La machine à chiffrer B-211

Jean-François Bouchaudy

B-211 versus Enigma

Depuis le milieu des années 1970, on sait que la machine à chiffrer Enigma a été « cassée » par les alliés. Bletchley Park, le lieu des principaux décryptements est devenu mondialement connu et abrite même un musée sur le sujet.

La plupart des articles concernant l'Enigma mettent l'accent sur l'inviolabilité de celle-ci pour mieux rendre admirables les pays, les personnes et les techniques qui ont permis de la casser.

Dans l'imaginaire collectif, et en partie chez les cryptologues, la deuxième guerre mondiale n'a connu qu'une machine à chiffrer: l'Enigma. Des films comme « U-571 » ou « The Imitation Game » ont renforcé ce sentiment.

À l'époque de la seconde guerre mondiale, la France utilisait au niveau de ses corps d'armée la machine à chiffrer B-211. Cette dernière fut améliorée durant la guerre. Ce modèle offrait une très grande sécurité, qui plus est supérieure à l'Enigma. Ce n'est pas moi qui le dis, ce sont des experts allemands de l'époque ainsi que le célèbre cryptologue français André Muller [20][21].

La B-211 fut utilisée après la guerre par l'armée française comme moyen de chiffrement le plus élevé pendant près de dix ans. Or son histoire et son fonctionnement n'ont jamais fait l'objet de plus d'un paragraphe dans un livre ou dans une revue consacrée à la cryptologie. Ce présent article va essayer, modestement, de combler cette lacune.

Son histoire

La B-21 et l'armée suédoise

En 1925 l'armée suédoise était prête à s'équiper de machines Enigma (le modèle commercial, sans le tableau de connexions). Apprenant cette nouvelle, Boris Hagelin décida de construire la machine B-21 comme alternative à l'Enigma. En moins de six mois un prototype était prêt et la B-21 remporta le marché.

M. Hagelin était membre d'une petite société suédoise fabriquant justement des machines à chiffrer: l'Aktiebolaget Cryptograph. Elle était dirigée par son fondateur, M. Damm. À la mort de ce dernier en 1927, M. Hagelin rachète la société et la rebaptise A.B. Cryptoteknik [12].

Extérieurement, la B-21 ressemble énormément à l'Enigma: quand on frappe sur une touche du clavier, une des lettres du tableau lumineux s'éclaire indiquant la lettre chiffrée ou clair selon le mode utilisé. Par contre, intérieurement, elle est complètement différente car son principe de chiffrement l'est également.

Figure 1 : B-21, l'extérieur

Figure 2: B-21, l'intérieur

La naissance de la B-211

Dans les années trente, M. Hagelin joua le rôle de commis voyageur. Il fit de nombreux voyages à travers le monde pour présenter sa machine B-21. La France fut son principal nouveau client.

L'armée française était très intéressée par cette machine mais demanda des améliorations : la machine devait pouvoir imprimer les messages (le clair ou le cryptogramme) et être transportable. La machine résultante fut baptisée B-211.

La fabrication eut lieu en France près de Paris par une filiale de la société suédoise Ericsson. En 1939, juste avant la guerre, les 500 machines commandées avaient pu être livrées.

La B-211 ne fut pas utilisée uniquement par la France. Elle le fut également par les Pays-Bas et l'Union Soviétique. En effet M. Hagelin fut forcé par les autorités suédoises de vendre une B-211 à l'ambassade russe. Les Soviétiques copièrent la machine et l'appelèrent K-37 Crystal [17]. Jamais les Allemands n'interceptèrent son trafic et pour cause : elle fut utilisée en extrême orient en 1945. Les Américains par contre interceptèrent son trafic et le décryptèrent. Son trafic s'éteignit en 1947.

La machine française B-211 au début de la 2e guerre mondiale

La B-211 fut utilisée au niveau stratégique : armées et corps d'armée. La machine C-36, également fabriquée par Hagelin, était utilisée au niveau tactique (division et en dessous).

À l'époque, le système indicateur de la B-211 (qui protège la clé de message) n'était pas sûr. Qui plus est, la même méthode était utilisée pour indiquer les positions de départ des roues de la C-36 [22].

Durant la drôle de guerre, les Allemands furent incapables de déchiffrer les messages français aussi bien ceux de la B-211 que ceux de la C-36. La qualité cryptographique de ces machines n'était pas en cause. En fait le trafic était trop faible et utilisait majoritairement des lignes terrestres et non la radio.

Après la débâcle, les Allemands purent récupérer des B-211 et après son étude, ils purent élaborer des méthodes leur permettant de déchiffrer les messages qu'ils avaient accumulés [7].

La B-211 équipée du surchiffreur

Au milieu de la guerre (1942-1943), les Français ajoutèrent à la machine un kit conçu par l'A.B. Cryptoteknik afin d'améliorer sa sécurité cryptographique. Cet ajout a dû être prévu dès le début ou tout au moins dans les premières phases de développement de la version française. La guerre empêcha son installation [20].

La sécurité du premier modèle de la B-211 est loin d'être parfaite. Des méthodes manuelles permettent même d'en venir à bout. Inversement, la B-211 équipé du surchiffreur (nom du kit cité plus haut) offre un très haut degré de sécurité pour l'époque et même supérieure à celle de l'Enigma et peut-être même à la machine anglaise TypeX.

Ce second modèle entra en service en 1942 (ou 1943). Ni les Allemands ni les Américains (à l'époque) ne purent casser ce modèle.

La B-211 après la guerre et son retrait du service

Après la guerre, l'armée de terre et l'armée de l'air françaises continuèrent à utiliser la B-211 comme moyen de chiffrement le plus sur. La France commanda même 100 exemplaires de plus pour compenser les machines perdues ou détruites pendant la guerre.

L'intervention franco-britanique en Egypte en 1956 après la nationalisation du canal de Suez par Nasser signa la fin de l'utilisation de la B-211. En effet, les britanniques avertirent leur allié français que cette machine n'était pas sure et qu'ils pensaient que les américains pouvaient la déchiffrer. Du fait de l'accord BRUSA entre la Grande-Bretagne et les USA au lendemain de la seconde guerre mondiale, ces deux nations étaient complètement interconnectées dans la guerre des renseignements liés aux télécommunications (SIGINT). Le GCHQ (l'équivalent britannique de la NSA) était au minimum au courant, au plus partageait les méthodes d'attaques de la B-211 [13].

Après la crise de Suez, la B-211 fut remplacée par la KL-7 de l'OTAN.

Fonctionnement

B-21

Le fractionnement des lettres

La grande originalité de la B-21 par rapport à la plupart des machines de l'époque est le fractionnement des lettres du texte clair au moyen d'un tableau carré 5x5. Ainsi chaque lettre du clair devient un couple de deux entiers chacun ayant cinq valeurs possibles compris entre 0 et 4. Pour faciliter l'utilisation de la machine (notamment sa mise à la clé), ces cinq valeurs sont représentées par deux ensembles de lettres (voyelles, consonnes) ou de chiffres (arabes, romains), l'une pour indiquer les coordonnées horizontales et l'autre les coordonnées verticales. Concrètement, le fractionnement est réalisé par le clavier. Quand on appuie sur une touche du clavier, on ferme deux circuits électriques correspondant respectivement aux coordonnées horizontale et verticale de la touche.

Ensuite chaque composant (ligne, colonne) est chiffré séparément et finalement une recombinaison des deux circuits permet l'illumination de la lettre chiffrée sur le tableau lumineux.

Remarques:

1) Le tableau de fractionnement fait partie intégrante de la construction de la ma-

chine. Il n'est pas configurable. Bien sur, différents modèles de la B-21 (et de la B-211) peuvent posséder des tableaux différents.

2) Le tableau 5x5 ne permet le chiffrement d'un alphabet composé uniquement de 25 lettres. Pour coder la 26e lettre, il faut utiliser une astuce, par exemple coder la lettre W par « V V » (si on omet la lettre W).

Exemple (utilisant le tableau de fractionnement donné par W.F. Friedman [3]):

	L	N	R	S	T
A	L	M	Y	F	X
E	O	J	B	R	S
I	P	U	G	C	W
O	K	N	T	D	Q
U	I	H	V	E	A

Le chiffrement du texte « ATTAQUER » donne la suite de couples (U,T), (O,R), (U,T), (O,T), (I,N), (U,S), (E,S). Une autre façon de présenter le fractionnement est d'indiquer les deux messages résultants : UOOUOIUE (pour la voie horizontale) et TRRTTNSS (pour la voie verticale).

Les demi-rotors

Après le fractionnement des lettres, chaque composante (ligne, colonne) est chiffrée séparément.

Pour chaque voie (ligne ou colonne), le signal passe par un demi-rotor qui réalise une permutation de celui-ci.

L'Enigma chiffre les lettres au moyen de rotors. Un rotor est un commutateur sous forme d'un disque ayant 26 contacts sur chaque face. Le câblage interne qui relie les contacts des deux faces réalise une permutation des 26 lettres de l'alphabet. L'Enigma dispose de plusieurs rotors qui avancent au fur et à mesure du chiffrement et réalisent ainsi des permutations composées et différentes pour chaque lettre saisie. La sécurité de la machine repose en grande partie sur le câblage des rotors qui doit rester secret.

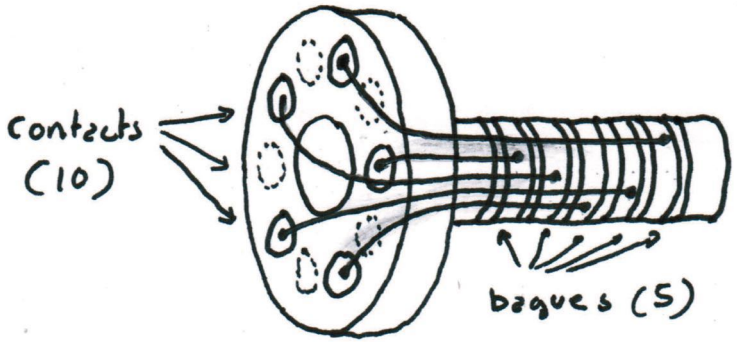

Figure 3 : Un demi-rotor (on n'a représenté que le câblage des contacts pairs).

La B-21 utilise des demi-rotors inventés par Damm. Un demi-rotor est composé d'un tambour comportant sur une face 10 contacts en entrée, chacun repéré par les lettres A, B, C, D, E, F, G, H, I, K (J est omis). En sortie, on dispose de cinq bagues qui sont placées sur l'axe du demi-rotor. En fait, chaque demi-rotor contient deux câblages, le premier associe les contacts impairs A, C, E, G, I aux cinq bagues, le deuxième relie les contacts pairs B, D, F, H, K aux cinq bagues. Ainsi, à chaque position, un seul de ces deux câblages n'est utilisé. À chacune des 10 positions, on obtient une permutation différente.

Exemple : Voici les permutations des demi-rotors (le premier que l'on nommera « voyelle », le deuxième « consonne ») de la B-21 décrite par W.F. Friedman [3] :

```
    AEIOU      LNRST
A   01243      23104
B   32410      34201
C   12304      12043
D   43021      23140
E   23410      01432
F   04132      12034
G   34021      40321
H   10243      01423
I   40132      34210
K   21304      40312
```

Les roues clés

Chaque demi-rotor avance de manière irrégulière grâce à un ensemble de roues clés.

Chaque demi-rotor avance sous le contrôle de deux roues. Chaque roue avance régulièrement d'un pas à chaque lettre tapée. Chaque roue est composée d'un nombre différent de secteurs. Chaque secteur contient un ergot qui dépasse la roue sur la droite ou sur la gauche. Pour la roue de gauche, si l'ergot dépasse sur la droite, il est actif, pour la roue de droite, l'ergot est actif s'il dépasse sur la gauche. En effet les ergots actifs du secteur face au demi-rotor provoquent l'avancement de celui-ci via un petit engrenage situé au milieu des deux roues. Si l'un des deux (ou les deux) ergots est actif lors de la frappe d'une lettre, le demi-rotor avance d'un cran. Si aucun ergot est actif, le demi-rotor reste en position. L'avancement des demi-rotors a lieu avant l'établissement des circuits électriques et donc avant le chiffrement.

- Le demi-rotor de gauche (nommé « voyelle ») avance sous le contrôle de la roue à 23 secteurs et de la roue à 21 secteurs.

- Le demi-rotor de droite (nommé « consonne ») avance sous le contrôle de la roue de 19 secteurs et de la roue à 17 secteurs.

Chaque position d'une roue est identifiée par une lettre :
- La roue 23 possède les positions suivantes : 'ABCDEFGHIKLMNOPQRSTUVXY'
- La roue 21 possède les positions suivantes : 'ABCDEFGHIKLMNOPQRSTUV'
- La roue 19 possède les positions suivantes : 'ABCDEFGHIKLMNOPQRST'
- La roue 17 possède les positions suivantes : 'ABCDEFGHIKLMNOPQR'

Quand les roues 23, 21, 19, 17 sont à la position « A » (clé visible quand le capot est

fermé), les ergots qui agissent sur l'avancement des demi-rotors, sont respectivement GFHG.

La machine possède donc un cycle de 23 x 21 x 19 x 17 = 156009 pas. Au bout de celui-ci, on obtient le même avancement des demi-rotors. Par contre la période de la machine (nombre de pas au bout duquel on obtient la même suite de permutations) peut-être plus élevé, au maximum 10 x 10 x 156009 = 15600900 pas.

Les tableaux de fiches

Après le fractionnement des lettres, chaque composante (ligne, colonne) est chiffrée séparément. Après que chacun des deux signaux soit permuté par un demi-rotor, il est permuté grâce à un tableau de fiches avant que les deux signaux soient regroupés au niveau du tableau lumineux et affiche la lettre chiffrée.

Chaque tableau de fiches est composé de cinq prises dans chacune desquelles on emboîte une des cinq fiches électriques du tableau relié au reste de la machine par un câble. Chaque fiche est identifiée par une lettre (cf. Figure 7).

Chaque tableau de fiches réalise une permutation, mais qui est fixe pour toute la durée du chiffrement contrairement aux permutations générées par les demi-rotors qui peuvent changer à chaque lettre frappée.

- La voie « voyelle » utilise les fiches identifiées par les lettres A, E, I, O, U
- La voie « consonne » utilise les fiches identifiées par les lettres L, N, R, S, T

Si pour le tableau de fiches « voyelle », on a les fiches dans l'ordre AEIOU, on obtient la permutation identité (01234). Si on a les fiches dans l'ordre OEUIA, on a la permutation (31420).

Du fait que les fiches soient reliées à la machine par des câbles suffisamment longs, on peut « croiser » les deux tableaux. Il est ainsi possible de positionner les fiches « voyelles » dans les prises du tableau « consonne » et inversement. Cette possibilité (absente des premiers modèles de la B-21) augmente le nombre de permutations possibles (cf. Figure 6).

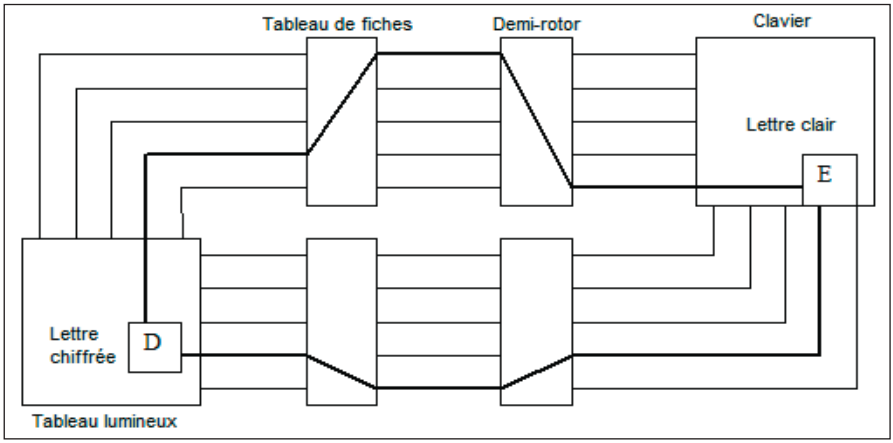

Figure 4: Le chiffrement

Déchiffrement

L'Enigma, via le réflecteur permet un fonctionnement réversible : le chiffrement est identique au déchiffrement (mais avec l'inconvénient qu'une lettre ne peut être chiffrée par elle-même).

On vient de le constater, le chiffrement effectué par la B-21 n'est pas réversible : chaque signal, après le fractionnement est d'abord chiffré par les demi-rotors, le signal électrique entrant par une des bagues et sortant par un des 10 contacts. Ensuite il passe par le tableau de fiches et enfin il aboutit au tableau lumineux.

Le déchiffrement impose d'inverser les circuits : après le fractionnement effectué par le clavier, les signaux doivent passer par les tableaux de fiches (mais via la permutation inverse) et ensuite via les demi-rotors (également via la permutation inverse : on entre par les contacts et on sort par les bagues).

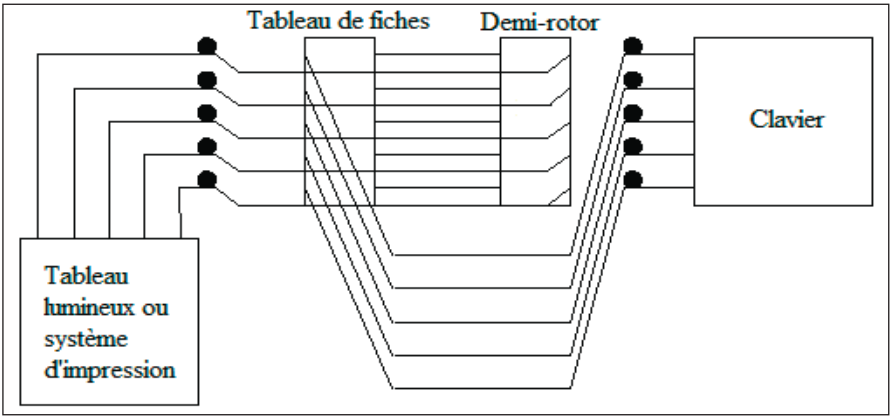

Figure 5 : Le déchiffrement

Pour réaliser l'inversion des circuits on actionne une manette présente sur le côté droit de la machine : En position « C », on travaille en mode « Chiffrement », en position « D », on travaille en mode déchiffrement.

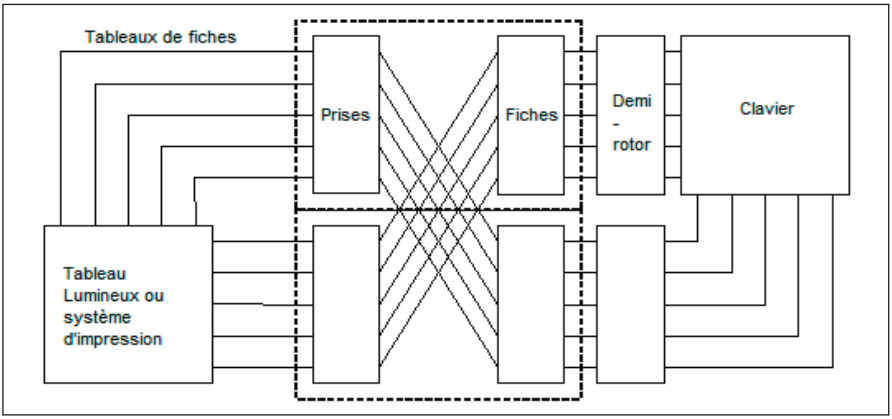

Figure 6 : Le croisement des circuits

La mise à la clé

Il faut d'abord mettre la machine à la clé du jour en se basant sur un tableau de clé distribué à tous les membres d'un même réseau. Ce tableau indique le positionnent des éléments internes de la machine, c'est-à-dire l'arrangement des ergots et la position des fiches. Pour réaliser cette opération, il est nécessaire d'ouvrir le capot de la machine (qui est normalement fermé à clé).

Voici un exemple de clé interne (typiquement valable une journée) :

```
Tableaux de fiches (voyelle, consonne): OEUIA:NTLRS

roue 23 : _B_D_F_H_K___OP___T_V__
roue 21 : A_C_E__HIK_M___QR__U_
roue 19 : _B_D___H_K_MN__Q__T
roue 17 : _BC__F__I_L_N_P__
```

Un ergot représenté par un souligné est inactif. Les ergots des roues 23 et 19 sont actifs quand ils dépassent sur la droite, les ergots des roues 21 et 17 sont actifs quand ils dépassent sur la gauche.

Ensuite, on positionne une nouvelle clé externe pour chaque message envoyé. La clé est composée de six lettres indiquant la position initiale des roues clés et des demi-rotors. La clé externe (appelée également clé de message) doit être transmise au correspondant en même temps que le message chiffré. Il est sage que cette clé soit chiffrée sinon, l'exploitation des clés de messages de plusieurs messages permet de mettre « en phase » les messages et dans le meilleur des cas de déchiffrer les messages (via la méthode d'Auguste Kerckhoffs) sans autre connaissance.

Voici un exemple de clé de message : CELINE. Le demi-rotor de gauche (voyelle) est mis à la position « C », le demi-rotor de droite (consonne) est mis à la position « E » et les quatre roues clés 23, 21, 19, 17 sont respectivement mis en position « L », « I », « N », « E ».

Exemple de chiffrement

Essayons de chiffrer le message « ATTAQUER ». On utilise la clé décrite précédemment.

```
       1 2 3 4 5 6 7 8
23 (L) S T U V X Y A B
       0 1 0 1 0 0 0 1
21 (I) P Q R S T U V A
       0 1 1 0 0 1 0 1
DMV(C) C D E F F G G H    DMV: position du Demi-rotor voyelle
19 (N) B C D E F G H I
       1 0 1 0 0 0 1 0
17 (E) M N O P Q R A B
       0 1 0 1 0 0 0 1
DMC(E) F G H I I I K A    DMC: position du Demi-rotor consonne
Clair  A T T A Q U E R    Le message en clair
voy    U O O U O I U E    Fractionnement voyelle
con    T R R T T N S S    Fractionnement consonne
voyDM  U I E I O A E A    La voie voyelle après le demi-rotor V
```

```
conDM  T S T L L T N L    La voie consonne après le demi-rotor C
voyTF  A U E U I O E O    La voie voyelle après les fiches V
conTF  S R S N N S T N    La voie consonne après les fiches C
Cryto  F V R H U D S N    Le cryptogramme
```

Utilisation

L'utilisation est simple : on met la machine à la clé du jour. Ensuite on positionne la clé de message. Pour ce faire, il faut libérer les roues clés (en mode normal elles actionnent les demi-rotors) en les reculant. On réalise cette opération grâce à une manette présente sur le côté gauche de la machine. En position « R », les roues sont libres et on peut positionner la clé. En position « A » on est en mode opérationnel (pour chiffrer ou déchiffrer). Ensuite on met la machine en mode chiffrement ou déchiffrement via une autre manette (positions « C » ou « D »). Enfin on chiffre le message on tapant chaque lettre du message clair (ou chaque lettre du cryptogramme). Comme avec l'Enigma, on note sur papier la lettre qui s'illumine sur le tableau lumineux.

B-211 (le modèle d'origine)

Le clavier et le système d'impression

La principale différence entre la B-21 et la B-211 sans le surchiffreur est que la B-211 peut imprimer. Non seulement elle peut imprimer les lettres mais également les chiffres et plusieurs caractères spéciaux. Un mécanisme appelé « shift » permet l'impression non pas de 25 mais de 50 caractères (dont l'espace représenté deux fois).

Voici les caractères tel qu'ils apparaissent sur la roue des types :

```
V Q8M7KZB4Y1H2L=C+J5P%D6NW    ?  G"FKZ.U3R9T°S/A0I E-D,X
```

Le clavier comporte 29 touches portant des signes noirs et des signes rouges. Comme pour la B-21, l'appui sur une touche provoque l'activation de deux circuits composés chacun de cinq voies. On n'utilise donc toujours qu'un seul carré de 5x5 = 25. Plusieurs touches ont en effet la même action :

- La touche « Espace » (noire) est équivalente à la touche « K » (rouge)
- La touche « Espace » (rouge) est équivalente à la touche « Q » (noire)
- La touche « Lettres » (rouge) est équivalente à la touche « P » (noire)
- La touche « Chiffres » (noire) est équivalente à la touche « Z » (rouge)

Voici les deux tableaux de fractionnement (signes noirs et signes rouges) :

Signes noirs	1	2	3	4	5
V	R	U	Chiffre	F	G
IV	E	I	A	S	T
III	M	Q	V	X	D
II	L	H	Y	B	Espace
I	N	O	P	J	C

Signes rouges	I	2	3	4	5
V	I	4	Z	7	8
IV	%	5	+	=	2
III	"	Espace	?	W	6
II	° [degré]	9	3	.	K
I	,	-	Lettre	0	/

Voici une description du clavier. Par exemple l'expression (+/A) représente une touche. La partie haute contient le caractère « + » rouge et la partie basse, le caractère « A » noir. Certaines touches n'ont qu'une valeur (haute ou basse)

(/Q) (Z/) (%/E) (1/R) (2/T) (3/Y) (4/U) (5/I) (-/O) (/P)
(+/A) (=/S) (6/D) (7/F) (8/G) (9/H) (0/J) (K/) (°/L)
(chiffres) (/ Esp) (W/X) (/ /C) (?/V) (. / B) (, /N) (« / M) (Lettres) (Esp /)

Les éléments chiffrant

Le demi-rotor de gauche correspond à la voie chiffres arabes et le demi-rotor de droite à la voie chiffres romains.

- Le tableau de fiches de la voie chiffres arabes (coté gauche) utilise les lettres ADEGL.
- Le tableau de fiches de la voie chiffres romains (coté droit) utilise les lettres IORST.

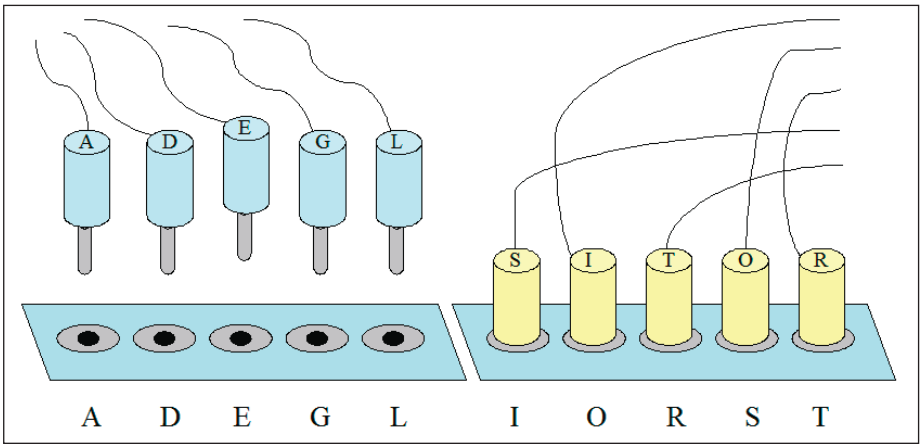

Figure 7: Les deux tableaux de fiches (fiches et prises)

Utilisation de la machine

Mise à la clé (clé du jour et clé de message)

La mise à la clé de la B-211 s'effectue de manière identique à la B-21 : Si l'on veut pouvoir tourner librement les roues clés, il faut reculer celles-ci en mettant la manette 4 (cf. Figure 8) sur la position « 1 ». Après la mise à la clé, on met la manette 4 sur la position « 3 » (ainsi les roues clés vont pouvoir actionner les demi-rotors).

Chiffrement

D'abord, il faut alimenter la machine. On peut utiliser le secteur. Grâce à un rhéostat situé sur le devant, la machine accepte des courants de 80 à 220 volts. Il est possible aussi d'utiliser une batterie qui se branche sur le côté droit grâce à deux plots. Le switch 36 (cf. Figure 8) situé à côté du clavier met la machine sous tension. Enfin, en absence de source électrique, une manivelle (N° 44 sur la Figure 8) permet d'actionner la machine.

Contrairement à la B-21, si l'on veut chiffrer un message, il faut obligatoirement se mettre en mode chiffrement (grâce à la manette 11 en position « C »). En effet le mode chiffrement ou déchiffrement de la B-21 n'est qu'un paramètre de la clé : il est tout à fait possible de chiffrer en mode déchiffrement et inversement de déchiffrer en mode chiffrement. Simplement les circuits sont inversés. Dans le cas de la B-211, du fait de l'impression, le mode chiffrement permet seul l'affichage du cryptogramme sous forme d'une suite de groupes de 5 lettres. Les lettres d'un cryptogramme proviennent essentiellement du jeu des signes noirs, mais les caractères « chiffre » et « espace » sont remplacés respectivement par « Z » et « K ».

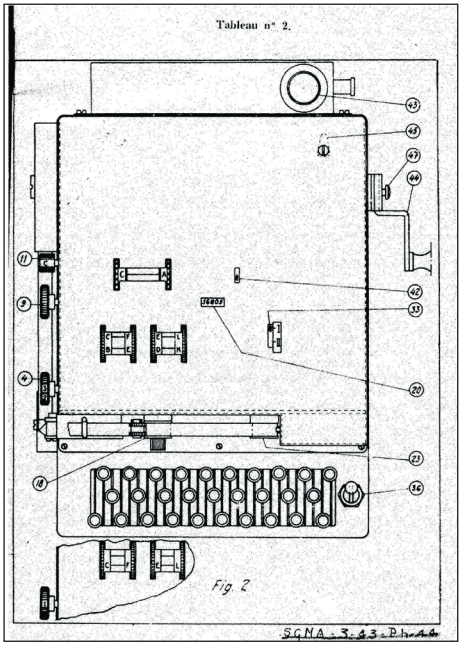

Figure 8 : B-211, l'extérieur

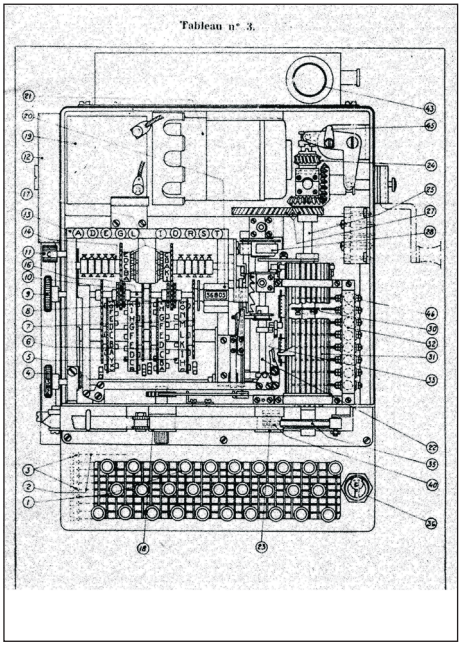

Figure 9 : B-211, l'intérieur

Lors du chiffrement on tape régulièrement les lettres du clair. Si l'on veut saisir des signes rouges, il faut au préalable basculer dans le mode « Chiffre » et inversement si l'on veut saisir ultérieurement des signes noirs, il faut rebasculer dans le mode « Lettre ». L'indicateur 42 sur le capot (cf. Figure 8) indique à l'opérateur dans quel mode il est couramment : « L » pour Lettre (c'est-à-dire signes noirs) ou « C » pour Chiffre (c'est-à-dire signes rouges).

Exemple : Le chiffrement du message « Pertes = 342 tués » s'obtiendra par l'appui des touches suivantes : (P), (E), (R), (T), (E), (S), (chiffre), (espace rouge), (=), (espace rouge), (3), (4), (2), (lettres), (espace noir), (T), (U), (E), (S).

Déchiffrement
On met la machine en mode déchiffrement (grâce à la manette 11 en position « D »). Ensuite on a saisi les lettres du cryptogramme (évidement on ne saisit pas les espaces qui séparent les groupes de 5 lettres). Le texte clair normalement espacé apparaît sur la bande de papier.

Mode « Machine à Écrire »
La B-211 permet également de saisir un texte directement comme si l'on utilisait une machine à écrire. Pour ce faire, on met la machine en mode Opérateur (grâce à la manette 11 en position « O ») et ensuite on saisit un texte en respectant les mêmes consignes que celles décrites pour le mode chiffrement. Par contre, ce n'est pas un texte chiffré qui s'imprime sur la bande de papier mais tout simplement les caractères saisis.

B-211 équipée du surchiffreur

Le surchiffreur

Le modèle d'origine de la B-211 contient un vaste emplacement vers le fond de la machine qui pouvait contenir la batterie. C'est dans cet endroit que le surchiffreur est physiquement placé. Les tableaux de fiches d'origine étant déplacés sur le côté droit de la machine.

D'un point de vue logique, le surchiffreur se place entre les deux tableaux de fiches et le système d'impression.

Le surchiffreur est composé de deux parties, chacune intervenant dans le chiffrement d'une des deux voies (chiffres arabes ou chiffres romains).

Chaque partie est composée de deux rotors et d'un tableau de fiches. On a bien dit « rotor » et non demi-rotor comme la plupart des documents décrivant la B-211 le disent à tort. Chaque rotor comporte sur chacune de ses faces 15 contacts repérés par les lettres ABCDEFGHIKLMNOP. Comme pour les demi-rotors à une position donnée, seuls 5 contacts de chaque face sont accessibles. Du fait qu'il y a quinze positions, il y a en fait trois jeux de câblages : l'un pour les positions A,D,G,K,N un autre pour les positions B,E,H,L,O et un troisième pour C,F,I,M,P. Chacun des câblages permute les contacts d'une face par rapport aux contacts correspondant de l'autre face (comme les rotors de l'Enigma).

Pour chaque voie, le rotor de droite avance de manière synchrone avec le demi-rotor de la voie. Le rotor de gauche avance d'un cran quand le rotor de droite passe de la position « H » à « I ».

Dans le mode chiffrement, le courant, provenant de la sortie d'un tableau de fiches d'origine (ADEGL ou IORST) aboutit à l'entrée du rotor de droite. Il passe ensuite dans le rotor de gauche et finalement dans le tableau de fiches du surchiffreur. Les prises en sortie (en fait qui sont les anciennes sorties du tableau de fiches du premier modèle) aboutissent au système d'impression.

- Le tableau de fiches de la voie chiffres arabes (coté gauche) utilise les lettres BCHKM.
- Le tableau de fiches de la voie chiffres romains (coté droit) utilise les lettres PWXYZ.

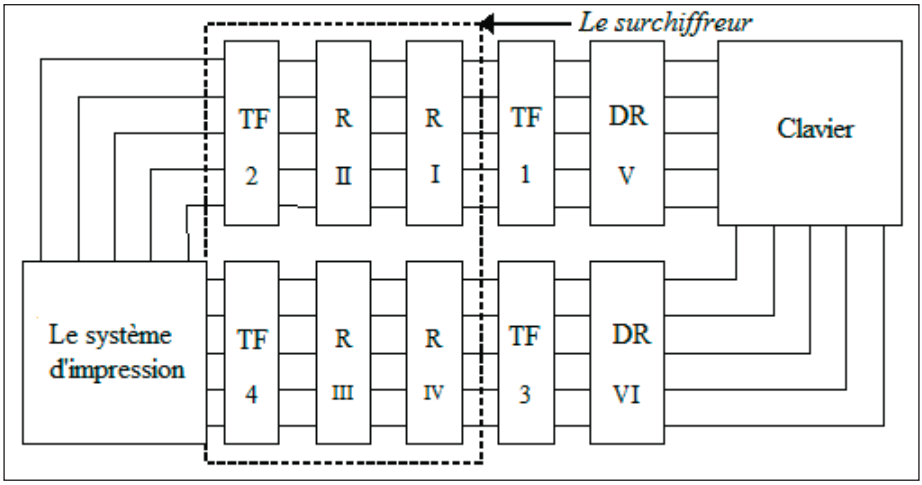

Figure 10: B-211 équipé du surchiffreur
(TF: Tableau de fiches, DR: Demi-rotor, R: Rotor)

Le croisement des circuits

Déjà dans les modèles B-21/B-211, on pouvait au moyen des tableaux de fiches croiser les deux voies de chiffrement. Du fait de l'apparition de deux nouveaux tableaux de fiches, on peut également croiser les deux voies au niveau du surchiffreur ce qui augmente encore l'espace de clés.

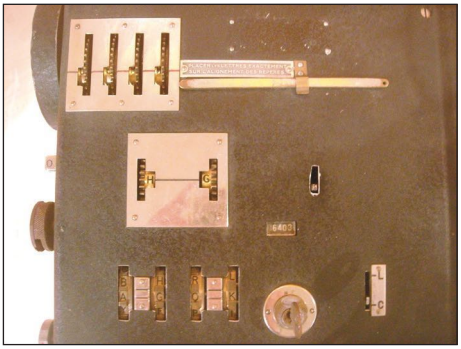

Figure 11: B-211 – Le capot

Figure 12: B-211 – Le clavier

La mise à la clé

La configuration de la clé interne est très similaire à celle du modèle sans surchiffreur: On indique d'abord le positionnement des fiches présentes dans les prises des tableaux d'origine (qui maintenant sont sur le côté droit). ATTENTION! La clé peut préciser un croisement des circuits. Dans ce cas, les fiches de la voie chiffres arabes seront mises dans les prises des chiffres romains et inversement.

On indique ensuite les fiches du surchiffreur (qui sont présentes vers le fond de la machine). Ici également les fiches peuvent être branchées dans les prises de l'autre tableau, ce qui permet de nouveau de croiser les circuits.

Remarque : contrairement à l'Enigma, les rotors ne sont pas amovibles mais fixes.

En ce qui concerne la clé de message, elle est maintenant composée de 10 caractères : La position initiale des 4 rotors, puis la position initiale des 2 demi-rotors et enfin la position initiale des 4 roues clés.

Figure 13 : L'intérieur de la B-211 équipé du surchiffreur

Le mode de compatibilité

Si l'on branche les fiches qui sont à la sortie des demi-rotors sur les prises du surchiffreur, on court-circuite ce dernier. On travaille en mode « compatibilité » avec le premier modèle.

Sur la machine que j'ai inspectée, ce n'était pas directement possible. En effet la gaine qui contenait les câbles des fiches ADEGL et IORST passait dans le fond de la machine pour aboutir près des prises situées sur la partie droite de la machine. Ces dernières étant l'entrée du surchiffreur. Du fait que la gaine était coincée dans le fond, les fiches qui en sortaient avaient un faible degré de liberté. Si la gaine avait été passée par le dessus, les fiches qui la termine pouvaient sans problème atteindre les prises à la sortie du surchiffreur.

Dans l'état, il était toujours possible d'ajouter des rallonges aux câbles (en les branchant à la sortie des fiches) et d'obtenir quand même le mode compatibilité.

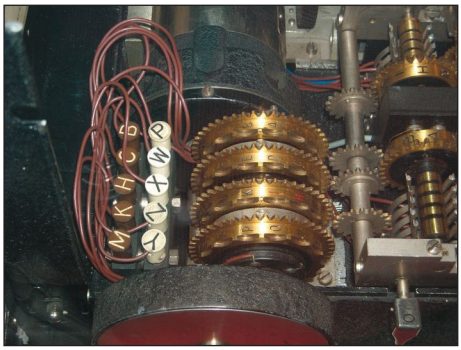

Figure 14: B-211 – Le surchiffreur

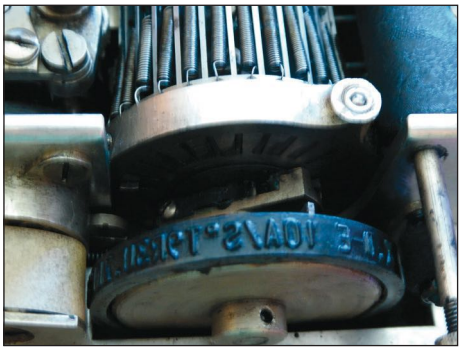

Figure 15: B-211 – La roue des types

Cryptanalyse

Cryptanalyse secrète réalisée par des États

Avant la deuxième guerre mondiale

En 1931, W. F. Friedman, cryptologue en chef de l'armée américaine, demanda à ses assistants, Soloman Kullback, Frank Rowlett, Abraham Sinkov et John Hurt, de concevoir une méthode d'attaque de la B-211. Ils arrivèrent à le faire et la publièrent dans un document nommé « Analysis of the Hagelin Cryptograph Type B-211 » [19]. En 2016, ce document est toujours classifié par la NSA.

En 1954, le FBI arrêta J.S. Petersen, un employé de la NSA. Durant une décennie, il fournit aux Néerlandais des documents secrets et parmi eux, la version de 1939 de l'analyse de la B-211. Les Pays-Bas utilisaient la B-211 (modèle sans surchiffreur) comme le moyen de protection de plus haut niveau de leurs communications diplomatiques.

Durant la deuxième guerre mondiale

Durant la Deuxième Guerre mondiale, les Allemands réussirent à casser la B-211 mais uniquement le premier modèle, sans le surchiffreur.

Les FFL (Les forces françaises libres) fournirent aux Américains pour inspection, une copie du modèle avec le surchiffreur. Par contre, le câblage des rotors était différent de la machine en service. Les Américains approuvèrent la machine pour les échanges de plus haut niveau au sein des FFL. Les cryptologues américains ne purent casser la machine [8].

Après la deuxième guerre mondiale

Après la deuxième guerre mondiale, les Américains (et les Britanniques ?) réussirent à casser le modèle équipé du surchiffreur. Mais pour ce faire ils utilisèrent des machines cryptanalytiques puis des ordinateurs.

Jusque dans les années quarante, la cryptanalyse était réalisée entièrement à la main. Après la deuxième guerre mondiale et jusqu'en 1955, les Américains, à l'image des Britanniques avec leur Bombe et leur Colossus, développèrent des machines cryptanalytiques spécialisées, appelées RAM (Rapid Analytic Machinery). Plusieurs de celles-ci furent développées contre la B-211. Par exemple, la « B-211 SteckerFinder » dédiée à la recherche du câblage des tableaux de fiches. La « Frog » dédiée à la recherche de la clé

de message en se basant sur un crib (mot probable). Ces deux machines (et les autres utilisées contre la B-211) sont toujours classifiées [14].

À partir de 1955, les machines cryptanalytiques spécialisées furent peu à peu remplacées par des programmes informatiques exécutés sur des ordinateurs.

Cryptanalyse publique réalisée par des particuliers

Cryptanalyse de la B-21

C.A. Deavours et L. Kruh dans leur livre « Machine Cryptography and Modern Cryptanlysis » non seulement décrivent le fonctionnement de la B-21 mais aussi ils décrivent un essai de décryptement d'un message en supposant le début connu ainsi que les tableaux de fiches [2].

Dès que je me suis intéressé à la B-211 j'ai communiqué sur le sujet avec George Lasry. George est un développeur de métier qui travaille actuellement chez Google. C'est également un cryptologue amateur qui s'est attaqué à plein de systèmes historiques : L'Enigma, la Lorentz SZ-40, la M-209, l'ADFGVX, la double transposition… Il est l'auteur de plusieurs articles parus dans Cryptologia.

À sa demande j'ai réalisé quelques challenges utilisant la B-211 sans surchiffreur. Très rapidement il a créé un programme permettant de les casser. Au début, en utilisant des Cribs et ensuite en se basant uniquement sur la connaissance de la langue utilisée. Son programme permet de casser y compris des messages très courts de quelques dizaines de lettres. Je ne m'étendrai pas sur les méthodes qu'il a utilisées, elles feront sans doute l'objet d'un futur article.

En tout état de cause on peut conclure que la B-211 sans surchiffreur n'offre aucune sécurité même peut-être moins que la C-36 (un comble !).

Cryptanalyse de la B-211 équipée du surchiffreur

Pour le moment il y en a aucun article publié sur la cryptanalyse de la B-211 équipé du surchiffreur.

G. Lasry pense (pour le moment, mais il continue de chercher), qu'il n'y a pas de faille évidente à exploiter pour « casser » un cryptogramme y compris d'une longueur de plusieurs milliers de caractères. L'attaque par « brute force » étant hors de question. Bien sûr, on suppose connaître le câblage des rotors et des demi-rotors.

Ainsi, l'attaque de la B-211 est soumise à la communauté scientifique. Que le meilleur gagne ! Prochainement je publierai des challenges sur le sujet (comme je l'avais fait pour la machine à chiffrer M-209 [18]).

Références

[1]. Les écritures secrètes, par André Muller, Presses Universitaires de France, 1971. Un chapitre est dédié à la B-211 sans surchiffreur. Le fractionnement du clavier est décrit en détail.

[2]. Machine Cryptography and Modern Cryptanalysis, par Cipher A. Deavours et Louis Kruh, 1985. Cet ouvrage donne un exemple de chiffrement effectué avec la B-21. Le

décryptement d'un message avec le tableau de fiches en position identité est décrit en utilisant un Crib.

[3]. Military Cryptanlytics Part II – Volume 2, par Lambros D. Callimahos et William F. Friedman, From Aegean Park Press. Un exemple de chiffrement utilisant la B-21 est donné.

[4]. Instruction sur le fonctionnement et l'entretien de la Machine à Chiffrer Hagelin Type B-211, N° 125 CH./CAB, 29 mars 1943. Ce document est classifié « Secret ». Malheureusement la présence du surchiffreur est juste évoqué et aucunement décrit. Le document reprend pour l'essentiel la version précédente sans surchiffreur.

[5]. CryptoMuseum – Ce site, géré par Paul Reuvers et Marc Simons, est le plus complet au monde concernant les machines à chiffrer. Une page très complète décrit la Hagelin B-21 : http://cryptomuseum.com/crypto/hagelin/b21/index.htm

[6]. Crypto-Museum. – Une autre page décrit la Hagelin B-211 sans surchiffreur. On peut voir des photos de ce modèle et lire l'histoire du modèle soviétique : http://cryptomuseum.com/crypto/hagelin/b211/index.htm

[7]. TICOM I-58, Interview of Dr. Otto Buggisch. En 1942 il déchiffra le trafic de la B-211 émis en 1939 et 1940. Par contre il fut incapable de décrypter le trafic courant. C'est normal, car la B-211 était alors équipée du surchiffreur. http://cryptomuseum.com/ticom/files/i58.pdf

[8]. Christos Triantafyllopoulos - French Hagelin cipher machines, B-211. Sur cette page on apprend que les Allemands appelaient la B-211 « F-20 » (Französisch N° 20). On y apprend également que ni les Allemands, ni les Américains ne purent lire le trafic généré par le modèle équipé du surchiffreur. http://chris-intel-corner.blogspot.fr/2011/12/french-hagelin-cipher-machines.html

[9]. The Hagelin, B-21 and B-211 John J. G. Savard, Ce site offre des schémas très clair de la B-21. http://www.quadibloc.com/crypto/ro020601.htm

[10]. D'Hagelin à Rita, ARCSI, B-211. On peut voir une photo d'une B-211 sans surchiffreur. Une diapo donne l'architecture de la machine mais contient des erreurs (les tableaux de fiches sont incorrectement placés). https://www.arcsi.fr/colloque-10-10-08/docs/hier-diapo.pdf

[11]. Crypto Machine, Jerry Proc, B-21. http://jproc.ca/crypto/b21.html

[12]. The Story of the Hagelin cryptos, by Boris C. W. Hagelin, Edited by David Kahn, Cryptologia, July 1994. Les mémoires de B. Hagelin peuvent être trouvées également sur le site du Crypto-museum : http://cryptomuseum.com/crypto/hagelin/files/hagelin_story_en.pdf

[13]. L'histoire de la machine Myosotis, Xavier Ameil, Jean-Pierre Vasseur et Gilles Ruggiu. http://www.aconit.org/histoire/colloques/colloque_2004/ruggiu.pdf

[14]. NSA - Cryptanalytic Machines in NSA – 1953. https://www.nsa.gov/news-features/declassified-documents/friedman-documents/assets/files/reports-research/FOLDER_107/41743419078275.pdf

[15]. NSA - Mechanization in support of COMINT Phase II- Ce document classifié « TOP SECRET » (déclassifié en 2013) décrit dans le détail la B-211 équipé du surchiffreur. Ce document m'a permis de vérifier la description que j'avais faite de la machine.
https://www.nsa.gov/news-features/declassified-documents/friedman-documents/assets/files/reports-research/FOLDER_181/41753169079241.pdf

[16]. Dirk Rijmenants - Hagelin B-21 Cipher Machine – Sur ce site, on peut voir les schémas qui accompagnaient les brevets déposés aux USA par Hagelin.
http://users.telenet.be/d.rijmenants/en/b21.htm

[17]. Christos Triantafyllopoulos - The soviet K-37 Cristal cipher machine.
http://chris-intel-corner.blogspot.fr/2012/06/soviet-k-37-crystal-cipher-machine.html

[18]. Challenge M-209, http://www.jfbouch.fr/crypto/challenge/index.html

[19]. The Story of Magic, par Frank B. Rowlett chez Aegean Park Press.1998.

[20]. Report Of Visit To Crypto A.G. (HAGELIN) By William F. Friedman, Special Assistant To The Director, NSA.
https://archive.org/stream/41741409078064/41741409078064_djvu.txt

[21]. TICOM I-206 : Interview of Wilhelm Fenner. Ce cryptologue allemand émet l'avis que la B-211 (équipée du surchiffreur) est supérieure à l'Enigma.
https://archive.org/stream/ticom/TicomI-206#page/n0/mode/2up

[22]. Les bulletins de l'ARCSI. « Essai d'Historique du Chiffre de l'Armée de Terre ». Dans cet article (qui s'étant sur les bulletins de 1975, 1976, 1977, 1986), les moyens de chiffrement, dont la C-36 et la B-211 sont de nombreuses fois évoqués. Le bulletin de 1978 donne des informations sur le système indicateur utilisé conjointement par la B-211 et la C-36 au début de la guerre (39/40).