COMMUNIQUE DE PRESSE 2

Diffusion : Immédiate

En 1949, Claude Shannon publie une théorie du chiffrement des communications restée, jusque-là, du domaine de la recherche.

En 2022, Internet et les vrais nombres aléatoires associés au calcul binaire rendent possible une solution simple et peu couteuse, pour restaurer une liberté fondamentale : celle de communiquer librement à l'abri des regards indiscrets.

« La simplicité est la sophistication ultime » – (Léonard de Vinci)

- Nous sommes un groupe d'ingénieurs désireux de partager une technologie qui brise « les règles »
- La vie privée est mise à mal et nos technologies brevetées vous redonnent à nouveau la liberté et protègent vos données (texte-voix- vidéo…)
- Notre système est une grande chance d'utiliser un moyen totalement impiratable et d'échanger sans aucune peur tout type de données.
- Nous mettons à disposition de tout un chacun cette technologie.
- L'utilisation commerciale, gouvernementale et autre de notre système est soumise à différentes licences d'exploitations, après accord

I) GENERALITES:

Le système de cryptage est basé sur l'utilisation d'un code dit « symétrique » à code jetable. Il répond aux critères d'invulnérabilité définis par Shannon.
Le code est composé d'une suite de valeurs vraiment aléatoires (VTRN) dont la longueur est égale au message à transmettre. Le codage la voix (échantillonnage) nécessite un nombre important de valeurs.
La miniaturisation actuelle des mémoires permet de stocker suffisamment de valeurs aléatoires pour assurer plusieurs dizaines, voire centaines d'heures de communication.
La mise en œuvre du procédé décrit dans ces pages a fait l'objet de dépôts de brevets.
La méthode de cryptage utilisée est symétrique, deux exemplaires des mêmes valeurs aléatoires sont nécessaires, une pour chaque poste mobile.
Le cryptage n'est théoriquement possible qu'entre deux postes. Néanmoins, il existe une possibilité d'extension jusqu'à huit postes.
Au-delà, l'extension utilise un serveur GSM de transcodage. Mis a part cette dernière option, l'ap application de cryptage ne nécessite aucun service additionnel particulier (VOIP par ex.).

II) DESCRIPTION GENERALE:

Cette description est subdivisée en plusieurs parties ;

- Généralités sur la transmission de la voix en « numérique »
- Structure des cartes supportant le code aléatoire
- Initialisation du processus suivi de l'organigramme correspondant
- Codage des échantillons à l'émission, synchronisation et organigramme correspondant
- Réception des échantillons cryptés, synchronisation à la réception, décodage et organigramme correspondant
- Remplacement des cartes en fin de vie.

III) GENERALITES SUR LA TRANSMISSION DE LA VOIX EN NUMERIQUE;

Les systèmes modernes de transmission de la voix, font appel à une transmission sous forme numérique. La forme de base de cette transmission se fait en échantillonnant le signal analogique capté par un microphone et en transformant l'amplitude de ces échantillons en valeurs numériques, qui une fois transmises subissent le processus inverse, ce qui reconstitue le signal original. La représentation discrète d'un signal par des échantillons régulièrement espacés exige une fréquence d'échantillonnage supérieure au double de la fréquence maximale présente dans ce signal.(Théorème de Nyquist-Shannon).

Dans le cas de la voix, l'échantillonnage se fait généralement à 8 KHz.

IV) STRUCTURE DES CARTES SUPPORTANT LE CODE ALEATOIRE:

Les cartes utilisées sont du type µSD. Les capacités deces cartes sont suffisantes pour avoir une durée d'utilisation de plusieurs dizaines, voire centaines d'heures de communication codée.

> NOTE : Les deux µSD destinées au cryptage symétrique ne diffèrent que par leur « Type » (1 ou 2). Elles contiennent donc le même nom, le même identifiant unique, et la même suite de valeurs aléatoires.

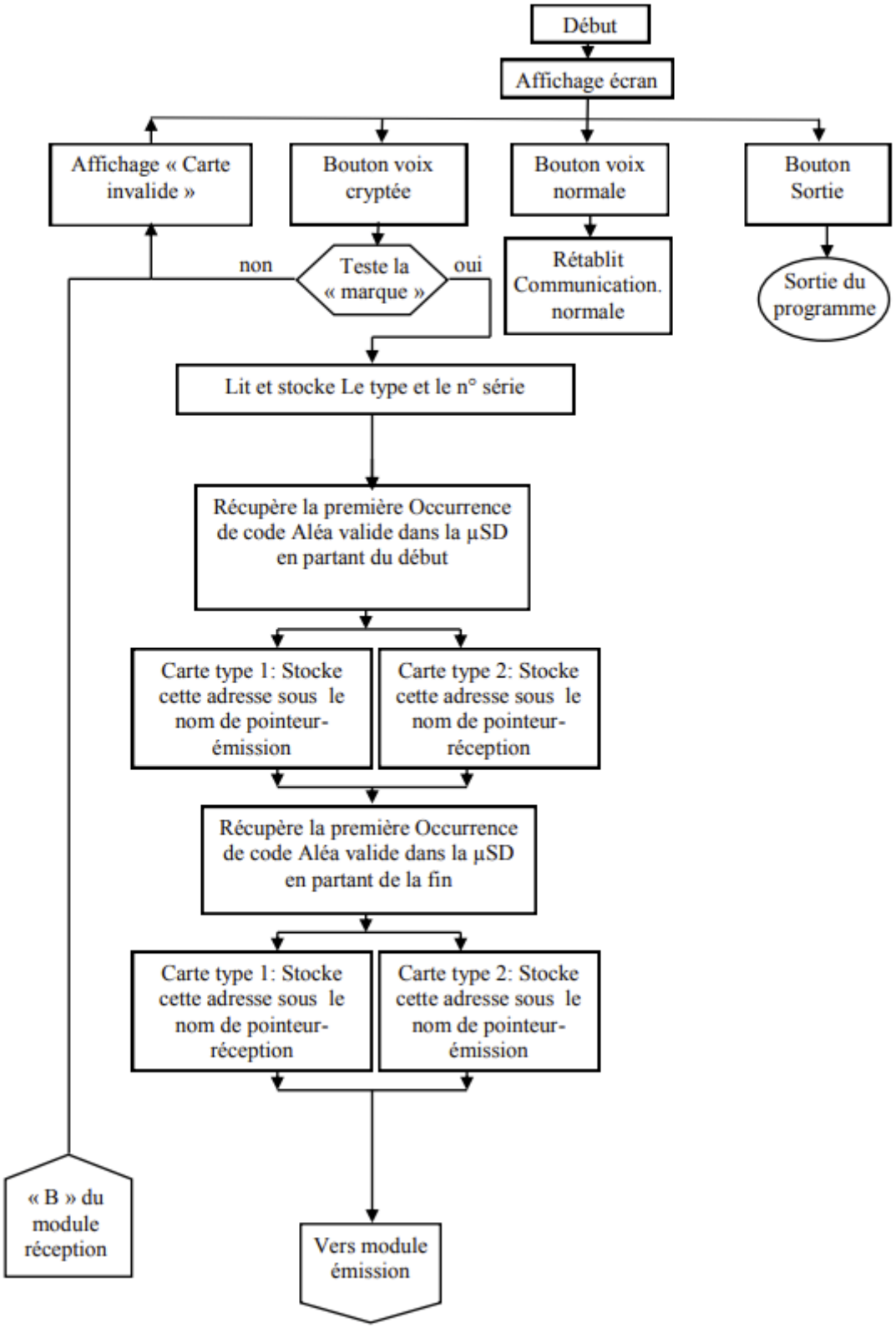
V) INITIALISATION DU PROCESSUS :

Le démarrage de l'application doit afficher à l'écran le nom du logiciel ainsi que trois boutons dans lesquels sont inscrits les textes suivants ; « voix codée », « voix normale », et « sortie ». Puis l'organigramme de la page suivante est effectué :

ORGANIGRAMME GENERAL

Partie initialisation

(NB : Le « N° de série
correspond au N° d'identification de la carte SD)



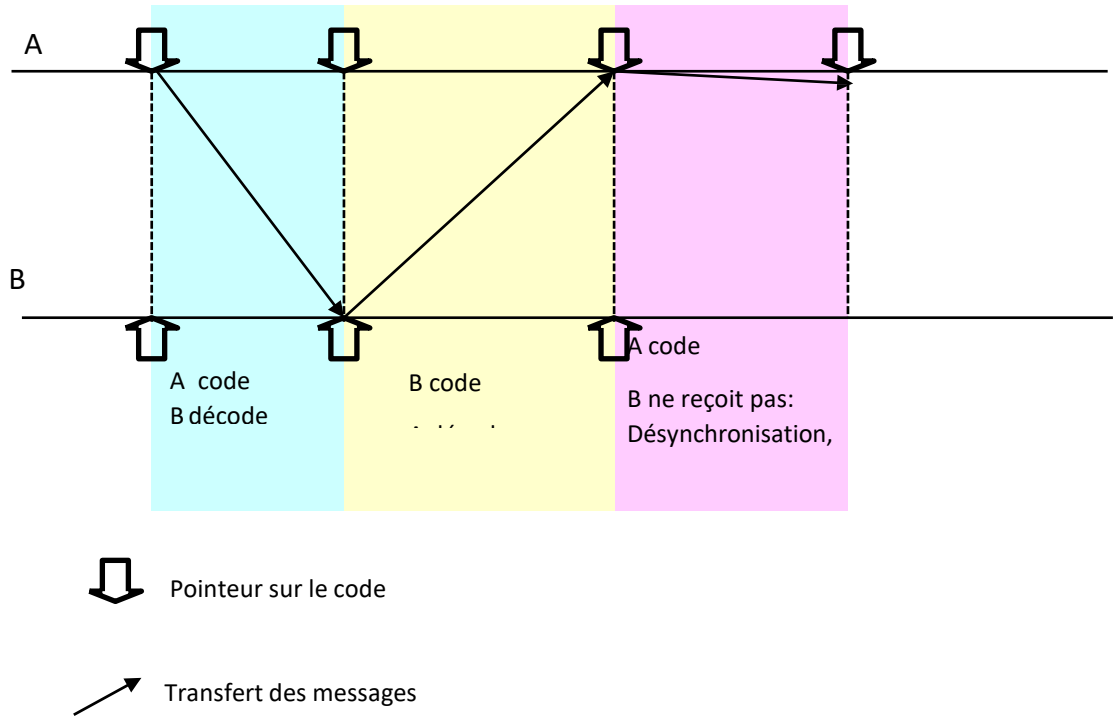
VI) SYNCHRONISATION ET CODAGE:

GENERALITES:

Le décodage des échantillons codés nécessite que les codes soient synchronisés. Les « pointeurs « Doivent avoir la même valeur au codage et au décodage.

Les sources de perturbation amenant la désynchronisation des pointeurs sont nombreuses et imprévisibles. Il est donc nécessaire de les resynchroniser régulièrement.

Dans le cas de l'utilisation d'un seul pointeur pour chaque appareil, l'absence de réception d'une partie des messages émis provoque la désynchronisation des pointeurs. L'un des deux prends « de l'avance » sur l'autre.



Dans le schéma précédent, B n'a aucun moyen de se resynchroniser sur A. S'il est simple d'imaginer que A peut resynchroniser B, à l'inverse, si B veut coder dans cette configuration, A est incapable de « revenir en arrière » pour décoder ; le message envoyé par B; Le code correspondant a été effacé sur A!.

.

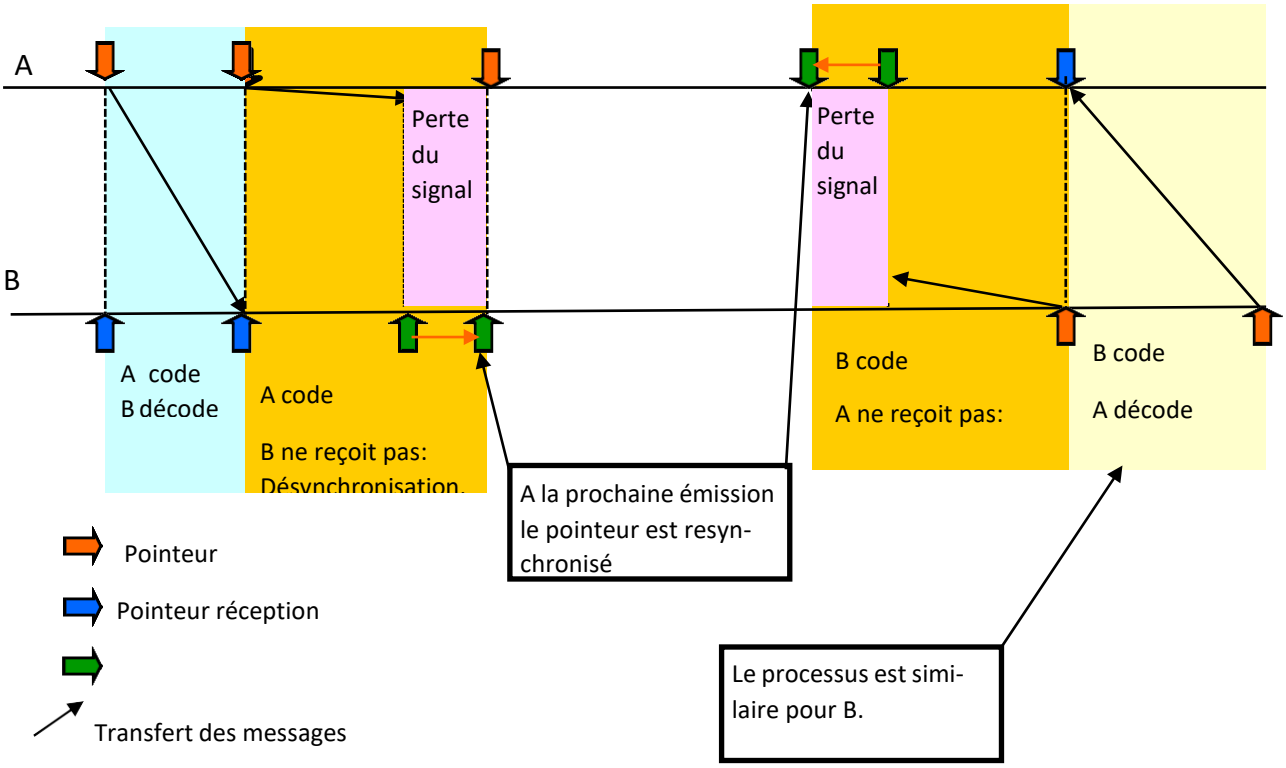
La solution adoptée ici consiste à établir une table de codes par poste. Afin de simplifier on utilise la même table de code, mais chacun utilise pour coder un pointeur différent.
A va pointer sur le début de la table, B va pointer sur la fin de cette même table. Le pointeur A va « Monter » et le pointeur B va « descendre ».

Chaque appareil possède donc deux pointeurs ; le pointeur de réception qui « suit » le pointeur d'émission de l'autre appareil, et un pointeur d'émission qui est suivi par le pointeur réception de l'autre appareil. Chaque pointeur d'émission « démarre » à une extrémité de la table des codes. Toutes les « N » échantillons envoyés, une trame de synchronisation est émise sous la forme d'un « Motif » binaire de reconnaissance, suivi du numéro d'identification unique de la carte, suivi de la valeur du pointeur. (L'envoi de l'identification unique de la carte ne peut se faire qu'au début d'une session; Il sert à validerl'utilisation de deux tables appariées).

Codage et décodage :
Le codage et le décodage se font par application entre la valeur à coder et la valeur aléatoire du code en appliquant une opération ou exclusif (XOR) entre ces deux valeurs. Le décodage s'effectue en appliquant le même opérateur booléen entre la valeur codée et le même code (à la réception)..

Exemple d'opération ou exclusif :

65 XOR 38 = 103 ————> 103 XOR 38=65.



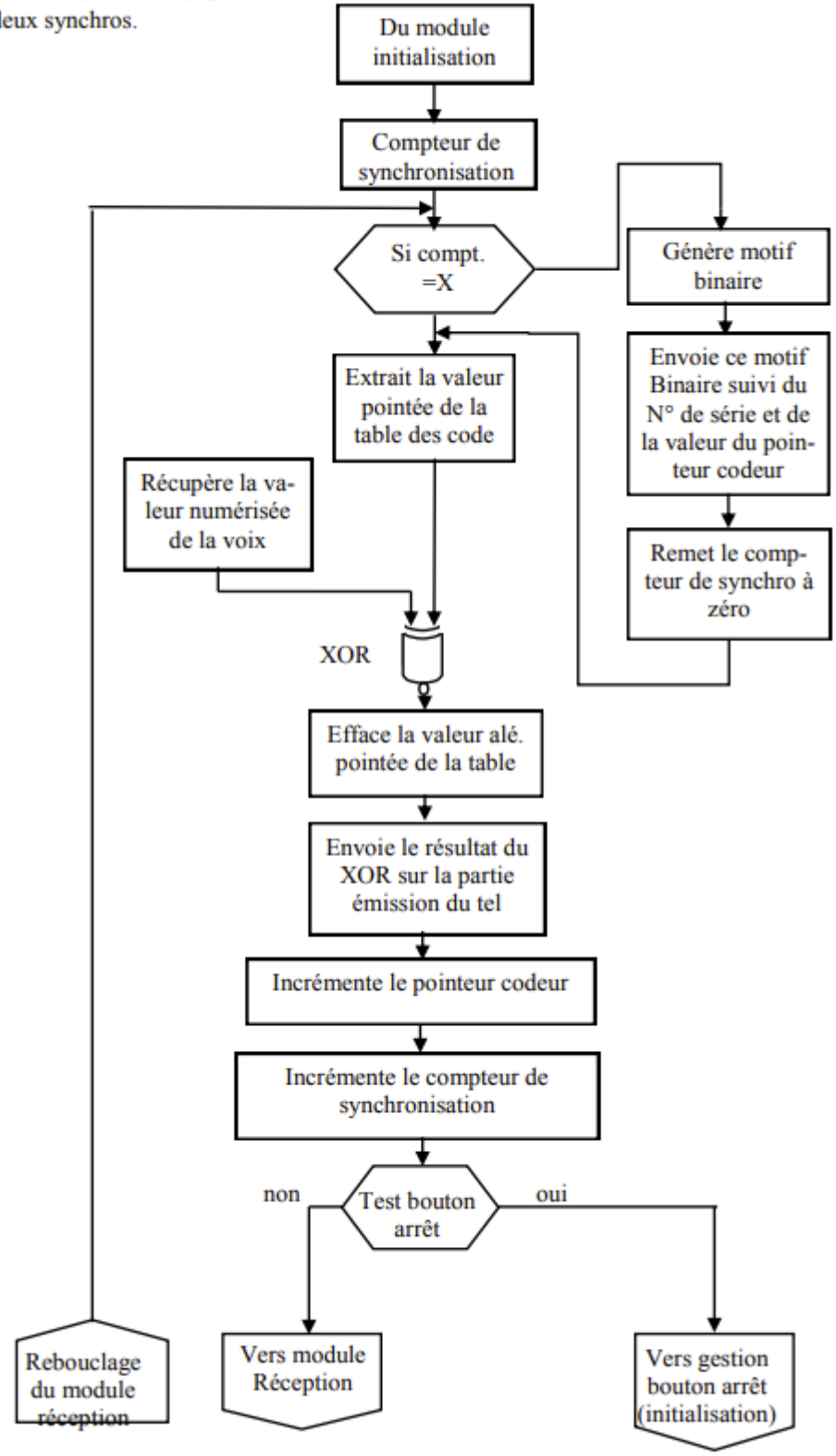
ORGANIGRAMME GENERAL

Partie émission

(NB : Le « N° de série

Correspond au N° d'identification de la carte SD)

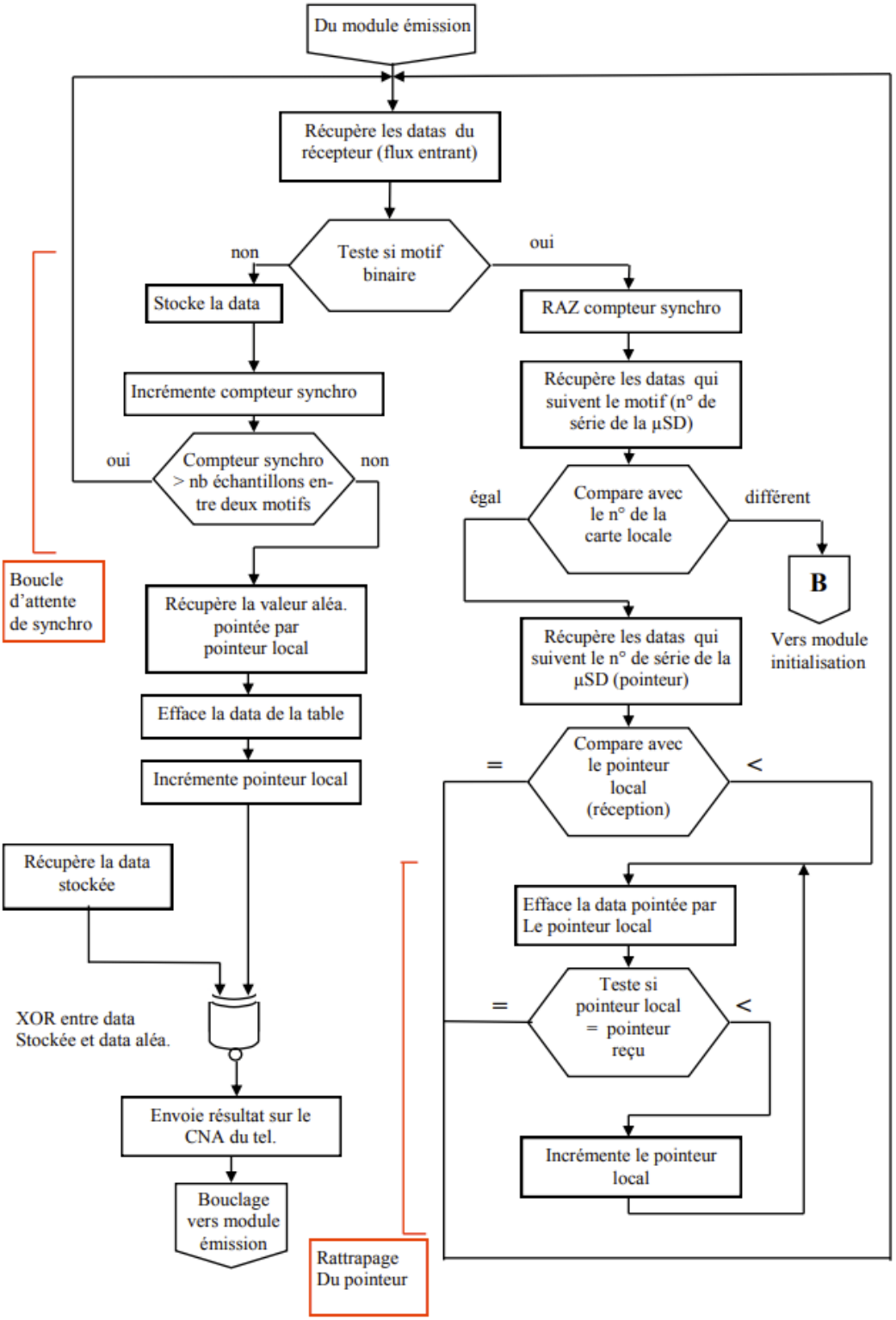
Note: « X »
Est le nombre d'échantillons
entre deux synchros.



ORGANIGRAMME GENERAL

Partie réception

(NB : Le « N° de série
correspond au N° d'identification de la carte SD)



VII) REMPLACEMENT DES CARTES EN FIN DE CYCLE

Le code étant détruit après utilisation, il sera nécessaire de changer les cartes lorsque celles-ci seront épuisées. Afin de prévenir à temps les utilisateurs, un « compteur de temps restant » est affiché sur l'écran du tel.
Le temps restant est obtenu en calculant le nombre de codes non encore utilisés, ce qui se traduit en pratique par le comptage des codes situés entre le pointeur réception et le pointeur émission. Cette valeur sera ramenée en nombre d'heures et de minutes. Le clignotement, et l'émission dans l'écouteur d'un « bip » en dessous d'une certaine valeur (quelques minutes par exemple) avertira l'utilisateur de la nécessité de changer d'urgence sa carte. La synchronisation du changement des deux cartes (utilisateur 1 et utilisateur 2) se fait en mode communication verbale codée ou non.

Une partie des techniciens de l'équipe (Noms de famille non communicables à des tiers) :

- L.A: Ingénieur diplômé : du Génie Civil EFIB (ESIB), Electricien Supelec, Mécanique et Matériaux ISMCM Supmeca, Frigoriste de l'IFFI Energie Atomique (Saclay, Euratom, IFP, CEA, sécurité nucléaire (26 brevets)

- R.R : Ingénieur Télécom en charge des études et expérimentations

Pour en savoir plus sur la recherche de Claude Shannon :
https://dkrizanc.web.wesleyan.edu/courses/351/1.pdf

- Echantillon d'un message vocal original
- Echantillon de ce message codé avec le principe décrit dans ce communiqué