

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

(affiliée à l'Organisation Internationale de Normalisation — ISO)

NORME DE LA CEI

INTERNATIONAL ELECTROTECHNICAL COMMISSION

(affiliated to the International Organization for Standardization — ISO)

IEC STANDARD

Publication 489-7

Première édition — First edition

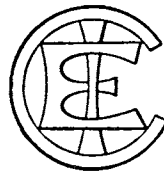
1976

**Méthodes de mesure applicables au matériel de radiocommunication
utilisé dans les services mobiles**

**Septième partie: Systèmes de secret
Définitions supplémentaires**

Methods of measurement for radio equipment used in the mobile services

**Part 7: Privacy equipment
Supplementary definitions**



Droits de reproduction réservés — Copyright - all rights reserved

Bureau Central de la Commission Electrotechnique Internationale

1, rue de Varembe
Genève, Suisse

Révision de la présente publication

Le contenu technique des publications de la CEI est constamment revu par la Commission afin d'assurer qu'il reflète bien l'état actuel de la technique.

Les renseignements relatifs à ce travail de révision, à l'établissement des éditions révisées et aux mises à jour peuvent être obtenus auprès des Comités nationaux de la CEI et en consultant les documents ci-dessous:

- **Bulletin de la CEI**
- **Rapport d'activité de la CEI**
Publié annuellement
- **Catalogue des publications de la CEI**
Publié annuellement

Terminologie utilisée dans la présente publication

Seuls sont définis ici les termes spéciaux se rapportant à la présente publication.

En ce qui concerne la terminologie générale, le lecteur se reportera à la Publication 50 de la CEI: Vocabulaire Electrotechnique International (V.E.I.), qui est établie sous forme de chapitres séparés traitant chacun d'un sujet défini, l'Index général étant publié séparément. Des détails complets sur le V.E.I. peuvent être obtenus sur demande.

Symboles graphiques et littéraux

Seuls les symboles graphiques et littéraux spéciaux sont inclus dans la présente publication.

Le recueil complet des symboles graphiques approuvés par la CEI fait l'objet de la Publication 117 de la CEI.

Les symboles littéraux et autres signes approuvés par la CEI font l'objet de la Publication 27 de la CEI.

Autres publications de la CEI établies par le même Comité d'Etudes

L'attention du lecteur est attirée sur la page 3 de la couverture, qui énumère les autres publications de la CEI préparées par le Comité d'Etudes qui a établi la présente publication.

Revision of this publication

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology.

Information on the work of revision, the issue of revised editions and amendment sheets may be obtained from IEC National Committees and from the following IEC sources:

- **IEC Bulletin**
- **Report on IEC Activities**
Published yearly
- **Catalogue of IEC Publications**
Published yearly

Terminology used in this publication

Only special terms required for the purpose of this publication are defined herein.

For general terminology, readers are referred to IEC Publication 50: International Electrotechnical Vocabulary (I.E.V.), which is issued in the form of separate chapters each dealing with a specific field, the General Index being published as a separate booklet. Full details of the I.E.V. will be supplied on request.

Graphical and letter symbols

Only special graphical and letter symbols are included in this publication.

The complete series of graphical symbols approved by the IEC is given in IEC Publication 117.

Letter symbols and other signs approved by the IEC are contained in IEC Publication 27.

Other IEC publications prepared by the same Technical Committee

The attention of readers is drawn to the inside of the back cover, which lists other IEC publications issued by the Technical Committee which has prepared the present publication.

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

(affiliée à l'Organisation Internationale de Normalisation — ISO)

NORME DE LA CEI

INTERNATIONAL ELECTROTECHNICAL COMMISSION

(affiliated to the International Organization for Standardization — ISO)

IEC STANDARD

Publication 489-7

Première édition — First edition

1976

**Méthodes de mesure applicables au matériel de radiocommunication
utilisé dans les services mobiles**

**Septième partie: Systèmes de secret
Définitions supplémentaires**

Methods of measurement for radio equipment used in the mobile services

**Part 7: Privacy equipment
Supplementary definitions**



Droits de reproduction réservés — Copyright - all rights reserved

Aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'éditeur.

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

Bureau Central de la Commission Electrotechnique Internationale

1, rue de Varembe
Genève, Suisse

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

MÉTHODES DE MESURE APPLICABLES AU MATÉRIEL DE RADIOCOMMUNICATION
UTILISÉ DANS LES SERVICES MOBILES

SEPTIÈME PARTIE: SYSTÈMES DE SECRET
DÉFINITIONS SUPPLÉMENTAIRES

PRÉAMBULE

- 1) Les décisions ou accords officiels de la CEI en ce qui concerne les questions techniques, préparés par des Comités d'Etudes où sont représentés tous les Comités nationaux s'intéressant à ces questions, expriment dans la plus grande mesure possible un accord international sur les sujets examinés.
- 2) Ces décisions constituent des recommandations internationales et sont agréées comme telles par les Comités nationaux.
- 3) Dans le but d'encourager l'unification internationale, la CEI exprime le vœu que tous les Comités nationaux adoptent dans leurs règles nationales le texte de la recommandation de la CEI, dans la mesure où les conditions nationales le permettent. Toute divergence entre la recommandation de la CEI et la règle nationale correspondante doit, dans la mesure du possible, être indiquée en termes clairs dans cette dernière.

PRÉFACE

La présente publication a été établie par le Sous-Comité 12F: Matériels utilisés dans les services mobiles, du Comité d'Etudes N° 12 de la CEI: Radiocommunications.

Le premier projet fut discuté lors de la réunion tenue à Munich en juin 1973. A la suite de cette réunion, le projet, document 12F(Bureau Central)7, fut soumis à l'approbation des Comités nationaux suivant la Règle des Six Mois en janvier 1974.

Les pays suivants se sont prononcés explicitement en faveur de la publication:

Allemagne	France
Argentine	Hongrie
Australie	Israël
Autriche	Japon
Belgique	Pays-Bas
Canada	Roumanie
Danemark	Royaume-Uni
Espagne	Suède
Etats-Unis d'Amérique	Turquie

Autre publication de la CEI citée dans la présente publication:

Publication n° 489-1: Méthodes de mesure applicables au matériel de radiocommunication utilisé dans les services mobiles, Première partie: Définitions générales et conditions normales de mesure.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**METHODS OF MEASUREMENT FOR RADIO EQUIPMENT
USED IN THE MOBILE SERVICES**

**PART 7: PRIVACY EQUIPMENT
SUPPLEMENTARY DEFINITIONS**

FOREWORD

- 1) The formal decisions or agreements of the IEC on technical matters, prepared by Technical Committees on which all the National Committees having a special interest therein are represented, express, as nearly as possible, an international consensus of opinion on the subjects dealt with.
- 2) They have the form of recommendations for international use and they are accepted by the National Committees in that sense.
- 3) In order to promote international unification, the IEC expresses the wish that all National Committees should adopt the text of the IEC recommendation for their national rules in so far as national conditions will permit. Any divergence between the IEC recommendation and the corresponding national rules should, as far as possible, be clearly indicated in the latter.

PREFACE

This publication has been prepared by Sub-Committee 12F, Equipment Used in the Mobile Services, of IEC Technical Committee No. 12, Radiocommunications.

The first draft was discussed at the meeting held in Munich in June 1973. As a result of this meeting, the draft, Document 12F(Central Office)7, was submitted to the National Committees for approval under the Six Months' Rule in January 1974.

The following countries voted explicitly in favour of publication:

Argentina	Israel
Australia	Japan
Austria	Netherlands
Belgium	Romania
Canada	Spain
Denmark	Sweden
France	Turkey
Germany	United Kingdom
Hungary	United States of America

Other IEC publication quoted in this publication:

Publication No. 489-1: Methods of Measurement for Radio Equipment Used in the Mobile Services, Part 1: General Definitions and Standard Conditions of Measurement.

MÉTHODES DE MESURE APPLICABLES AU MATÉRIEL DE RADIOCOMMUNICATION
UTILISÉ DANS LES SERVICES MOBILES

SEPTIÈME PARTIE: SYSTÈMES DE SECRET
DÉFINITIONS SUPPLÉMENTAIRES

1. **Domaine d'application**

Cette norme internationale s'applique aux dispositifs et systèmes électroniques conçus pour permettre le secret des communications en utilisant les procédés de codage de l'information avant la transmission, et de restitution ultérieure du message sous sa forme originale par un récepteur spécialisé. Les systèmes de ce genre sont conçus de façon que les transmissions interceptées par des récepteurs non spécialisés se révèlent intelligibles. Cette norme s'applique aux systèmes traitant l'information sous forme analogique, numérique ou hybride.

2. **Objet**

La présente norme donne les définitions normales applicables aux systèmes de secret, et non déjà incluses dans les définitions générales données dans la Publication 489-1: Méthodes de mesure applicables au matériel de radiocommunication utilisé dans les services mobiles, Première partie: Définitions générales et conditions normales de mesure. On utilisera ces définitions pour l'application des méthodes normales de mesure décrites ailleurs dans cette série * et sélectionnées pour caractériser les systèmes de secret.

3. **Termes et définitions**

Les termes suivants sont répertoriés et définis dans l'ordre alphabétique anglais. Cette méthode didactique a été retenue parce que le domaine du « secret » est relativement récent dans les services mobiles.

Note. — Dans la présente norme, on entend par « codeur » et « décodeur » les appareils destinés à travestir l'information; en conséquence, ces appareils diffèrent des codeurs et décodeurs employés en signalisation sélective.

3.1 *Décodeur analogique*

Dispositif qui, à partir d'un signal analogique codé, restitue le signal analogique initial, le signal codé et le signal initial étant liés par une fonction de décodage.

3.2 *Codeur analogique*

Dispositif qui convertit un signal analogique en un signal de forme différente, le signal initial et le signal codé étant liés par une fonction de codage.

3.3 *Signal analogique*

Signal qui suit de façon continue la variation d'un phénomène physique avec un nombre infini de valeurs possibles.

Note. — Cette définition est celle de la Recommandation 432.1 du CCIR, volume 1, New Delhi, 1970.

* A l'étude

**METHODS OF MEASUREMENT FOR RADIO EQUIPMENT
USED IN THE MOBILE SERVICES**

**PART 7: PRIVACY EQUIPMENT
SUPPLEMENTARY DEFINITIONS**

1. Scope

This international standard applies to electronic devices and systems designed to provide communications privacy through the techniques of encoding information prior to transmission and subsequent reconstruction of information to original form by the intended receptor. It is the intent of such systems that transmission intercepted by unauthorized receptors will prove unintelligible. This standard applies to systems acting on analogue, digital or combination of analogue and digital information.

2. Object

This publication gives standard definitions for privacy equipment, not otherwise included in the general definitions of Publication 489-1: Methods of Measurement for Radio Equipment Used in the Mobile Services, Part 1: General Definitions and Standard Conditions of Measurement. These definitions shall be used when applying the standard methods of measurement, described elsewhere in this series, * selected for the assessment of privacy equipment.

3. Terms and definitions

The following terms are listed alphabetically and defined. This tutorial approach has been taken because the field of "privacy" is relatively new in the mobile services.

Note. — The terms "encoder" and "decoder" used in this standard refer to apparatus intended for the purpose of disguising information and are, therefore, different from encoders and decoders that are used for selective signalling.

3.1 Analogue decoder

A device that converts an encoded analogue signal to the original analogue signal where the encoded and original signals are related by a decoding function.

3.2 Analogue encoder

A device that converts an analogue signal to a different signal format, where the original and encoded signals are related by an encoding function.

3.3 Analogue signal

A signal that follows the variation of a physical phenomenon continuously with an infinite number of possible values.

Note. — This definition is the same as in the CCIR New Delhi Recommendation 432.1, volume 1, 1970.

* Under consideration

3.4 *Indice de netteté*

(A l'étude.)

3.5 *Synchronisation automatique*

Type de synchronisation utilisant une information implicitement contenue dans le signal codé porteur de l'information, à l'entrée du décodeur. Aucun signal supplémentaire séparé (préambules, par exemple) n'est nécessaire pour effectuer la synchronisation.

3.6 *Codeur découpeur de bande*

Codeur qui réalise le secret des communications en découpant le spectre à fréquence acoustique en une série de bandes secondaires dont l'ordre dans l'échelle des fréquences est permuté avant transmission.

3.7 *Transmission en clair*

Mode de transmission des communications dans un système de secret dans lequel le signal porteur de l'information n'est pas codé. La transmission en clair s'effectue quand le codeur et le décodeur sont court-circuités. Un signal en clair est un signal non traité, c'est-à-dire un signal qui n'a pas été codé.

3.8 *Code*

Un code est un plan préétabli pour représenter l'information par un nombre limité de valeurs ou de symboles matérialisés par un ensemble particulier ou une séquence particulière de conditions désirées ou d'événements. Certains algorithmes de codage peuvent accepter des millions de codes possibles. Les règles, établies en commun pour le codeur et le décodeur, régissent les processus de codage et de décodage. Le code en vigueur reste constant pendant la durée de transmission du message.

3.9 *Délai de transition de code*

Intervalle de temps entre l'instauration d'une nouvelle clé caractéristique et le début de son influence utile sur le processus de codage ou de décodage.

3.10 *Système de secret des communications*

Système de communication dans lequel l'information est transmise sous forme codée de manière à être intelligible aux récepteurs non spécialisés. L'ensemble de réception du système est équipé d'un appareil de décodage qui rend intelligible aux récepteurs spécialisés l'information codée transmise.

3.11 *Corrélation*

Procédé employé pour contrôler la synchronisation, dans lequel le système est interrogé périodiquement pour vérifier que la synchronisation s'effectue correctement.

3.12 *Bande critique*

Bande de fréquences, centrée sur la fréquence d'une tonalité, hors de laquelle le bruit n'a pas d'effet de masquage notable.

Note. — Une tonalité masquée par un bruit à spectre continu est essentiellement affectée par les composantes du spectre de bruit situées à proximité immédiate (bande critique) de cette tonalité.

3.4 *Articulation index*

(Under consideration.)

3.5 *Automatic synchronization*

A type of synchronization utilizing information that is intrinsically part of the encoded information-carrying signal, at the input of the decoder. No additional separate signals (e.g. preambles) are required to accomplish synchronization.

3.6 *Bandsplitter encoder*

An encoder that achieves communications privacy by breaking the audio-frequency spectrum into a series of sub-bands and permutating their order on the frequency scale prior to transmission.

3.7 *Clear mode*

Communications within a privacy system in which the information-carrying signal is not encoded. A clear-mode transmission occurs when the encoder and decoder are by-passed. A clear signal is an unprocessed signal, i.e. a signal which has not been encoded.

3.8 *Code*

A code is a pre-arranged plan for representing information by a finite number of values or symbols as a particular arrangement or sequence of desired conditions or events. A given encoding algorithm may accept millions of possible codes. The code refers to a control setting which corresponds in both encoder and decoder, and which directs the encoding and decoding processes. The code in force remains constant for the duration of a message's transmission.

3.9 *Code switching-span*

The time lag between the institution of a new key character and the initiation of its useful operation in the encoding or decoding process.

3.10 *Communications privacy system*

A communication system in which information is transmitted in coded form so as to be unintelligible to unintended receptors. The receiving element of the system is equipped with decoding apparatus that renders the coded information being transmitted intelligible to the intended receptor.

3.11 *Correlation*

A process used to monitor the synchronization function. It is a process which periodically checks the system to ensure that proper synchronization is taking place.

3.12 *Critical band*

A frequency band, centred on the frequency of a tone, beyond which noise energy has no significant masking effect.

Note. — A tone masked by a continuous noise spectrum is primarily affected by components of the noise spectra in the immediate vicinity (critical band) of the tone.

3.13 *Algorithme de décodage*

Procédure logique employée pour décoder un signal codé.

3.14 *Procédé de décodage*

Procédure plus générale que l'algorithme de décodage, en ce qu'elle se rapporte non seulement au décodage proprement dit, mais encore aux caractéristiques du signal à l'entrée du décodeur, aux signaux aléatoires, à la production de clés caractéristiques et au processus de synchronisation.

3.15 *Système à décodage numérique*

Système qui reçoit des signaux sous forme numérique.

3.16 *Système à codage numérique*

Système qui fournit des signaux sous forme numérique.

3.17 *Signal numérique*

Signal qui, convenablement interprété, représente sous forme quantifiée, la valeur d'une grandeur physique (dans le cas d'une information) ou l'action requise d'une commande (dans le cas d'une commande) (V.E.I. 37-15-055).

3.18 *Mode de transmission codé*

Mode opérationnel d'un système destiné au secret des communications. Le signal porteur de l'information est codé avant émission et décodé par un récepteur spécialisé pour procurer à la sortie un message intelligible.

3.19 *Algorithme de codage*

Procédure logique employée pour coder le signal, par exemple au moyen des techniques de découpage de la bande ou de sauts de fréquence. La clé caractéristique et son programmeur de commande, le code, sont des variables d'entrée de l'algorithme de codage (voir aussi les définitions données aux paragraphes 3.8 et 3.25).

3.20 *Procédé de codage*

Ensemble des fonctions du système relatives au traitement du signal porteur de l'information.

3.21 *Paramètres excitateurs*

Valeur caractéristique (dans les vocoders) de la fréquence fondamentale (ou hauteur) des sons vocaux, plus un signal auxiliaire (ronflement-sifflement) indiquant la présence ou l'absence de vocalisation.

3.22 *Système à sauts de fréquence*

Système qui transpose un ou plusieurs segments de la bande de fréquences du signal d'entrée selon un code donné.

3.23 *Système à inversion de fréquence*

Système dans lequel le codage du signal à fréquence acoustique est obtenu par inversion de la gamme des fréquences acoustiques.

3.13 *Decoding algorithm*

The logical scheme used to decode an incoming encoded signal.

3.14 *Decoding process*

Decoding process is more general than “decoding algorithm” in that it pertains to decoder input-signal characteristics, random signals, key character generation and synchronization process as well as to direct-signal decoding actions.

3.15 *Digital decoder system*

A system for which input signals are in digital form.

3.16 *Digital encoder system*

A system for which output signals are in digital form.

3.17 *Digital signal*

A signal which, when suitably interpreted, expresses in a quantized form the values of a physical quantity in the case of an information signal or the action required in the case of a control signal (I.E.V. 37-15-055).

3.18 *Encode/decode mode*

Operational mode of a communications privacy system. The information-carrying signal is encoded prior to transmission and decoded after reception to provide an intelligible signal to the intended receptor.

3.19 *Encoding algorithm*

A logical scheme used to encode the signal. Examples of encoding algorithms are bandsplitting techniques and frequency hopping. The key character and its controller, the code, are variable inputs to the encoding algorithm (see also definitions given in Sub-clauses 3.8 and 3.25).

3.20 *Encoding process*

All system actions relative to processing the information-carrying signal.

3.21 *Excitation parameters*

A characteristic (in vocoder systems) of the fundamental frequency (or pitch) of voiced sounds, and an auxiliary (buzz-hiss) signal which indicates the presence or absence of voicing.

3.22 *Frequency hopper system*

A system which transposes one or more segments of the input-frequency band in accordance with a code.

3.23 *Frequency inverter*

A system which encodes an audio-input signal by inverting the audio-frequency band.

3.24 Codeur/décodeur idéal

Le codeur idéal code tout signal d'entrée dans la forme précise voulue par l'algorithme de codage et le code en vigueur.

Le décodeur idéal décode tout signal d'entrée dans la forme précise voulue par l'algorithme de décodage et le code en vigueur.

3.25 Signal porteur de l'information

Tout signal qui occupe à dessein une largeur de bande non nulle. Plus particulièrement, signal qui porte l'information destinée à être transmise d'une extrémité du système à l'autre.

3.26 Clé caractéristique

Élément de commande qui fait office de variable pour un algorithme donné et, le cas échéant, pour un code déterminé. La clé caractéristique agit sur le signal porteur de l'information pour en modifier la forme: dans un codeur, de la forme claire à la forme codée; dans un décodeur, de la forme codée à la forme claire.

3.27 Effet de masquage (brouillage)

Dissimulation d'un signal par addition de signaux parasites. Le masquage est habituellement réalisé par l'addition de bruit ou de pseudo-bruit au signal porteur de l'information.

3.28 Indice de masquage

Indice donné par la formule suivante:

$$M = 10 \log \frac{T}{T\sigma}$$

où:

M = indice de masquage, exprimé en décibels

$T\sigma$ = niveau de seuil du signal pur en environnement non perturbé

T = niveau correspondant au signal qui reste juste audible en présence du bruit

3.29 Pseudo-bruit (bruit simulé)

Signal qui apparaît comme une perturbation aléatoire pour un récepteur non spécialisé. Il est produit à dessein par un algorithme de codage dans le codeur du signal porteur de l'information et peut être éliminé dans le décodeur par l'emploi d'un algorithme de décodage complémentaire. Il est employé pour masquer le signal porteur de l'information et le rendre ainsi inintelligible aux récepteurs non spécialisés.

3.30 Signaux aléatoires

Signaux émis sans ordre ni structure déterminés. Des signaux aléatoires peuvent être employés dans le procédé de codage pour réduire la possibilité de décodage du signal porteur de l'information par des récepteurs non spécialisés.

3.31 Fiabilité

Probabilité d'effectuer sans défaillance une fonction spécifiée dans des conditions données et pendant un délai déterminé.

3.31.1 Fiabilité du décodage

Probabilité qu'un signal correctement codé présenté à l'entrée du décodeur donne, en sortie de celui-ci, le même signal porteur de l'information que celui primitivement utilisé pour créer le signal codé.

3.24 *Ideal encoder/decoder*

An ideal encoder is one which encodes any input signal to the precise form intended by the encoding algorithm and code in force.

An ideal decoder is one which decodes any input signal to the precise form intended by the decoding algorithm and code in force.

3.25 *Information-carrying signal*

In general, a signal which intentionally occupies a bandwidth greater than zero. The signal that carries the information intended to be communicated from one end of the system to the other.

3.26 *Key character*

The controlling agent which is a variable under a given encoding algorithm and, possibly, under a given code. The key character operates on an information-carrying signal to change its form; in an encoder, from clear to encoded form, or in a decoder, from encoded to clear form.

3.27 *Masking*

Obscuring a signal by adding spurious signal energy. Masking is usually accomplished by adding noise or pseudo-noise to an information-carrying signal.

3.28 *Masking figure*

The masking figure is given by the following formula:

$$M = 10 \log \frac{T}{T\sigma}$$

where:

M = masking figure, expressed in decibels

$T\sigma$ = threshold level of pure signal in quiet environment

T = level when the signal is just barely audible when noise is present

3.29 *Pseudo-noise*

A signal that appears to be a random disturbance to an unintended receptor. It is purposely generated by an encoding algorithm in the information-carrying signal encoder. The pseudo-noise can be removed by the decoder using a complementary decoding algorithm. Pseudo-noise is used to mask the information-carrying signal to make it unintelligible to unintended receptors.

3.30 *Random signals*

Signals emitted in no set order or pattern. Random signals may be used in the encoding process to minimize the possibility of decoding the information-carrying signal by unintended receptors.

3.31 *Reliability*

Reliability is the probability of performing, without failure, a specified function under given conditions for a specified period of time.

3.31.1 *Reliability of decoding*

Reliability of decoding is the probability that a correctly encoded signal at the input of the decoder is translated by the decoder to the same information-carrying signal that was used to create the encoded signal.

3.31.2 *Fiabilité du codage*

Probabilité que le signal porteur de l'information soit codé sous la forme prévue par l'algorithme de codage.

3.31.3 *Fiabilité du système de secret*

Probabilité qu'un élément d'information introduit à l'entrée du système et transmis suivant le mode de transmission codé soit interprété correctement par le récepteur spécialisé.

3.32 *Cadence de roulement*

Cadence à laquelle la clé caractéristique varie.

3.33 *Synchronisation*

Maintien des relations correctes de phase entre le signal porteur de l'information et les fonctions de codage et de décodage.

3.34 *Décodeur d'essai*

Décodeur spécifié convenant à l'essai des codeurs.

Note. — Il peut exister un jeu de spécifications définissant un « décodeur d'essai » pour chaque type de codeur.

3.35 *Codeur d'essai*

Codeur spécifié convenant à l'essai des décodeurs.

Note. — Il peut exister un jeu de spécifications définissant un « codeur d'essai » pour chaque type de décodeur.

3.36 *Affaiblissement de transition*

Altération globale à travers le système de la réponse en fréquence du signal porteur de l'information provoquée par les codeurs découpeurs de bande.

3.37 *Récepteur non spécialisé*

Tout dispositif, ou toute personne employant ce dispositif, qui intercepte sans y être autorisé le signal codé porteur de l'information.

3.38 *Paramètres caractérisant l'appareil vocal*

Paramètres d'un vocoder déduits du spectre en amplitude de la transformée de Fourier rapide du signal vocal, tel qu'il est mesuré par une batterie de filtres passe-bande contigus, de détecteurs et de filtres passe-bas.

3.39 *Vocoder*

Dispositif qui comprime la bande du signal vocal en utilisant les propriétés caractéristiques de celui-ci. Il opère en extrayant du signal les paramètres à variation lente et en les transmettant séparément des composantes à variation rapide. Ces paramètres, qui découlent de la configuration physique de l'appareil vocal et du caractère de son excitation, véhiculent une information suffisante pour permettre de recréer ou de synthétiser une approximation du signal vocal, d'origine à l'extrémité réceptrice du système.

3.31.2 *Reliability of encoding*

Reliability of encoding is the probability that an information-carrying signal is encoded in the form intended by the encoding algorithm.

3.31.3 *Reliability of the privacy system*

Reliability of the privacy system is the probability that a unit of information input to the system, and subsequently transmitted in the encode/decode mode, is judged by the intended receptor to be the same unit of information.

3.32 *Roll rate*

The rate at which the key character is varied.

3.33 *Synchronization*

The maintenance of the proper phase relationships between the information-carrying signal and the encoding and decoding functions.

3.34 *Test decoder*

A specified decoder suitable for testing an encoder.

Note. — There may be a set of specifications that define a “test decoder” for each type of encoder.

3.35 *Test encoder*

A specified encoder suitable for testing a decoder.

Note. — There may be a set of specifications that define a “test encoder” for each type of decoder.

3.36 *Transitional attenuation*

The overall system alteration of the information-carrying signal frequency response caused by the bandsplitter encoders.

3.37 *Unintended receptor*

Any device, or person using a device, which intercepts the encoded information-carrying signal in an unauthorized manner.

3.38 *Vocal-tract characterization parameters*

Parameters from a vocoder system derived from the fast Fourier amplitude spectrum as measured by a bank of contiguous band-pass filters, detectors and low-pass filters.

3.39 *Vocoder*

A system which achieves speech bandwidth compression by extracting slowly-varying parameters from the speech waveform and transmitting them separately from the more rapidly varying components. These parameters relate to the physical configuration of the vocal tract and to the character of its excitation. They convey sufficient information to enable one to recreate or synthesize an approximation of the original speech at the receiving end of the system.

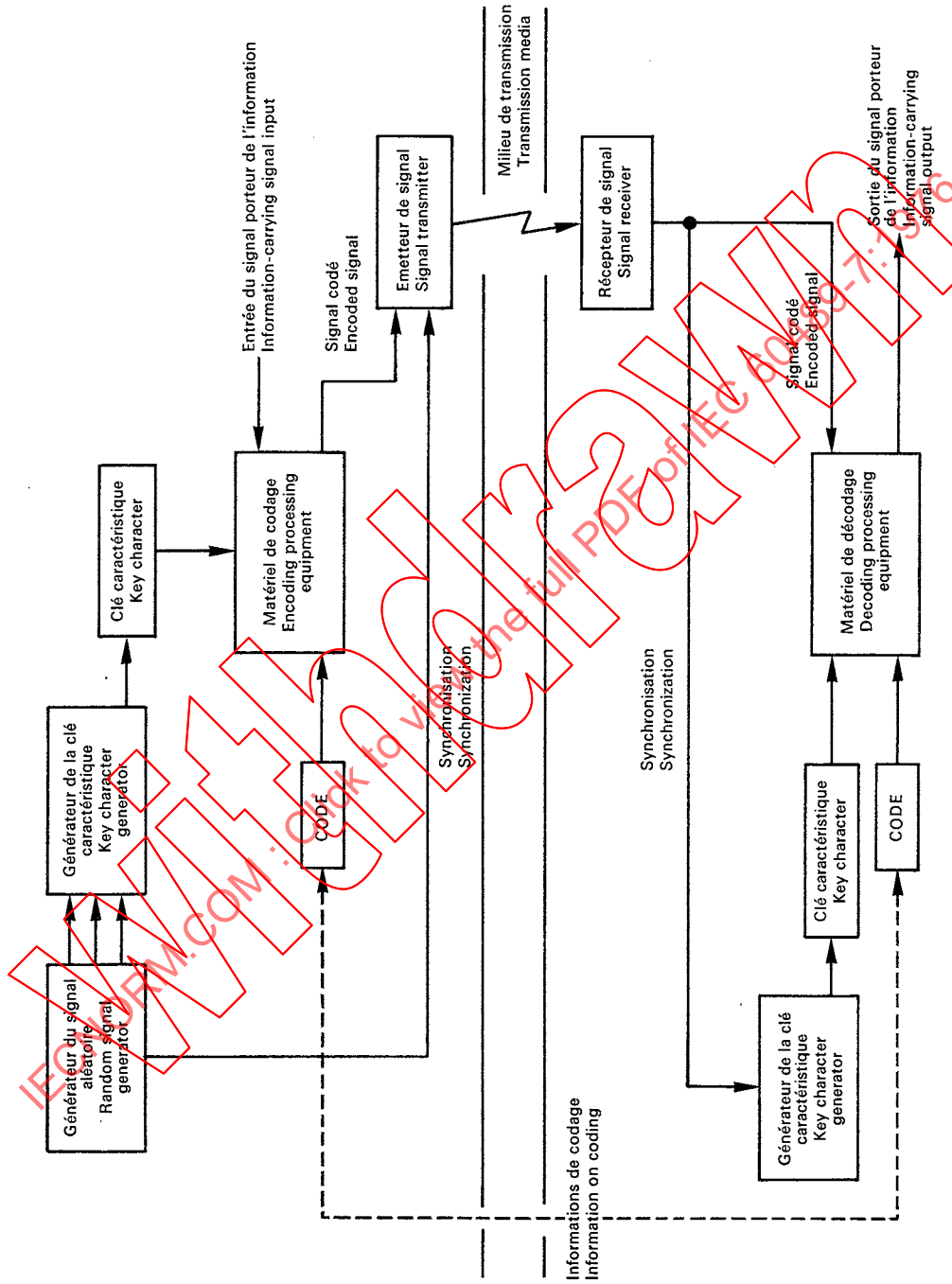


FIG. 1. — Schéma fonctionnel type d'un système de secret du signal vocal.
Block diagram of a typical speech privacy system.