

TRES SECRET

02032

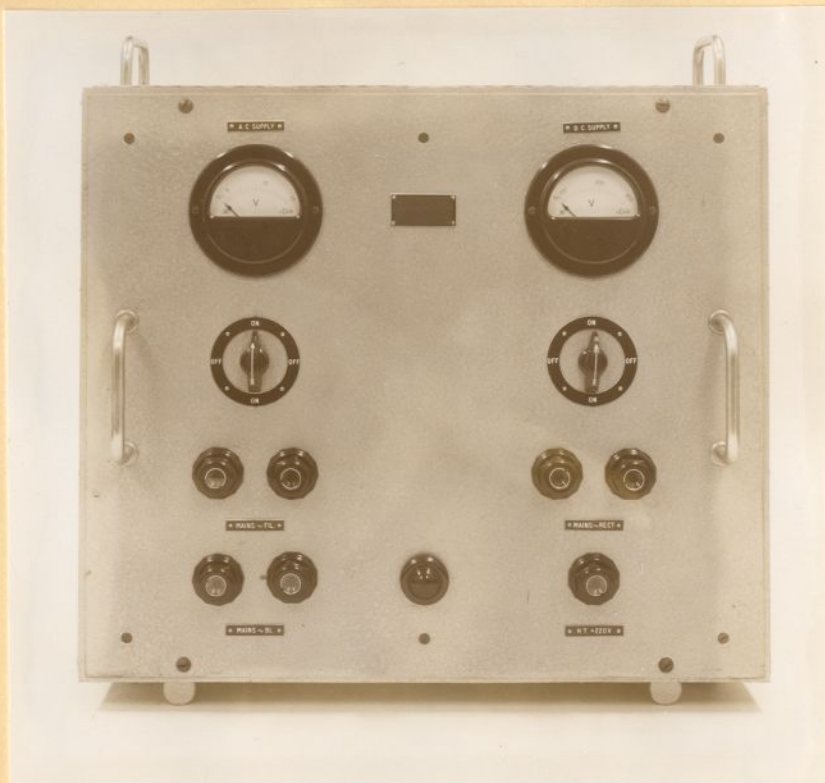
"Ecolex I Philips Usfa"
no. de type Us 8000.

Pour tous renseignements supplémentaires
s'adresser exclusivement et directement à la
"Philips Usfa N.V."
Schouwbroekseweg 49,
EINDHOVEN.
Pays Bas.

TRES SECRET



Poste crypto graphique comprenant "Ecolex I Philips Usfa" numéro de type Us 8000, avec émetteur pas à pas et téléimprimeur.



Appareil d'alimentation
"Ecolex I Philips Usfa",
no. de type Us 8000.

Appareil pour chiffrer et déchiffrer

"Ecolex I Philips Usfa", Numéro de type Us 8000.

1. Description générale.

L'appareil "Ecolex I" a été conçu par les Laboratoires du Gouvernement des Pays-Bas et est en production dans les usines de la "Philips Usfa N.V." à Eindhoven.

"L'Ecolex I Philips Usfa", numéro de type Us 8000 est un appareil cryptographique qui est utilisé en combinaison avec un émetteur pas à pas légèrement modifié et avec un téléimprimeur normal. L'appareil est capable par moyens électroniques de faire le chiffage et le déchiffage en utilisant les 26 caractères de l'alphabet et à la vitesse normale d'un téléimprimeur de 400 caractères par minute, alors que l'émission et la réception directes peuvent se faire en même temps par l'intermédiaire d'une ligne de téléimprimeur normale. Il a été considéré comme important de trouver un moyen pour établir une liaison cryptographique entre deux correspondants de telle façon que d'un côté le chiffage et le déchiffage puissent être effectués électroniquement, tandis que de l'autre côté ce travail puisse être également fait électroniquement mais aussi à la main, si on le désire.

Pour cela il fallait se limiter à l'usage des 26 caractères de l'alphabet dans le texte chiffré vu que sinon les cryptogrammes ne pourraient pas être transmis par les services du télégraphe publics et par le système Morse.

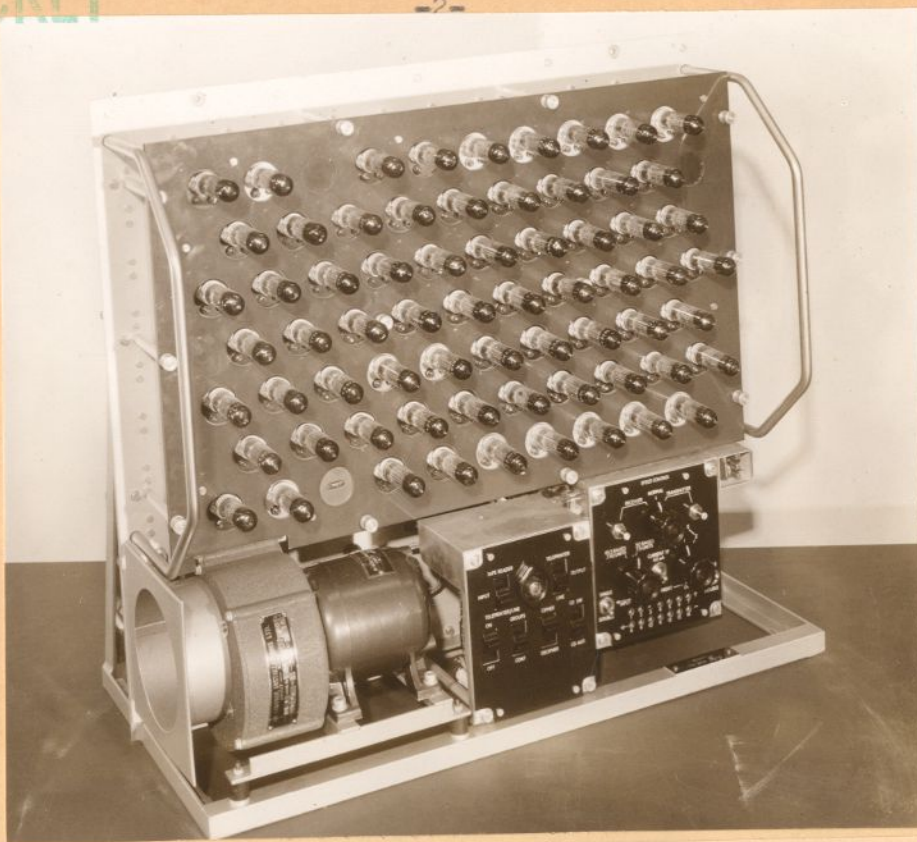
On obtient également qu'un bureau qui ne s'occupe que de quelques messages n'est pas forcé d'acheter un appareil cher et compliqué.

L'Ecolex I (Electronique, Code, TéLEX) qui opère sur un système de 26 caractères, à l'aide d'une clef cryptographique peut chiffrer du texte en clair et d'autre part déchiffrer des cryptogrammes en utilisant la même clef.

L'Ecolex Philips Usfa, numéro de type Us 8000 peut être utilisé tant "on line" que "off-line". Dans les deux cas on se sert d'un téléimprimeur normal.

Parce qu'il est nécessaire d'effectuer le chiffage de "l'espace"

TRES SECRET



"Ecolex I Philips Usfa" numéro de type Us 8000,
intérieur (du côté avant) avec tableau de commande.

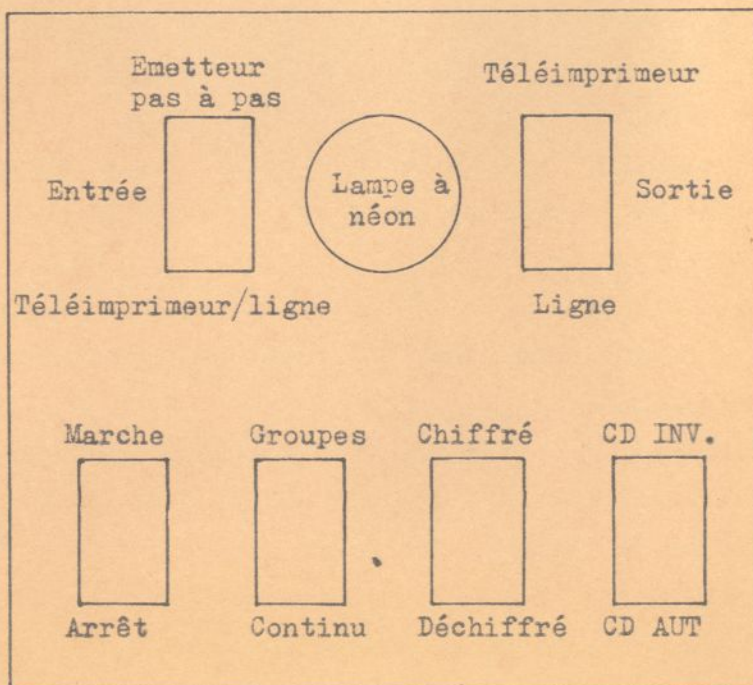


Fig.1.

Tableau de commande extérieur de l' "Ecolex I Philips Usfa"
numéro de type Us 8000.

du texte en clair, on peut remplacer le K (pour le français, l'italien, l'espagnol), le X (pour le néerlandais), et le Z (pour l'anglais) par le signal "espace". Par conséquent le message en clair peut contenir 25 caractères de l'alphabet et le signal "espace". Le chiffrage peut être effectué "en groupes" aussi bien qu'en séries continues; dans le premier cas la forme extérieure du cryptogramme est déterminée par la configuration de la clef cryptographique. Si, par exemple "une bande une fois" est utilisée avec 10 groupes de 5 caractères sur une ligne et avec un espace de deux lignes entre les lignes, le texte chiffré se présentera sous la même forme.

2. Construction.

Un châssis vertical porte un tableau de montage sur lequel sont fixées des unités "plug-in". En arrière du tableau sont fixées des boîtes qui contiennent les diodes. Un panneau en pertinax situé devant le tableau de montage et parallèle à celui-ci, maintient les unités "plug-in" en place. Les tubes électroniques des unités sont situés sur le côté avant du panneau en pertinax. Une boîte métallique enveloppe la combinaison. L'espace compris à l'intérieur de cette coiffe est divisé en trois compartiments par le tableau de montage et le panneau en pertinax.

Une circulation d'air dans le compartiment de milieu, produite par un ventilateur, empêche que se crée une trop grande élévation de température.

La face de la coiffe est constituée par une porte qui peut être fermée par deux serrures et derrière laquelle se trouve le tableau de commande.

La porte a une ouverture pour les 6 commutateurs de commande et une lampe à néon, qui fonctionne quand l'appareil est sous tension (fig. 1). Les autres commutateurs qui se trouvent sur le 2ème tableau de commande ne peuvent être manipulés que si la porte est ouverte. Pour cette raison, le personnel non-autorisé est dans l'impossibilité de modifier le réglage. Les câbles qui relient l'Ecolex I à l'appareil d'alimentation,

TRES SECRET

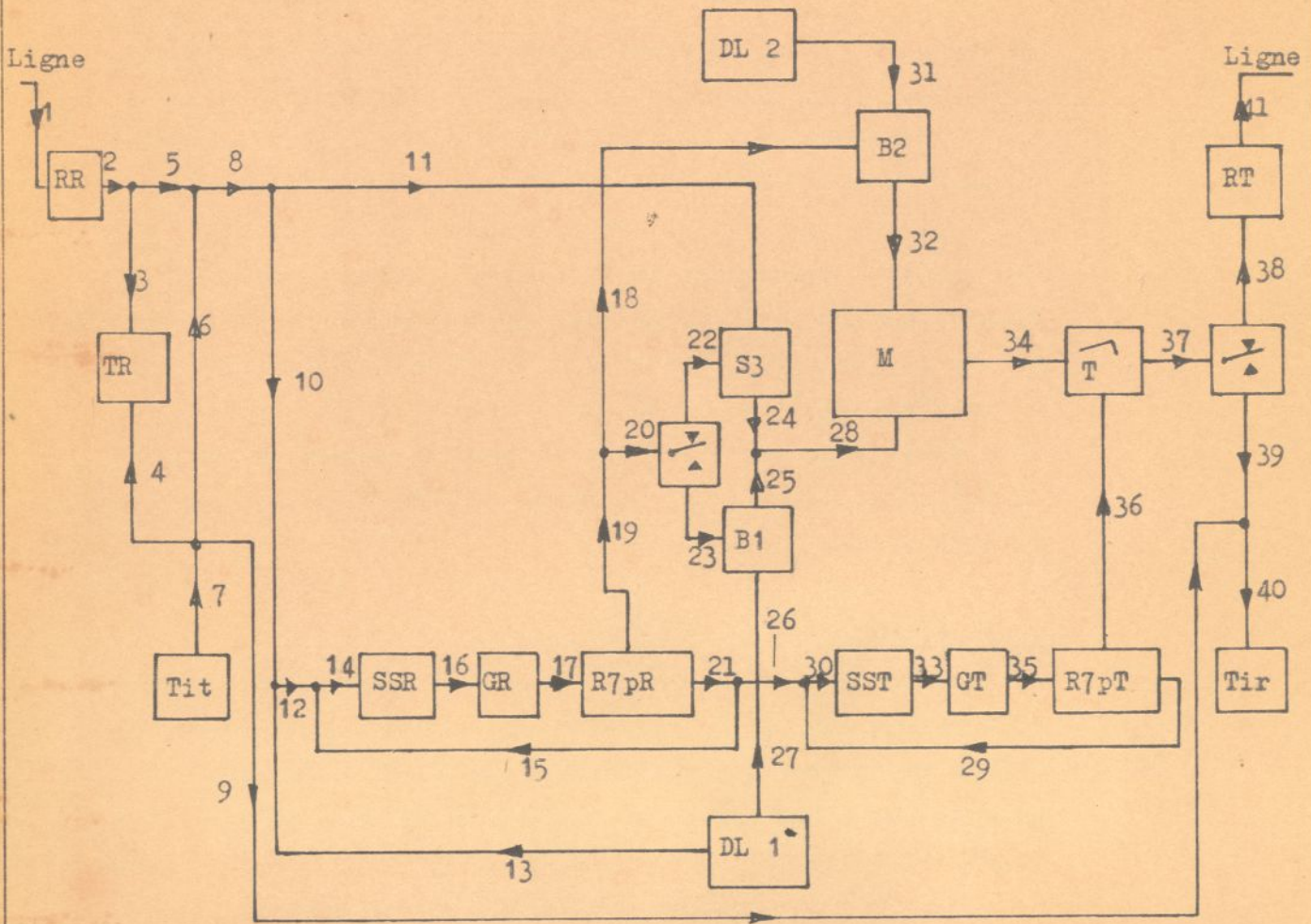


Fig.2.

Schéma synoptique de l' "Ecolex I Philips Usfa" No.de type Us 8000.

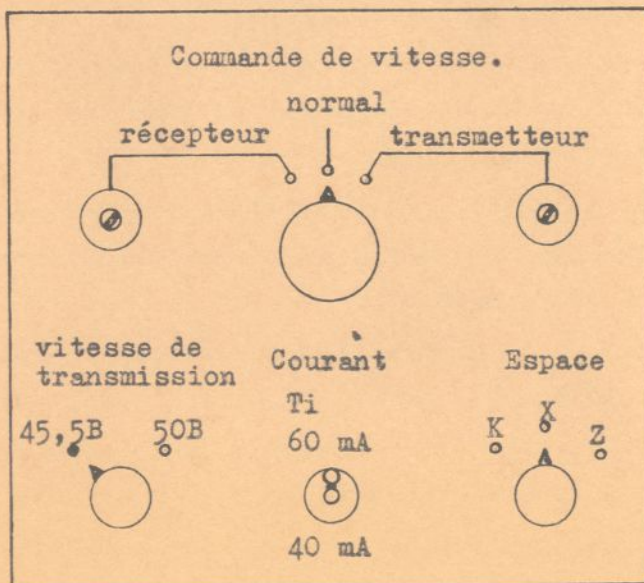


Fig.3.

Tableau de commande intérieur de l' "Ecolex I Philips Usfa", no. de type Us 8000.

au téléimprimeur et à l'émetteur pas à pas sortent de l'Ecolex en arrière.

Les dimensions (hauteur x largeur x profondeur) sont :

625 x 665 x 325 (mm) (Ecolex I proprement dit)

530 x 535 x 415 (mm) (appareil d'alimentation)

Le poids de l'Ecolex I est de 60 kg environ, celui de l'appareil d'alimentation de 86,5 kg environ.

3. Installation électrique.

La figure 2 donne le schéma synoptique.

L'Ecolex I contient 68 unités "plug-in", 67 doubles triodes et environ 600 diodes.

Il y a encore quelques relais ayant des fonctions secondaires. L'appareil contient aussi un relais thermique qui coupe l'alimentation en cas de surchauffage.

"L'Ecolex I Philips Usfa", numéro de type Us 8000 peut être utilisé sur des réseaux de courant alternatif de 110, 127 et de 220 volts, 50 ou 60 p/s.

La vitesse de transmission peut être soit de 45,5 ou de 50 bauds. Des téléimprimeurs à courant de 40 ou de 60 milliampères peuvent être utilisés. La consommation d'énergie de l'Ecolex I est de 400 watts environ, celle de l'émetteur pas à pas de 20 watts environ.

Variation tolérée de la tension du réseau : (-20%, + 10%).

4. Opération et fonctionnement.

On peut choisir le mode d'opération de l'appareil au moyen des 6 commutateurs accessibles (fig. 1). Le premier commutateur placé sur la rangée supérieure ("Entrée") est mis dans l'une ou l'autre position suivant que le texte provient de l'émetteur pas à pas, du clavier du téléimprimeur ou de la ligne.

Par le commutateur "Sortie" le texte chiffré peut être transmis soit au téléimprimeur soit à la ligne.

Le commutateur "marche-arrêt" est le premier de la rangée inférieure (à gauche). Le second commutateur détermine si le chiffrage ou le déchiffrage auront lieu "en groupes" ou "en continu". Le troisième commutateur fait la distinction entre chiffrage et déchiffrage.

Si l'on se sert d'une "bande une fois" continue, au moyen du commutateur situé le plus à droite, on peut déterminer si l'inversion de "chiffrage" à "déchiffrage" et inversement aura lieu automatiquement ou non.

Un des commutateurs enfermés dans l'appareil permet de choisir l'une des vitesses de transmission : 45,5 ou 50 bauds, dépendant du type de téléimprimeur utilisé. Cette vitesse peut être contrôlée au moyen d'un tube à néon et d'un diapason standard fourni avec l'appareil.

On peut ajuster la vitesse de la partie réceptrice lorsque le commutateur supérieur au milieu se trouve dans la position gauche (Cf. fig. 3); au contraire lorsque le commutateur se trouve dans la position droite, on peut mettre au point la vitesse de la partie transmettrice. On réalise l'adaptation de l'appareil à un courant de téléimprimeur de 40 ou de 60 milliampères par le commutateur du milieu. Au moyen du commutateur situé le plus à droite sur la rangée inférieure les caractères K, X ou Z peuvent être remplacés par "espace".

- a. Pour chiffrage d'un texte en clair au moyen "d'une bande une fois" en groupes. Le texte en clair est mis sur le dispositif de lecture DL1, la "bande une fois" sur le dispositif de lecture DL2. Un circuit "start-stop", SSR, est démarré par l'émetteur pas à pas DL1 en passant par 13, 12, 14, SSR et par 16; il fait démarrer à son tour le générateur GR qui commande un répartiteur à 7 pas (R7pR). Celui-ci, par 21 - 15, fait que le circuit "SSR", arrête le générateur après la transmission d'un seul symbole. Il y a deux circuits de balayage, B1 et B2, pour les deux dispositifs de lecture DL1 et DL2. B1 et B2 sont commandés par R7pR en passant par 19, 20, 23 (B1) et par 19, 18 (B2). Les 5 éléments du symbole en clair et ceux de la clef sont transmis en même temps au circuit mélangeur M, (par 25 et 28 respectivement par 32). Par M les deux symboles sont traduits en un symbole chiffré. Les 5 éléments du symbole chiffré sont transmis simultanément au circuit T qui les place en séquence de temps et y ajoute un élément de "start" et un élément de "stop".

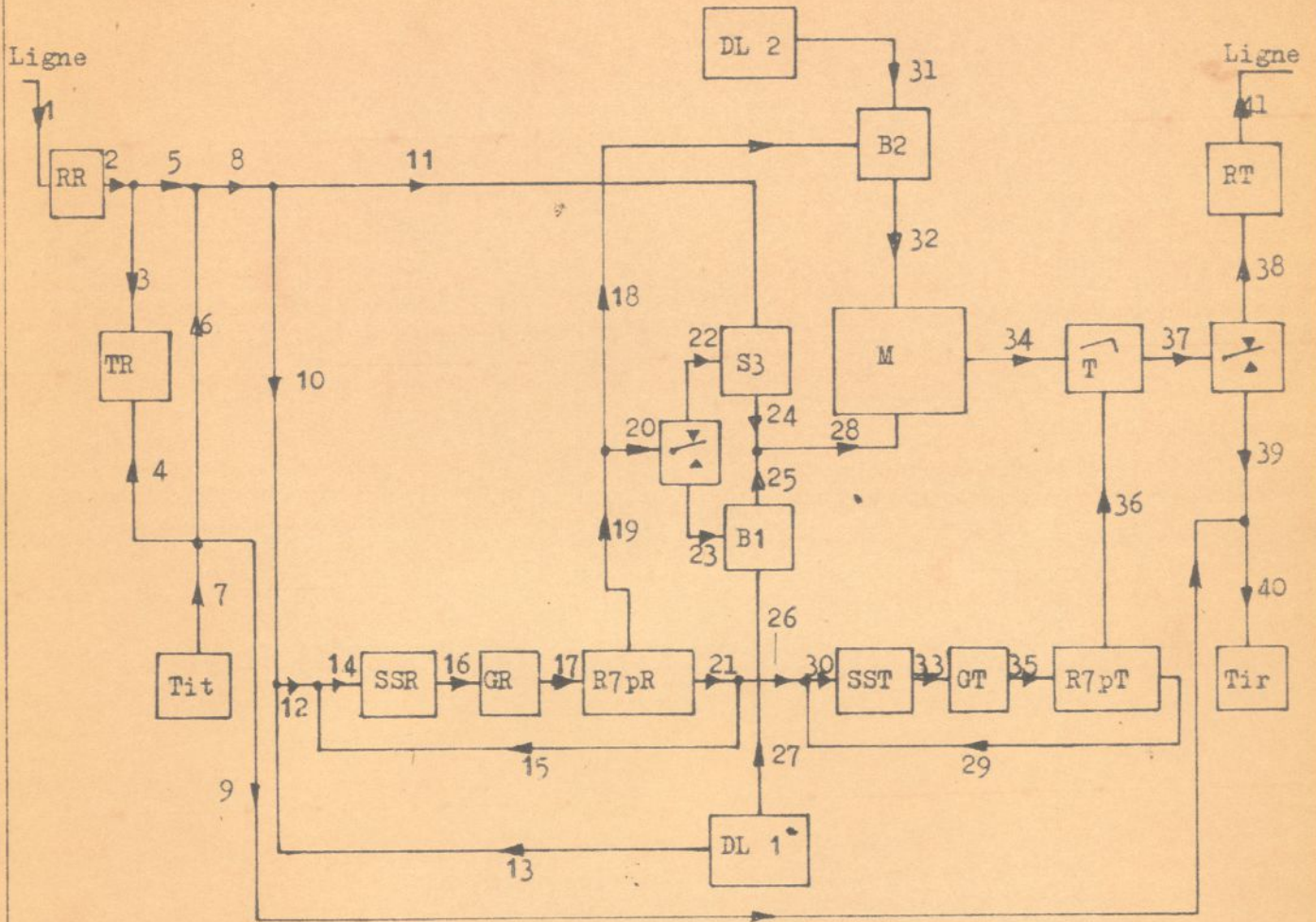


Fig. 2.

Schéma synoptique de l' "Ecolex I Philips Usfa" No. de type Us 8000.

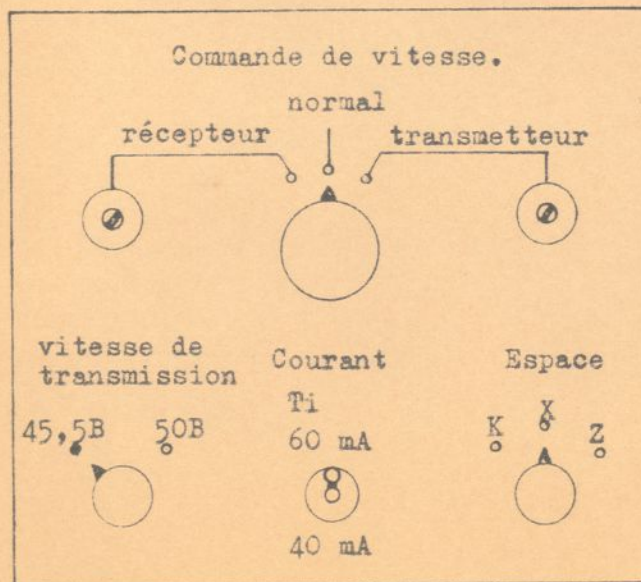


Fig. 3.

Tableau de commande intérieure de l' "Ecolex I Philips Usfa", no. de type Us 8000.

TRES SECRET

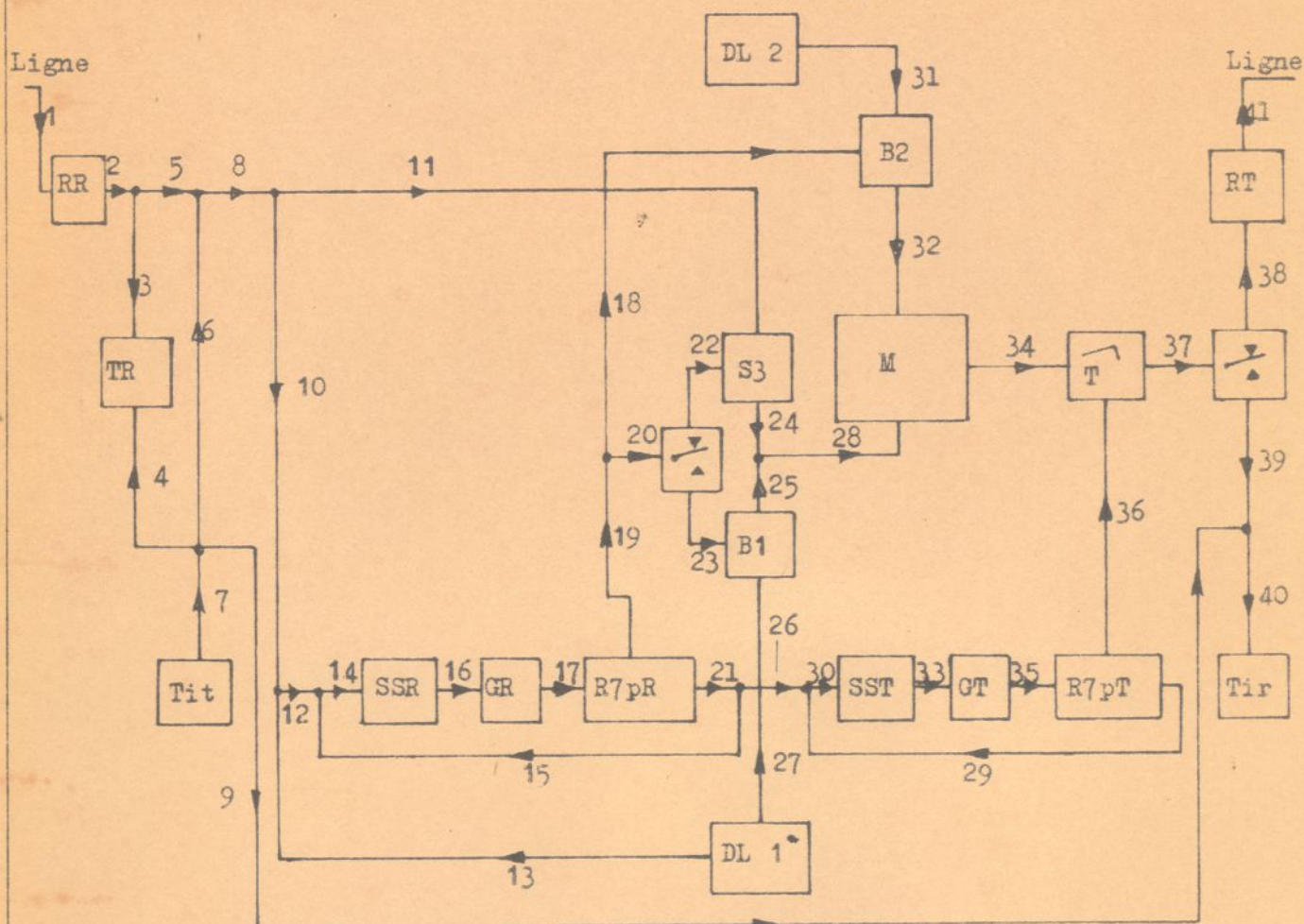


Fig. 2.

Schéma synoptique de l' "Ecolex I Philips Usfa" No. de type Us 8000.

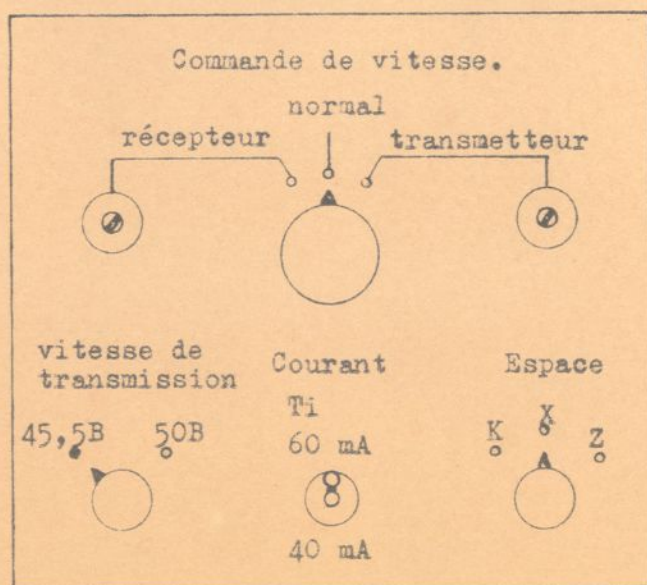


Fig. 3.

Tableau de commande intérieure de l' "Ecolex I Philips Usfa", no. de type Us 8000.

T est commandé par un second répartiteur à 7 pas (R7pT), à son tour commandé par le premier répartiteur (R7pR) en passant par 21, 26, 30, le dispositif "start-stop" (SST), 33, le générateur GT et par 35.

R7pT permet de nouveau que le dispositif "start-stop" fasse arrêter le générateur lorsque le cycle est terminé (par 29).

Le signal est conduit au relais de transmission RT par 37 et 38 si le texte chiffré doit être transmis par la ligne, et par 37, 39, 40 au récepteur Tir du téléimprimeur du poste si l'on veut chiffrer sur place. Dans le dernier cas le texte chiffré peut être imprimé sur feuille, ou enregistré sur bande et/ou perforé dans la bande.

Un préambule et un post-scriptum en clair peuvent dans ce cas être ajoutés au message en se servant du clavier Tit du téléimprimeur du poste. Les caractères tapés sur ce clavier sont délivrés au récepteur par l'intermédiaire de 7, 9, 40.

Le texte chiffré prend la forme de la clef; blocs de 10 lignes par exemple, chaque ligne se composant de 10 groupes de 5 caractères.

b. Pour déchiffrer un texte chiffré en groupes,

le texte chiffré est mis sur le dispositif de lecture DL1 si le texte chiffré est disponible sur bande perforée. La "bande une fois" est mise de nouveau sur TR2. De la même façon que sous a) les signaux sont transmis au circuit-mélangeur M, le texte déchiffré est mis en séquence de temps par T (en passant par 34) et transmis au récepteur du téléimprimeur Tir par 37, 39, 40.

Evidemment il est impossible que les signaux du texte déchiffré arrivent au relais de transmission par 38. Le texte déchiffré a le même nombre de caractères par ligne que la clef utilisée.

On peut réaliser en même temps la réception directe du texte chiffré provenant de la ligne ainsi que le déchiffrement. Dans ce cas les éléments de signal arrivent en séquence de temps de la ligne 1, par le relais de réception RR et par les connexions 2, 5, 8, 10, 12 et 14; ils sont transmis au dispositif "start-stop", SSR, qui provoque le démarrage

TRES SECRET

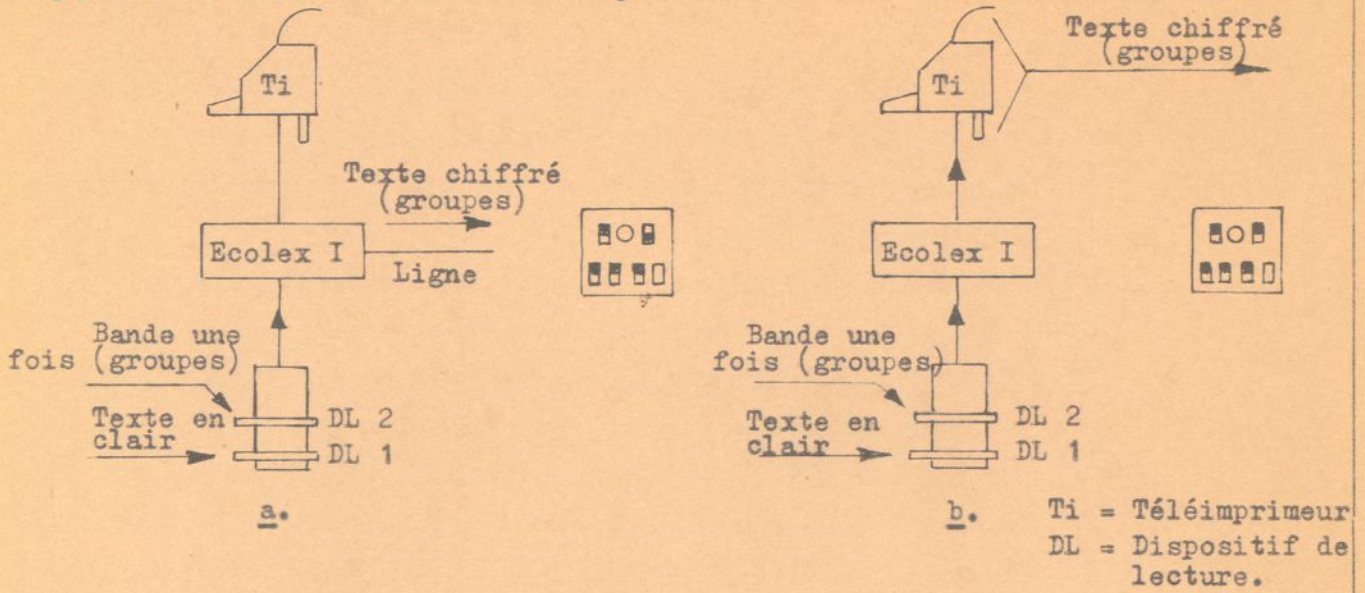


Fig.4. Chiffrage au moyen d'une bande une fois en groupes.

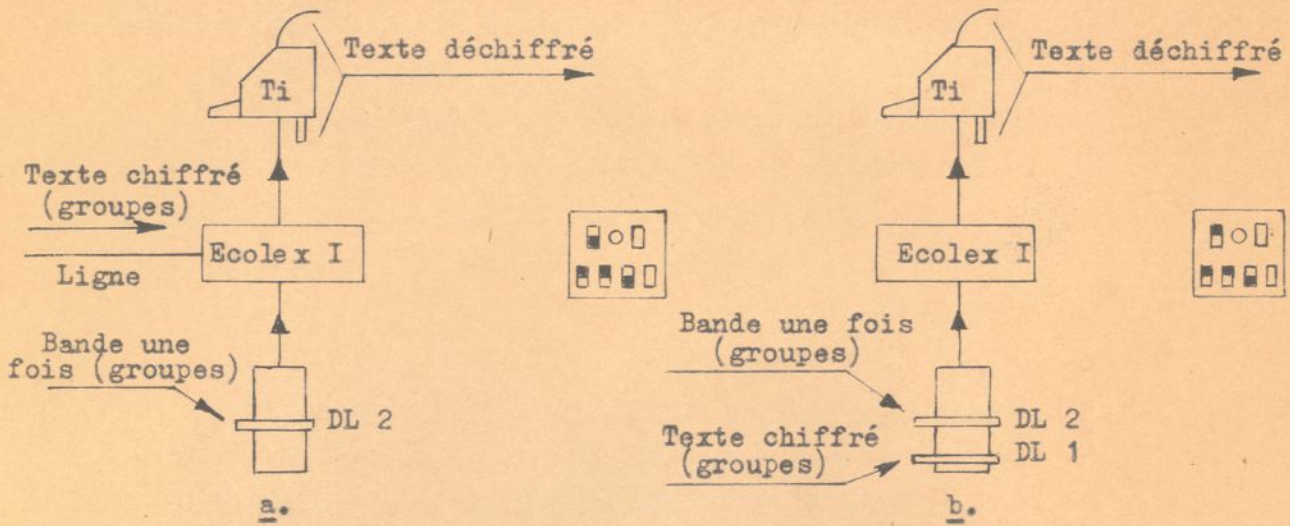


Fig.5. Déchiffrage de texte chiffré "en groupes".

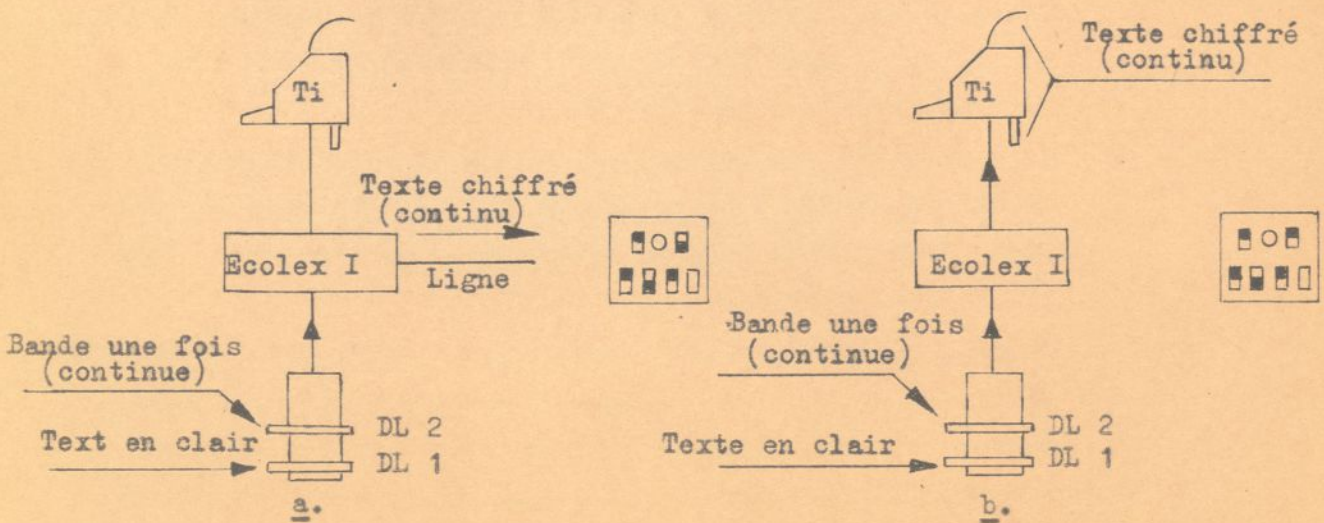


Fig.6. Chiffrage au moyen de bande une fois continue.

du générateur GR et du cycle du répartiteur à 7 pas, R7pR. D'autre part les éléments de signal arrivent par 2, 5, 8, 11 au "balayeur" S3 qui est commandé par les impulsions de R7pR en passant par 19, 20, 22. Par 24 et 28, les éléments de signal sont transmis de S3 au circuit mélangeur M. Après quoi l'appareil fonctionne comme décrit ci-dessus.

- c) Le chiffrage et le déchiffrage en utilisant une "bande une fois" continue diffère du précédent en ce que le texte en clair peut aussi, dans ce cas être transmis à partir du clavier du téléimprimeur.

Puis, la forme du texte chiffré correspond alors à celle du texte en clair, en tenant compte du fait que le caractère "espace" a été chiffré. Le texte déchiffré présentera de nouveau la même forme que le texte original en clair.

L'utilisation du clavier donne la possibilité additionnelle d'échanger des messages tandis que l'appareil change automatiquement de réception à transmission et inversement au moyen du dispositif TR, commandé par l'intermédiaire de 1, 2 et de 3 à partir de la ligne et commandé d'autre part par l'intermédiaire de 7 et de 4 par le transmetteur Tit du téléimprimeur du poste.

- d) Sécurité.

D'abord on a pris des mesures qui rendent impossible la transmission d'un texte si une bande à clef ne se trouve pas sur le dispositif de lecture DL2 de l'émetteur pas à pas.

Puis, l'interrupteur thermique coupe le branchement au réseau si la température devient trop élevée pour une raison quelconque.

Les modes d'opération de l'Ecolex I Philips Usfa", type nr. Us 8000 décrits dans ce qui précède sont récapitulés dans les figures 4 - 9:

- a) Le chiffrage de texte en clair au moyen "d'une bande une fois" en "groupes" et la transmission à la ligne du texte chiffré (fig. 4a), respectivement l'impression du texte chiffré sur feuille ou sur bande du téléimprimeur ou la perforation du

TRES SECRET

Philips N.V.

EINDHOVEN

-10-

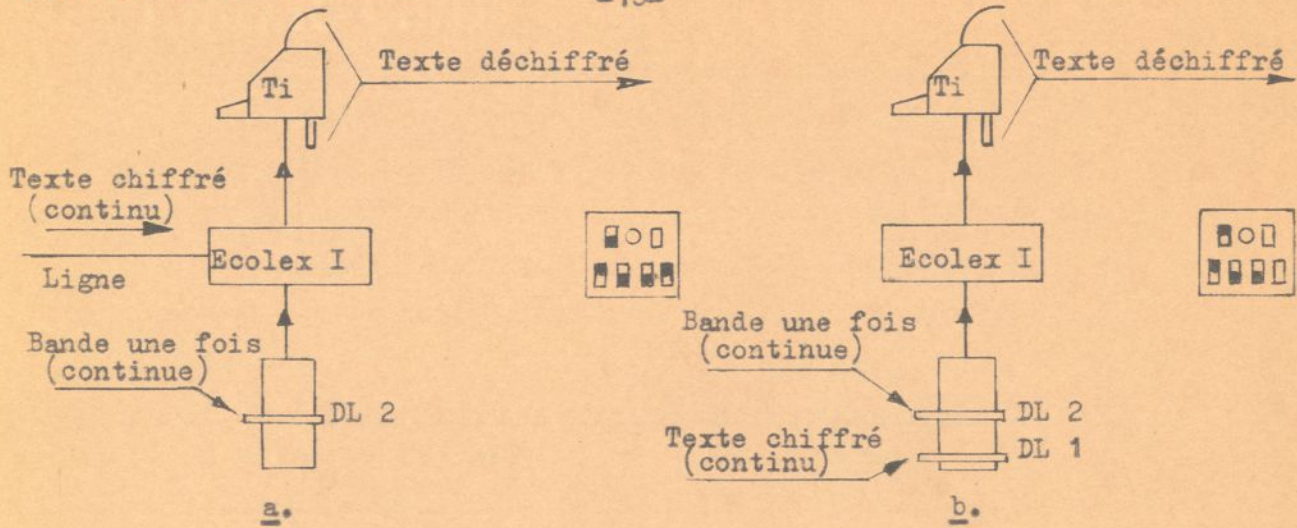


Fig.7. Déchiffrage d'un texte chiffré continu.

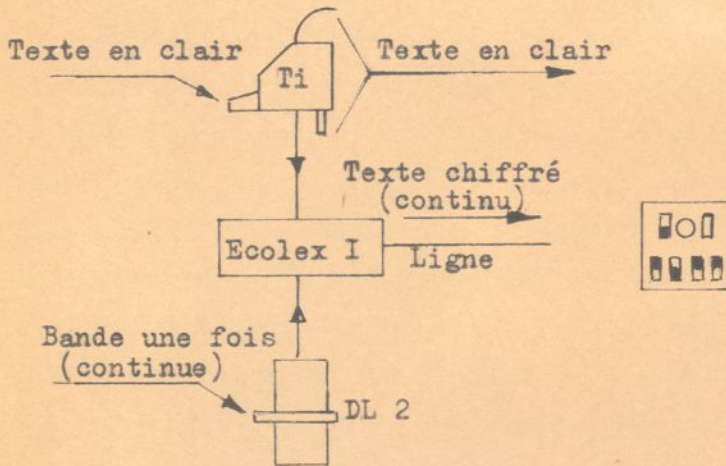


Fig.8. Chiffrage au moyen d'une bande une fois continue, avec utilisation du clavier.

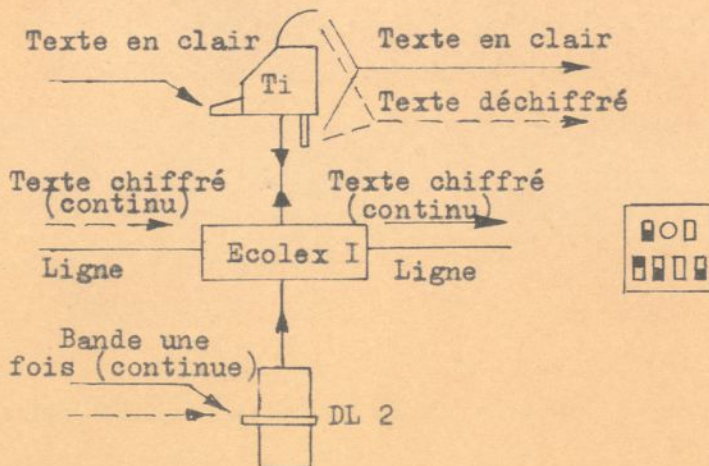


Fig.9. Echange de messages chiffrés. Transmission et réception (en pointillé) montrées par même diagramme.

texte chiffré dans la bande (fig. 4b).

- b) Le déchiffrage de texte chiffré en groupes en cas de réception de ce texte provenant de la ligne (fig. 5a) ou lorsque ce texte se trouve dans une bande perforée (fig. 5b).
- c) Le chiffage avec "une bande une fois" continue et la transmission du texte chiffré à la ligne (fig. 6a) ou bien l'impression du texte chiffré sur feuille ou sur bande du téléimprimeur ou la perforation du texte chiffré dans la bande (fig. 6b); le déchiffrage de texte chiffré en série continue à la réception provenant de la ligne (fig. 7a) et le déchiffrage d'une bande perforée (fig. 7b); le chiffage avec "une bande une fois" continue en utilisant le clavier du téléimprimeur (fig. 8); l'échange de messages chiffrés (fig. 9).

5. Résumé.

"L'Ecolex I Philips Usfa", type no Us 8000 en combinaison avec un émetteur pas à pas et avec un téléimprimeur sert au chiffage et au déchiffrage sur place et aussi à l'application "on line".

Dans les deux cas on emploie les 26 caractères de l'alphabet. La clef cryptographique peut être continue ou "en groupes".

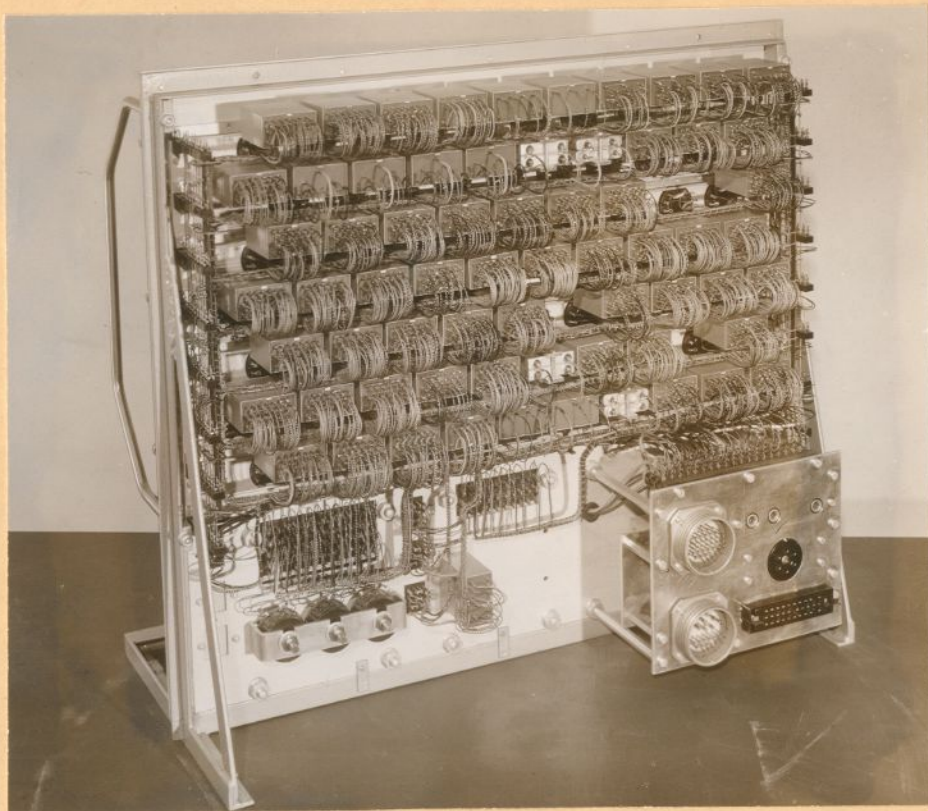
Les caractéristiques suivantes peuvent être mentionnées :

1. Le poids de l'Ecolex I proprement dit est de 60 kg environ, le poids de l'appareil d'alimentation de 86,5 kg environ.
2. Les dimensions de l'Ecolex I proprement dit sont :
625 x 565 x 325 (mm)
les dimensions de l'appareil d'alimentation sont :
530 x 535 x 415 (mm)
3. La consommation d'énergie est de 400 watts environ; la consommation d'énergie de l'émetteur pas à pas accessoire est de 20 watts environ.
4. Utilisable pour courant alternatif de 50 et de 60 p/s, de 110, 127 et de 220 volts.
5. Variation tolérée de la tension du réseau : (-20% + 10%).

TRES SECRET

-12-

6. Adaptable pour courant de téléimprimeur de 40 et de 60 milliampères.
7. Adaptable pour les vitesses de transmission de 45,5 et de 50 bauds par simple inverseur.
8. Le chiffrage peut se faire en utilisant le clavier du téléimprimeur ou en utilisant une bande perforée.
9. Transmission bloquée lorsqu'il n'y a pas de "bande une fois" sur l'émetteur pas à pas.



Intérieur de l' "Ecolex I Philips Usfa" numéro de type Us 8000.