Techniques analogiques et numériques de sécurisation des transmissions sonores

Sommaire

Introduction

Définition : La cryptophonie consiste à sécuriser un message sonore d'origine analogique à l'aide de méthodes de cryptage reposants sur des techniques de traitement du signal

Techniques analogiques

3 méthodes :

- L'inversion
- Le brouillage de bande
- Le multiplexage temporel

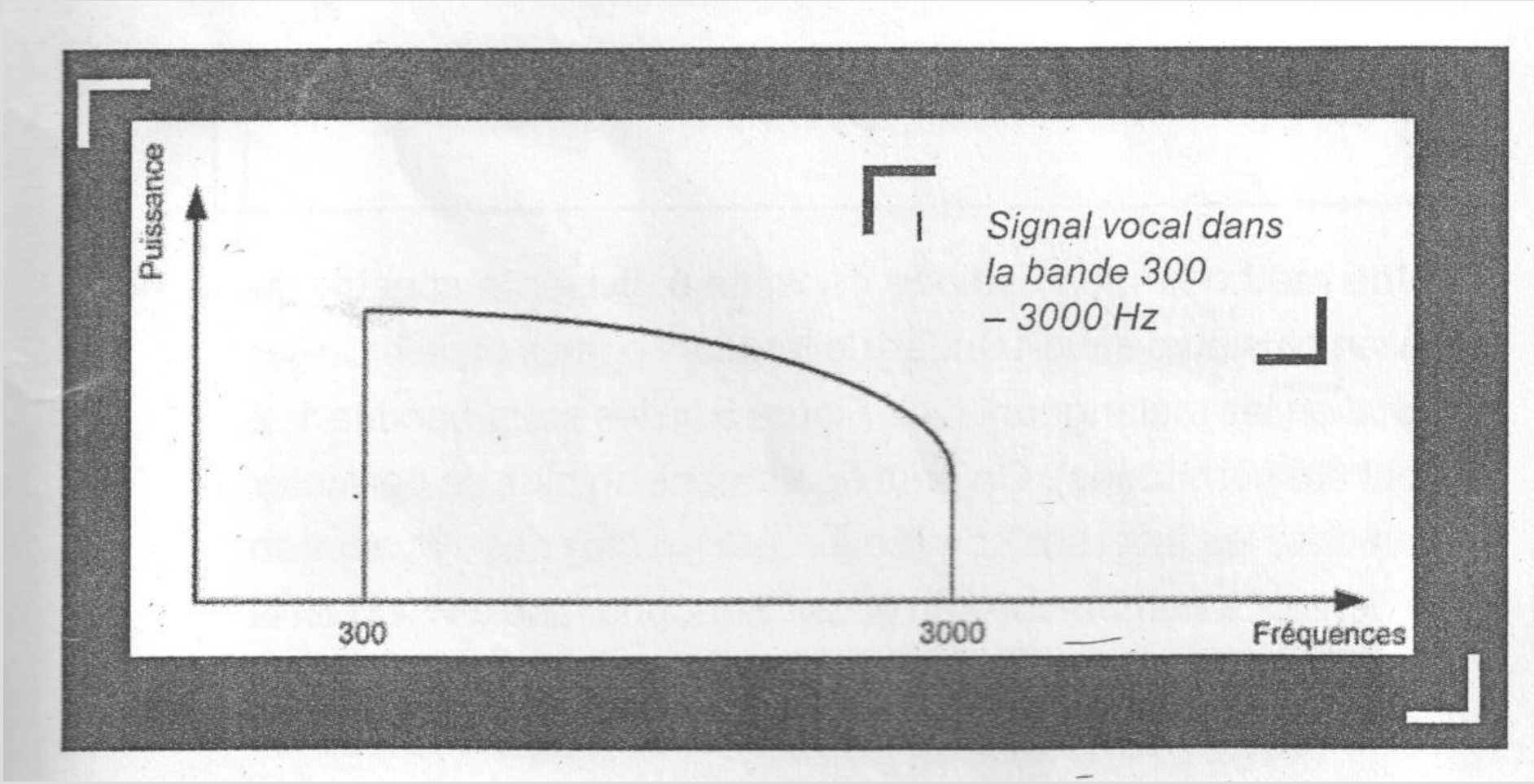
L'inversion

Principe : inverser les fréquences du signal.

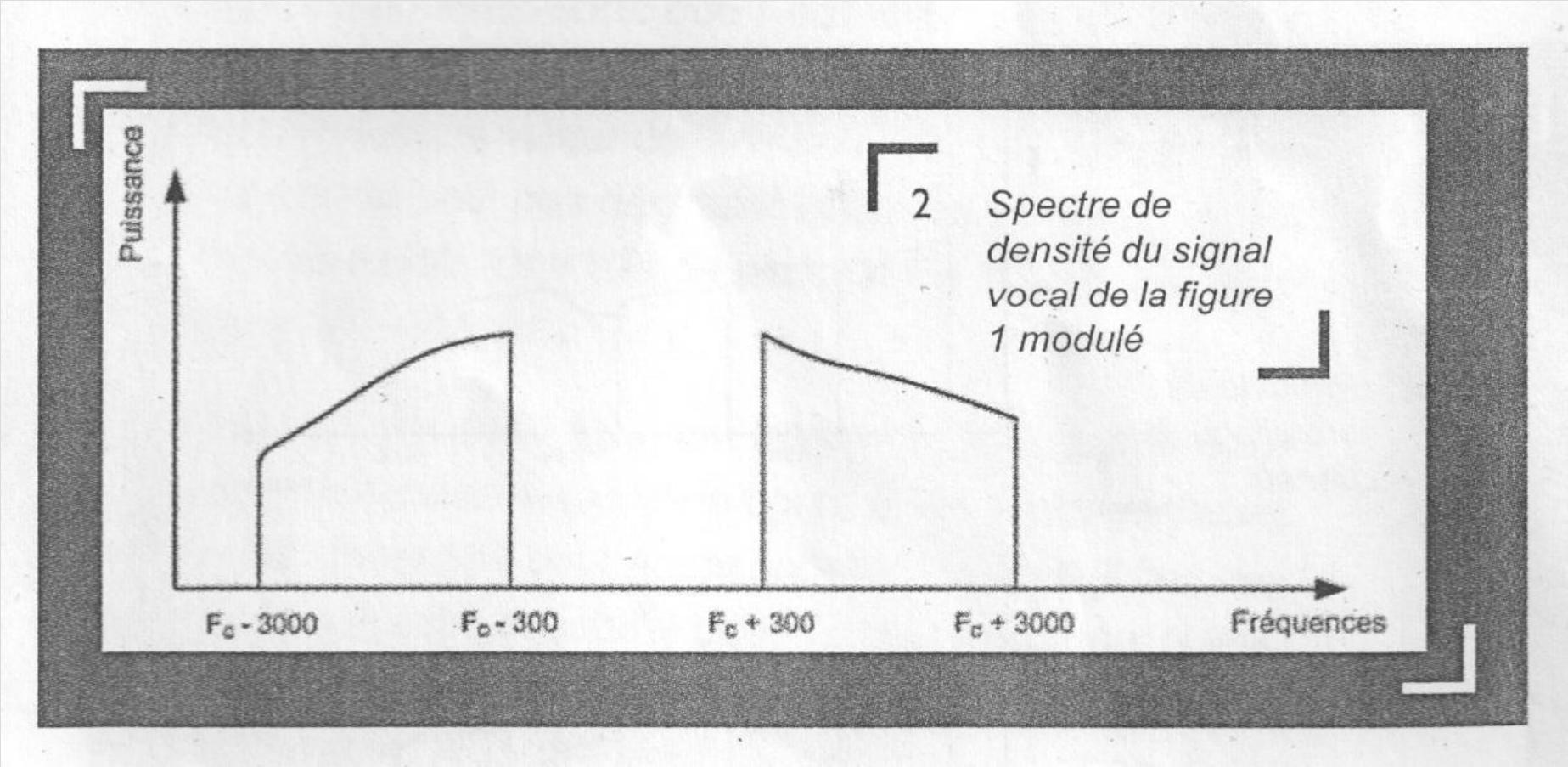
On introduit un signal dit « modulateur équilibré » au signal d'origine. On introduit une fréquence porteuse. Après filtrage, on obtient un signal inversé

Sécurisation : décalage de bandes

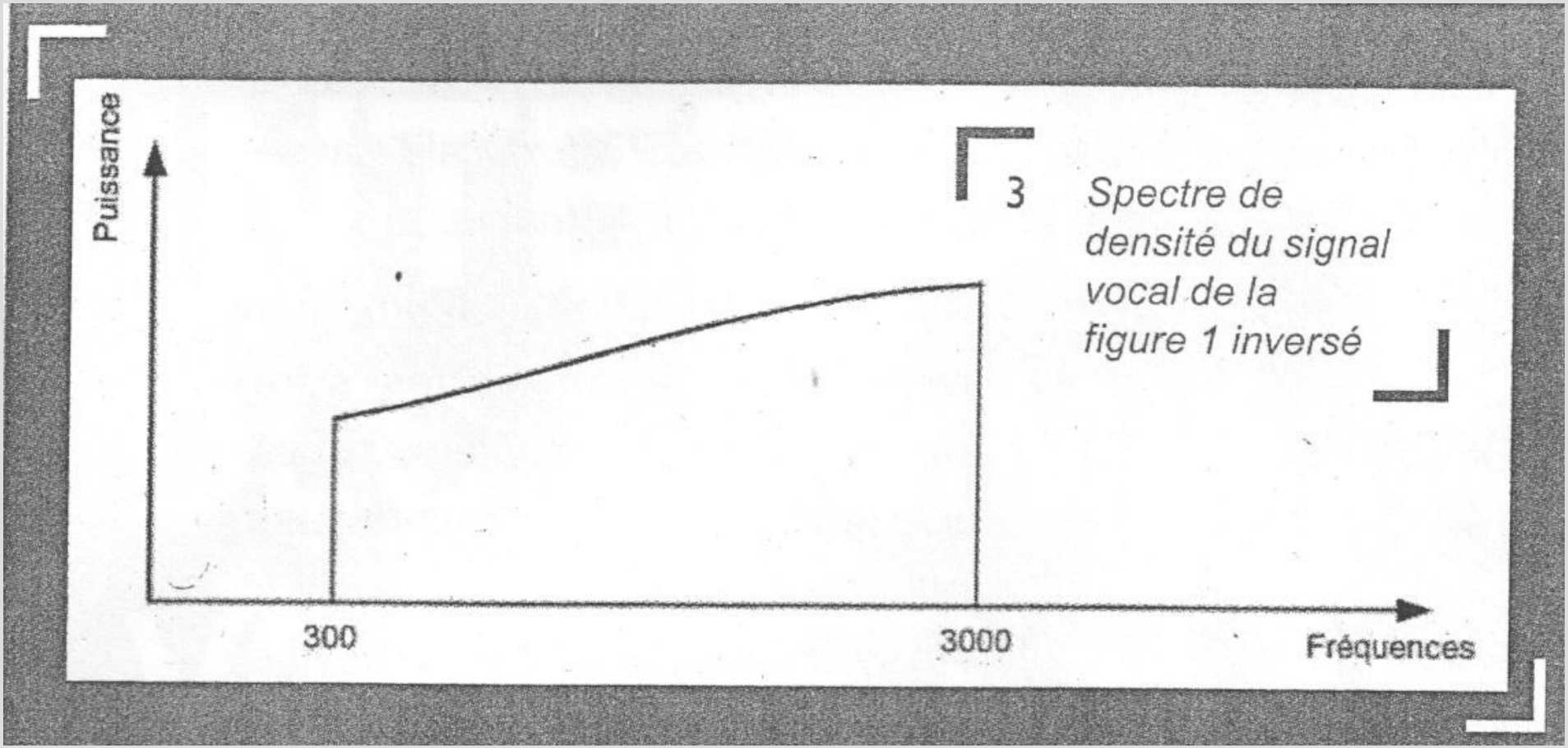
Exemple


Puissance
Signal vocal dans
la bande 300
– 3000 Hz
300
3000
Fréquences

Exemple


Puissance
2
Spectre de densité du signal vocal de la figure 1 modulé
Fc - 3000
Fc - 300
Fc + 300
Fc + 3000
Fréquences

Exemple



3 *Spectre de densité du signal vocal de la figure 1 inversé*

L'inversion

Inconvénients :

- Le nombre de possibilités de fréquences est insuffisant.
- Le signal n'est pas assez brouillé pour empêcher la compréhension du message

Le brouillage de bande

Principe : Divise le signal en sous-bandes de largeurs égales et permuter l'ordre des sous-bandes

On obtient N! permutations.

Le brouillage de bande

Problèmes :

- Certaines permutations sont trop proches du signal d'origine, il faut prendre en compte le nombre de dérangements.
- 40% de l'énergie d'un signal se trouve dans les deux premières sous-bandes.

Brouillage de bandes

Solution : Validation par l'écoute.

Sécurisation : Mise en mémoire des permutations validées, et sélection de la permutation par un générateur aléatoire.

Inconvénients : Risques de décodage par l'oreille humaine.

Le multiplexage temporel

Principe : Diviser le signal en trames, puis les diviser en segments permutables.

Sécurisation : Choix de la durée des trames et de la permutation des segments.

Choix de la durée

- Elle doit être assez courte pour que l'information ne soit pas importante, mais pas trop pour l'intelligibilité du signal.
- Elle doit respecter les délais d'attente acceptés pour la transmission du message.
- Une durée trop courte augmente le risque d'interception de la trame.

Choix de la permutation

- Problème similaire à la technique précédente.
- Contrainte supplémentaire : Le signal doit être le plus distordu possible (deux segments consécutifs ne doivent pas être à moins de trois positions l'un de l'autre).
- Aucune permutation ne doit permettre de restaurer une trame brouillée à l'aide d'une autre des permutations enregistrées.

Techniques numériques

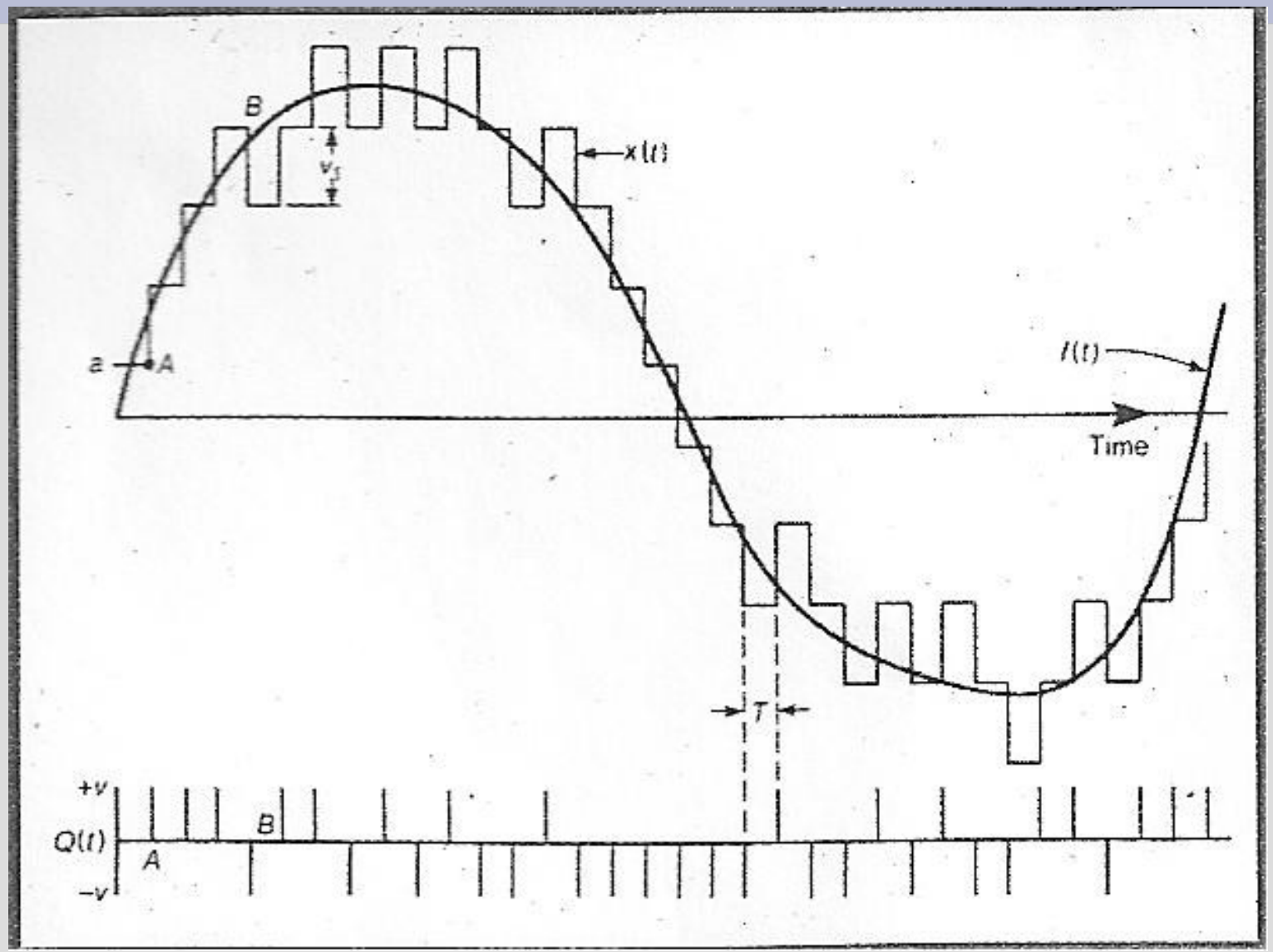
- Méthodes de conversion analogique/numérique :
  - Modulation linéaire delta (MLD)
  - Vocoders
- Application à la cryptophonie

Modulation linéaire delta

Principe : Construire un signal en escalier en comparant la valeur du signal échantillonné à la valeur réelle du signal.

Objectif : Diminuer la quantité d'informations transmises.

Modulation linéaire delta



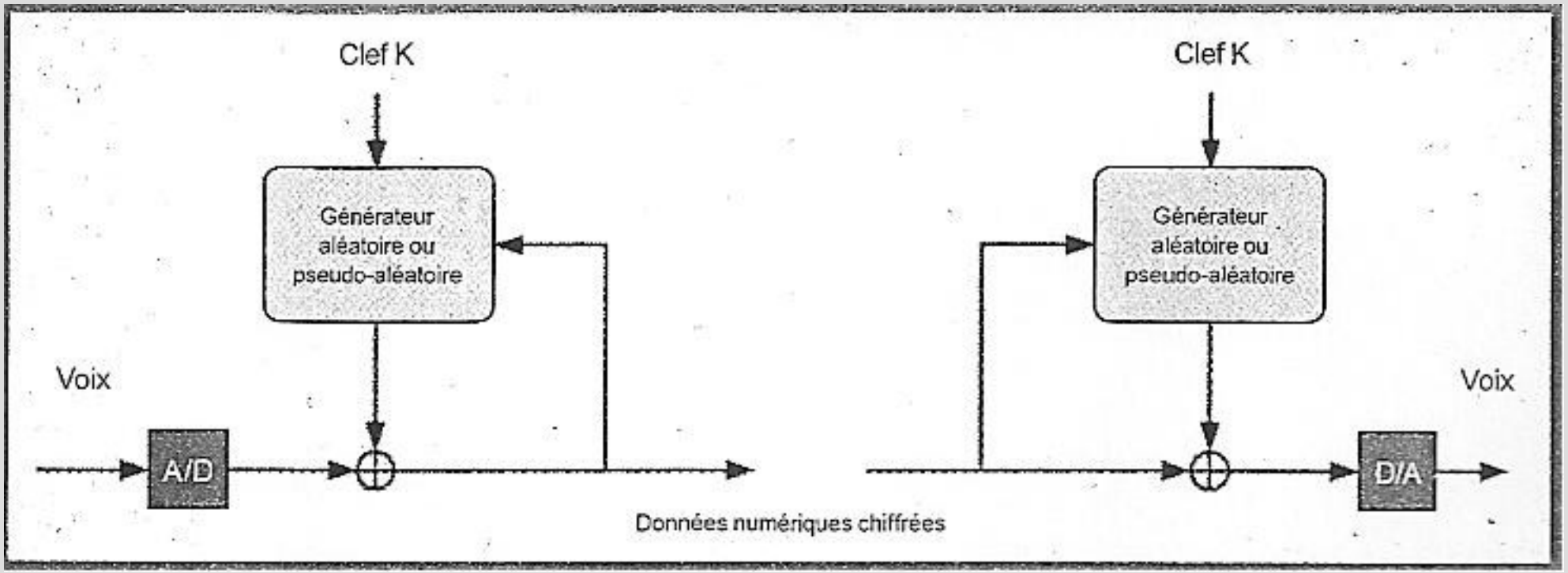
Application à la cryptophonie

Après numérisation, on peut appliquer un système de cryptologie numérique.

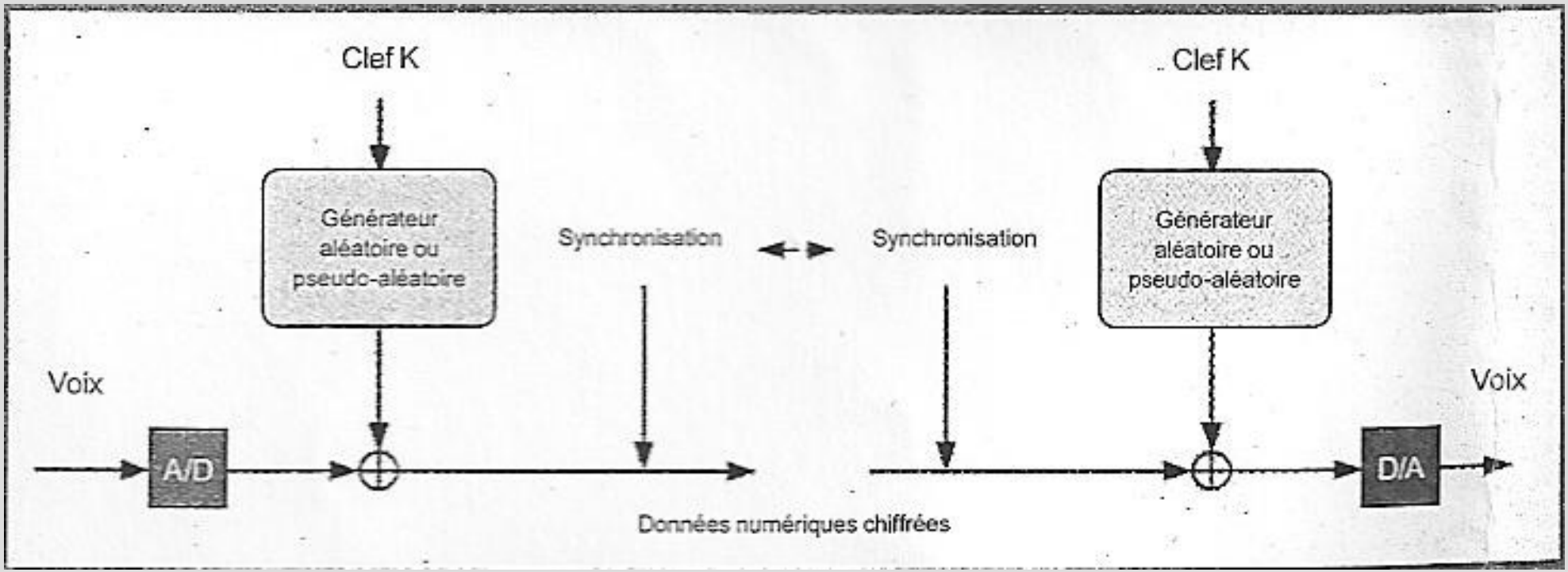
Généralement, on utilise un système par flot de type pseudo-aléatoire. On utilise une clef pour initialiser le système qui produira la séquence aléatoire combinée à la séquence numérisée.

Il y a deux types de systèmes.

Système « autoclave » sur le chiffré



Système avec synchronisation additionnelle



Conclusion