	0/5	61
52	0/4	60
51	0/3	59
50	0/2	58
49	0/1	57
Odd_parity	0/0	56
48	1/7	55
Etc.	Etc.	Etc.
NOTE – La notation technique utilisée ci-dessus est la suivante: msb = bit 63, lsb = bit 0.		

b) *fonction d'interopérabilité*

On entend par fonction d'interopérabilité l'algorithme normalisé de cryptage de données (DES) simple utilisé dans le mode du répertoire de codes électroniques (ECB) et dans l'état de décryptage. Cette fonction est décrite dans FIPS PUB 46-3 [3] et FIPS PUB 81 [4]. La clé de l'algorithme est l'identificateur ID actif mappé de 64 bits[1]. Le bloc de données de décryptage est le mot de session crypté (ESW). A noter que la notation technique (msb = bit 63, lsb = bit 0) est utilisée dans la présente Recommandation, alors que l'algorithme DES utilise la notation *FIPS* (msb = bit 1, lsb = bit 64). Le mappage des bits est donc le suivant:

– clé DES (1 ... 64) → Identificateur ID actif mappé (63 ... 0);

– bloc de données DES (1 ... 64) → Mot ESW (63 ... 0).

Le résultat de l'algorithme de décryptage, défini en 64 bits, est appelé mot de session SW'.

Le mappage entre les mots de session SW' et SW" est indiqué dans le Tableau 3. Ce mappage a simplement pour effet de supprimer le bit de plus fort poids et le bit de plus faible poids de chaque octet. La troisième colonne du tableau indique le résultat de l'algorithme DES, les bits étant numérotés selon la notation FIPS.

[1] L'algorithme DES n'utilise pas les bits 8, 16, 24, 32, 40, 48, 56 et 64 de la clé, numérotés selon la notation FIPS. De ce fait, la longueur utile de la clé est en réalité de 56 bits, ce qui est compatible avec les restrictions d'exportation.

Tableau 3/J.96 – Mappage entre les mots de session SW' et SW"

SW"(47)	SW'(62)	D(2)
SW"(46)	SW'(61)	D(3)
SW"(45)	SW'(60)	D(4)
SW"(44)	SW'(59)	D(5)
SW"(43)	SW'(58)	D(6)
SW"(42)	SW'(57)	D(7)
SW"(41)	SW'(54)	D(10)
SW"(40)	SW'(53)	D(11)
SW"(39)	SW'(52)	D(12)
SW"(38)	SW'(51)	D(13)
SW"(37)	SW'(50)	D(14)
SW"(36)	SW'(49)	D(15)
SW"(35)	SW'(46)	D(18)
SW"(34)	SW'(45)	D(19)
SW"(33)	SW'(44)	D(20)
SW"(32)	SW'(43)	D(21)
SW"(31)	SW'(42)	D(22)
SW"(30)	SW'(41)	D(23)
SW"(29)	SW'(38)	D(26)
SW"(28)	SW'(37)	D(27)
SW"(27)	SW'(36)	D(28)
SW"(26)	SW'(35)	D(29)
SW"(25)	SW'(34)	D(30)
SW"(24)	SW'(33)	D(31)
SW"(23)	SW'(30)	D(34)
SW"(22)	SW'(29)	D(35)
SW"(21)	SW'(28)	D(36)
SW"(20)	SW'(27)	D(37)
SW"(19)	SW'(26)	D(38)
SW"(18)	SW'(25)	D(39)
SW"(17)	SW'(22)	D(42)
SW"(16)	SW'(21)	D(43)
SW"(15)	SW'(20)	D(44)
SW"(14)	SW'(19)	D(45)
SW"(13)	SW'(18)	D(46)
SW"(12)	SW'(17)	D(47)
SW"(11)	SW'(14)	D(50)
SW"(10)	SW'(13)	D(51)
SW"(9)	SW'(12)	D(52)

Tableau 3/J.96 – Mappage entre les mots de session SW' et SW"

SW"(8)	SW'(11)	D(53)
SW"(7)	SW'(10)	D(54)
SW"(6)	SW'(9)	D(55)
SW"(5)	SW'(6)	D(58)
SW"(4)	SW'(5)	D(59)
SW"(3)	SW'(4)	D(60)
SW"(2)	SW'(3)	D(61)
SW"(1)	SW'(2)	D(62)
SW"(0)	SW'(1)	D(63)

9.3.4 Fonction de post-traitement

La fonction de post-traitement ***P( )*** convertit le mot de session SW" en mot de session (SW) en langage clair, comme le montre l'exemple ci-dessous. Les résultats de la conversion diffèrent en fonction du type d'identificateur ID utilisé pour décrypter le mot de session crypté ESW. Lorsque la clé active est l'**identificateur ID injecté**, la fonction ***P( )*** est la **fonction d'identifié** (c'est-à-dire SW" = SW). Si l'**identificateur ID implicite** facultatif est utilisé, la fonction ***P( )*** consiste à **faire tourner** le mot de session SW" d'**un bit vers la droite**.

Si SW" = b47 b46 ... b1 b0

SW = ***P(***SW"***)*** =

b47 b46 ... b1 b0	Si la clé active est un **identificateur ID injecté**
b0 b47 b46 ... b2b1	Si la clé active est un **identificateur ID implicite**
Non défini	**Autres** cas

Dans les **autres** cas, la définition de la fonction ***P( )*** n'entre pas dans le cadre de la présente Recommandation. Cette fonction doit toutefois avoir un comportement mathématique différent (c'est-à-dire qu'elle doit produire des résultats différents) que lorsque la clé active est l'identificateur ID *injecté* ou l'identificateur ID *implicite*.

Bibliographie

[1] *DVB Common Scrambling Algorithm*, V. 2.0. (juillet 2002). http://portal.etsi.org/dvbandca/DVB/DVBINTRO.asp

[2] ETSI ETR 289 (1996), Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems. http://webapp.etsi.org/workprogram/SimpleSearch/QueryForm.asp

[3] FIPS PUB 46-3 (1999), *Data Encryption Standard*. http://www.itl.nist.gov/fipspubs/by-num.htm

[4] FIPS PUB 81 (1980), *DES Modes of Operation*. http://www.itl.nist.gov/fipspubs/by-num.htm

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série B	Moyens d'expression: définitions, symboles, classification
Série C	Statistiques générales des télécommunications
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	**Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias**
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	RGT et maintenance des réseaux: systèmes de transmission, circuits téléphoniques, télégraphie, télécopie et circuits loués internationaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données et communication entre systèmes ouverts
Série Y	Infrastructure mondiale de l'information et protocole Internet
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2002