

09) Générer une configuration secrète.

Pour s'exercer à conditionner notre réplique nous avons utilisé une page de codes ultra secrets montrée en Fig.2 qui précisait l'initialisation d'Énigma pour un mois entier. Bien que la couleur et la présentation sont choisies pour donner l'impression de lire un document historique, il n'en est strictement rien. Cette page respecte avec rigueur la combinatoire réelle en usage à l'époque, mais les données qui y sont indiquées sont générées aléatoirement par un logiciel gratuit tel que **Codebook tool Tool.exe** que l'on trouve sur :

<https://www.ciphermachinesandcryptology.com/en/codebook.htm>

Pour aboutir à une autonomie totale dans l'exploitation de notre chiffreuse, avec la commande **[G]** il sera possible comme avec l'utilitaire mentionné de générer une séquence complète relative à une journée, *avec l'avantage qu'elle sera directement intégrée en initialisation de notre réplique d'Énigma.*

MANIPULATIONS :

- 01) RESET pour repartir sur une configuration commune.
- 02) Touche **Mode** pour revenir au mode **COMMANDE**.
- 03) Cliquer sur **[G]** suivi du **OUI** pour confirmer.

Le programme **P08_EXPLOITER_Enigma.ino** génère une configuration aléatoire complète et ouvre l'affichage qui liste les éléments de cette dernière. Puis, après deux touches quelconques pour sortir de l'affichage, il y a passage automatique en mode **TEXTE**, la LED triple s'illuminant en "blanc". C'est la touche '&' du clavier qui permettra de revenir au mode **COMMANDE**.

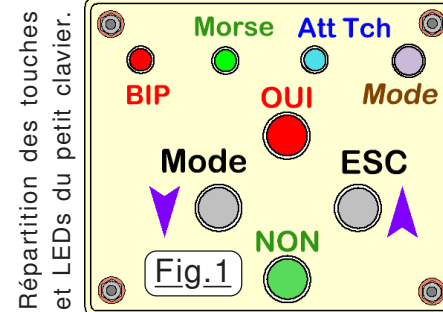
➤ Le code Morse.

Puisqu'il reste encore un peu de place dans ce document, voici le code Morse, ce qui vous permettra de pouvoir facilement vérifier lors des exercices pour lesquels il y a de la télégraphie. Ce petit tableau évitera de chercher sur Internet.

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

UTILISER ÉNIGMA

À la mise sous tension de **P08** ou lors d'un RESET, la machine se trouve en Mode **CRYPTAGE**. Dans cette configuration la LED tricolore *clignote en vert* incitant l'opérateur à *frapper une LETTRE* sur le clavier principal ou sur la touche **Mode** du petit clavier secondaire de la Fig.1 pour revenir en Mode **COMMANDE**. Dans ce mode la LED tricolore *clignote en bleu* incitant l'opérateur à *frapper une LETTRE* sur le clavier principal pour activer l'une des vingt-six fonctions ou options disponibles. La liste des commandes valides est fournie dans les trois **Fiches** non numérotées nommées *Liste des lettres de COMMANDE valides*. C'est la touche **Mode** du clavier secondaire représenté sur la Fig.1 qui permet d'alternier avec le Mode **CRYPTAGE**. Chaque fois que le programme est en attente d'une touche quelconque la petite LED bleue nommée **Att Tch** s'illumine en continu. Dans presque toutes les fonctions et options il y a demande préalable de confirmation. Dans ce cas la petite LED bleue est complétée par la **LED tricolore qui s'allume en rouge**.



Répartition des touches et LEDs du petit clavier.

Seule la touche **OUI** du petit clavier sera considérée comme une approbation. **NON**, **ESC**, **Mode** ou n'importe quelle touche du clavier principal font revenir au mode **COMMANDE** sans effet, la commande étant alors ignorée.

01) INITIALISATION de la machine

Lors d'un redémarrage avec **P08** la machine est automatiquement initialisée avec la dernière sauvegarde qui a été effectué en EEPROM avec la commande **[S]**. Pour changer librement la configuration de la machine on doit procéder en deux étapes. La première consiste à changer la structure du **Brouilleur**. La deuxième sert à modifier l'arrangement sur le tableau des **Fiches croisées**.

Nous allons commencer par l'organisation du **Brouilleur**. Elle se déroule en saisie ordonnée respectivement :

- Du choix du **Rotor** de Gauche, (I à V)
- Du choix du **Rotor** du Centre, (I à V)
- Du choix du **Rotor** de Droite, (I à V)
- De l'indexation Interne du **Rotor** de Gauche, (1 à 24)
- De l'indexation Interne du **Rotor** du Centre, (1 à 24)
- De l'indexation Interne du **Rotor** de Droite, (1 à 24)
- De l'orientation initiale du **Rotor** de Gauche, (A à Z)
- De l'orientation initiale du **Rotor** du Centre, (A à Z)
- De l'orientation initiale du **Rotor** de Droite, (A à Z)
- Du choix du Réflecteur. (B ou C)

➤ Un retour en arrière.

Pour imaginer notre propos, nous allons supposer que nous sommes le 16 février 1942. L'état major a fourni en début de mission le document ultra secret **CODEBOOK-2-1942.txt** de la Fig.2 qui est disponible dans <Documents> et que vous pouvez imprimer si vous le désirez. Il définit les initialisations des

GEHEIM!

SONDER-MASCHINENSCHLUSSEL: FEVRIER 1942

FEBRUAR 42

Tag	UKW	walzenlage				Ringstellung				steckerverbindungen										kenngruppen			
29	C	III	I	II		17	19	15		BG	CT	EM	FQ	HY	IR	KW	NS	PV	UZ	KMP	MQI	TEG	QUL
28	C	I	II	V		23	25	20		BQ	CV	DG	EI	JO	KP	LY	NW	RT	XZ	JEQ	TLV	LNS	PMP
27	B	I	II	V		07	15	21		BQ	DU	ES	FY	HN	IX	JV	KT	MZ	OW	UXG	IVJ	GDC	URC
26	C	III	I	V		24	15	09		AH	BT	CD	GI	JX	KL	NQ	PV	RZ	SU	CSU	RXA	WOA	QST
25	C	III	II	I		08	10	11		AV	CF	DK	EW	GM	IL	NQ	PU	RT	VZ	ZNP	KJU	OJZ	WMY
24	B	III	V	II		04	17	13		AL	CG	DN	ES	HP	IM	OW	RT	UZ	XY	JDH	MEE	ZEA	WEV
23	C	IV	V	II		05	20	09		AZ	BV	CG	EX	FO	HM	IW	KT	LR	PS	OWS	VTP	UVZ	IGN
22	C	V	I	IV		24	26	20		BT	CK	DI	FG	JO	MR	PZ	QY	SU	VW	YTM	STX	KZA	FLF
21	C	V	II	III		10	01	25		AR	BZ	DQ	FT	GI	HW	KP	LY	MV	UX	B5X	JOJ	CXD	HLN
20	B	I	IV	V		20	01	11		BN	CS	DU	EG	FM	HR	KO	LQ	PX	TY	VYX	WHJ	Q8Z	VTF
19	B	V	III	I		19	12	03		AD	BF	CW	EV	GN	IM	KL	QT	RY	SX	QKV	JPS	WTD	ILA
18	C	V	II	I		19	24	03		AL	BI	CG	EK	FN	MQ	OV	PU	SZ	WX	NTH	UAF	FEK	TXK
17	C	III	IV	II		09	16	09		CL	EW	FY	GR	IT	JU	KQ	MO	NX	PV	KMH	EGM	CXN	SGY
16	C	II	IV	III		18	03	02		BE	CK	DF	GT	HJ	IX	MN	OP	UW	VZ	DGL	DIJ	XII	ETO
15	B	I	V	IV		15	21	05		AH	BY	CQ	DK	EL	GZ	MS	NW	OR	UX	JCF	PYY	KKC	FOF
14	B	II	IV	I		13	25	25		BZ	CQ	DP	ET	FG	HI	JK	MW	RV	UY	VFD	MKP	ZAW	HZI
13	B	I	III	V		07	17	26		BT	DJ	EO	FS	GX	HP	KZ	MQ	UY	VW	WNL	HNB	MJX	LKU
12	B	IV	V	III		26	23	07		BJ	CQ	DI	FM	GO	HR	KW	PY	TU	XZ	DLP	IWQ	GWY	OAD
11	C	I	II	V		08	13	11		AM	BX	CT	EV	FY	GO	IN	JP	KQ	WZ	NNF	DID	KRR	ROA
10	C	V	II	I		20	11	02		AF	BY	CX	DO	ET	GL	JU	NZ	RS	VW	RUO	NRI	JSJ	PRQ
09	B	I	IV	III		21	06	13		AM	BO	CU	FX	GY	HV	IP	PQ	SZ	TY	PMF	XHG	RIX	YBB
08	B	V	I	II		26	14	14		DN	EP	FU	GW	HQ	IX	JY	KZ	LV	OW	WWM	QIH	VZM	NLO
07	C	V	II	III		08	23	17		AQ	BU	DF	GL	IZ	JW	KT	MU	NR	PS	TLW	ZSL	FCF	YGX
06	B	II	I	V		10	12	20		BP	CI	EK	FJ	GW	HQ	IX	JY	KZ	LV	BKL	MPN	DJE	HRO
05	C	IV	V	III		17	10	17		DU	EY	FI	HP	JR	KW	MX	NT	OQ	SZ	HWN	VYH	KEA	YYC
04	C	III	II	IV		21	07	06		AH	BQ	DR	EG	FX	IN	JY	LV	OW	SW	JHF	SDA	WKK	IZB
03	B	III	IV	I		08	22	10		CV	DS	EX	FP	GL	IZ	JW	KT	MU	NR	RBO	JNB	JAT	FPJ
02	C	IV	III	II		03	05	04		AJ	BE	CT	FS	GH	IM	KX	LY	NV	PU	RLD	KUQ	CZC	BED
01	C	II	IV	V		14	01	07		AE	CV	DH	FU	GK	IT	LX	MR	OW	SY	KHD	XTE	ONP	YTU

Fig.2

chiffreuses pour tout le mois en cours. Dans ces informations :

- **UKW** désigne le **Réflecteur** à installer sur la machine,

- **Walzenlage** donne les **Rotors** à Gauche, au Centre et à Droite,
- **Ringstellung** fixe les trois indexations internes " " " " " " " ",
- **Steckerverbindungen** indique les dix **Fiches croisées** à installer,
- **Kennguppen** est le groupe de tête qui doit débiter toute transmission dont les **trois premiers caractères** constituent dans l'ordre les **Orientations initiales à imposer aux Rotors** avant chaque cryptage ou décodage d'un message secret.

Pour toute la journée, il faut installer les **Rotors II, IV et III** qui seront en interne Indexés sur les Bagues **18, 3 et 2**, le tout associé au **Réflecteur C**. On devra installer sur le tableau virtuel des dix **Fiches croisées BE CK DF GT HJ IX MN OP UW VZ**. Avant chaque décodage ou chiffage on devra commencer par recaler les trois **Rotors** de gauche à droite avec la lettre **D, G et L** sous la fenêtre.

➤ Choix des Rotors utilisés.

Parmi les cinq éléments disponibles dans le coffret virtuel de notre Énigma, il faut en sélectionner trois. Dans notre exemple, respectivement le **II**, le **IV** et le **III** de la Gauche vers la Droite dans le mécanisme virtuel du **Brouilleur**.

MANIPULATIONS :

- 1) Mettre sous tension notre réplique qui en standard démarre en contexte **CRYPTAGE**. **La LED triple clignote en vert.**
- 2) Cliquer sur la touche **Mode** pour revenir en **COMMANDE**. **La LED triple clignote maintenant en bleu.**
- 3) Cliquer sur [**B**] pour couper le Bruiteur, la petite LED rouge **BIP** s'éteint pour en informer l'opérateur.
- 4) Frapper un [**A**] puis accepter avec **OUI**. On a un message d'erreur mais pas d'avertissement sonore.
- 5) Réitérer [**B**] pour couper rétablir le Bruiteur : **BIP** s'allume.
- 6) Consigner à nouveau [**A**] puis accepter avec **OUI**. Cette fois le bruiteur s'active signalant une erreur de manipulation.

Conclusion : Couper le bruiteur est avantageux pour ne pas polluer l'environnement sonore, c'est important si d'autres personnes partagent le local. Par contre, on perd les alertes d'erreurs qui ne sont pas accompagnés d'une page de texte.

07) Frapper un [D] confirmé par **OUI** pour initialiser la configuration par défaut. C'est celle de l'Énigma de référence décrite dans les **Fiche n°27 à n°32**. (Voir la Fig.1 de la Fiche n°27)

NOTE : Chaque fois que dans ce document il sera allusion à la simulation logicielle de référence, elle sera désignée par [Énigma].

08) Utiliser deux touches quelconques pour sortir des affichages.

09) Cliquer sur [I] et accepter avec **OUI** pour débiter une séquence d'initialisation du **Brouilleur** virtuel.

NOTE : Chaque Rotor est sélectionné par un chiffre. Hors le clavier ne comporte que des lettres. Aussi, pour pouvoir facilement sélectionner les trois éléments à installer sur la machine, on va utiliser arbitrairement [X], [C], [V], [B] et [N] qui ont été choisie pour leur position qui facilite sur la façade l'écriture des inscriptions pour la double signification de ces touches [1], [2], [3], [4] et [5].

10) Frapper respectivement sur [2], sur [4] puis sur [2] : Un BIP d'alerte et un texte adapté nous informe de l'erreur commise alors que la LED tricolore s'illumine en rouge durant une seconde. (Allumage utile si le BIP a été suspendu.)

Comme la vérification ne se fait que lorsque les trois **Rotors** ont été proposés, **la saisie reprend à partir du premier**.

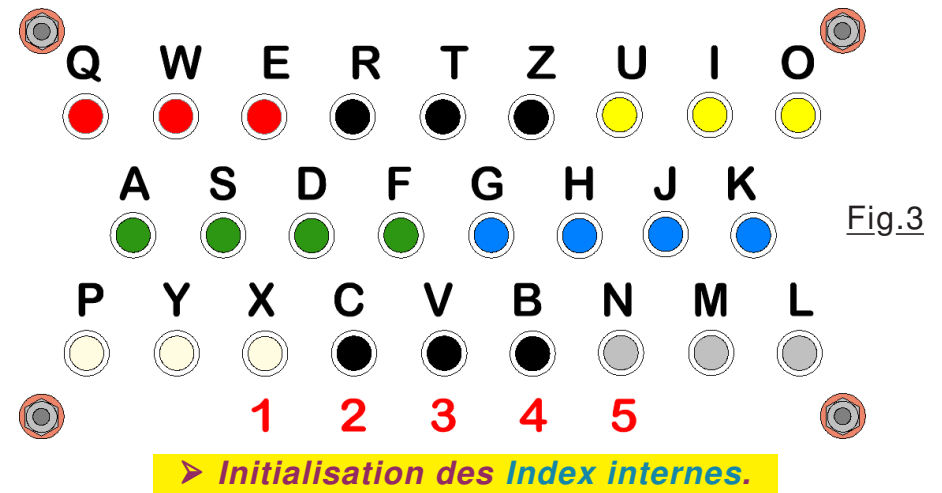
11) Donner les trois valeurs [2], [4] et [1]. (Erreur volontaire.)

12) Vous venez de constater que le dernier **Rotor** n'est pas correct, du coup vous voulez corriger le choix des **Rotors** : Fuir à ce stade de la saisie avec la commande **ESC**.

13) Sortir de l'affichage écran et réitérer [I] suivi de **OUI**.

14) Reprendre entièrement la séquence avec [2], [A], [4], [W] et [3]. Les lettres non valide génèrent un BIT d'alerte et sont ignorées. noter que si le BIP est suspendu, Il ne se passe rien et il n'y a pas de changement d'affichage pour indiquer le **Rotor**.

NOTE : La commande **ESC** fait sortie de la saisie des éléments du **Brouilleur** sans modifier les initialisations de ceux qui ont déjà été saisis. Par exemple, supposons que l'intégralité de l'initialisation a été effectuée et que vous constatiez que l'un des **Rotors** a été mal saisi. Il suffit de reprendre entièrement l'initialisation avec [I] et de fuir avec **ESC** lorsque les trois **Rotors** sont indiqués correctement.



NOTE : Pour préciser l'indexation interne de la Bague, on doit consigner dans l'ordre les nombres 18, 3 et 2. Autant repérer en double les cinq chiffre comme sur la Fig.3 n'encombre pas le clavier, autant doubler les indications sur toutes les touches le rendrait complètement illisible vu le peu de place qui reste. Nous allons donc utiliser l'ordre alphabétique des touches pour leur affecter un nombre. Il suffit de savoir que [A] vaut [1], [B] vaut [2] ... [P] vaut [16] ... [Z] vaut [26]. **Fastoche !** Pour faciliter ce travail de transposition, le tableau de correspondance est fourni avec la commande [C] qui par raison de place disponible sur la page-écran commence avec le chiffre 3.

03-C	04-D	05-E	06-F
07-G	08-H	09-I	10-J
11-K	12-L	13-M	14-N
15-O	16-P	17-Q	18-R
19-S	20-T	21-U	22-V
23-W	24-X	25-Y	26-Z

15) Touche **ESC**, revenir au mode **COMMANDE**, puis tester [C].
 16) Les trois indexages désirés sur les **Rotors** étant 18, 3 et 2, on devra proposer dans l'ordre [R], [C] et [B].

CONCLUSION : Avant de commencer une initialisation du **Brouilleur** avec [I] il sera pertinent en préambule de consulter les correspondances Lettres/Chiffre avec la commande [C].

17) Maintenant que nous avons tous les éléments on peut raisonnablement reprendre l'initialisation de la machine avec la séquence [I] > **OUI** > [2] > [4] > [3] > [R] > [C] et [B].

- 18) Pour les orientations initiales proposer [D], [G] et [L].
- 19) Pour le **Réflecteur** indiquer [A], [X], [O] etc. Tant que l'on utilisera une lettre incorrecte, le logiciel générera un BIP d'alerte et restera en attente d'une réponse correcte. La seule façon de sortir de cette situation (*Mis à part RESET*) consiste à consigner l'une des deux lettres valides [B] ou [C].
- 20) Pour cet exemple imposer [C]. L'écran affiche la configuration prévue pour le 16 février 1942. On peut passer à la suite.
- 21) Frapper une touche quelconque pour revenir au mode commande.

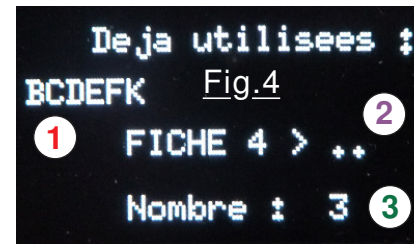
02) Initialisation du tableau des Fiches croisées.

Brancher virtuellement les dix **Fiches croisées** de la journée en cours constitue la deuxième étape fondamentale de l'initialisation de la chiffreuse. Sur la machine réelle, ce n'était pas forcément l'action la plus facile à mener. Pour notre réplique, cette opération est celle pour laquelle on peut le plus se tromper. Aussi, pour la rendre conviviale plusieurs commandes sont prévues et permettent de corriger une erreur sans avoir à tout retaper.

NOTE : Historiquement l'opérateur radio branchait les dix jonctions filaires systématiquement. Ce n'est pas une obligation du tout, on peut parfaitement ne placer que quelques lignes, voir pas du tout. Aussi, la commande [A] n'impose pas un nombre de liaisons, et l'on peut *sortir à tout moment* de la fonction avec *l'une des quatre touches du petit clavier secondaire*.

MANIPULATIONS :

- 01) Frapper [E], **OUI**, puis **ESC** et [X] ou un [A] confirmé par **OUI**.
 - 02) Commencer par **BE > CK > DF** suivi de **NON** par exemple.
- NOTE :** La sortie anticipée de ce type de saisie se fait avec l'une quelconque des quatre touches du petit clavier secondaire. Quelle que soit cette touche, y compris avec **NON** les **Fiches croisées** correctes qui ont été désignées sont validées. Cette fonction ne peut qu'ajouter des lignes à celles déjà présentes.
- 03) Sortir de la page-écran puis reprendre la saisie avec [A] suivi de **OUI**. Noter sur la Fig.4 que les lettres déjà utilisées deviennent interdites. On va volontairement se tromper.



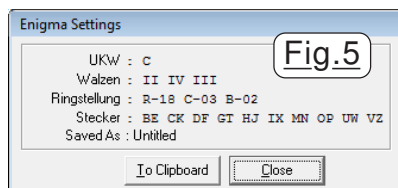
C'est dans la zone **2** que sont affichés les caractères frappés avec en **3** le nombre actuel de fiches. En **1** s'affiche **les lettres actuellement utilisées qui deviennent "interdites"** car on ne peut pas matériellement brancher deux fiches dans la même prise.

BE CK DF GT HJ IX MN OP UW VZ

- 04) Continuer avec **GT > HJ > IE**. Le programme nous avertit de l'erreur et reste sur la **Fiche n°6** en cours de saisie.
 - 05) Frapper l'une des touches du petit clavier pour reprendre la saisie.
 - 06) On devrait fournir IX, mais comme nous sommes étourdis, on clique deux fois sur **X** : Le logiciel surveille et filtre !
 - 07) **ESC** et on termine avec **IX > MN > OR > UW > VZ**. Arrivé à dix **Fiches** le programme quitte automatiquement la fonction.
- On constate à l'affichage du tableau que **Fch 08** est incorrecte. Pour alléger le programme, il n'existe pas de commande pour corriger une fiche. La technique consiste à effacer celle qui est incorrecte, puis à en ajouter une nouvelle qui elle sera exacte.
- 08) Sortir de la page-écran puis lettre [K] confirmé par **OUI**.
 - 09) Avec ▼ et ▲ on incrémente ou on décrémente le numéro de la fiche en permutation circulaire. Cliquer jusqu'à arriver à **08** sachant qu'ici décrémente avec ▼ est plus rapide.
 - 10) À ce stade, seule la touche **OUI** confirmera l'effacement. La fiche **OR** a bien été enlevée, il n'y a plus que neuf jonctions.
 - 11) On complète avec [X] ou [A] confirmé par **OUI**. Puis on fournit les bonnes lettres **O** et **P** cette fois. La sortie du mode est automatique puisque le tableau est saturé.

Peu importe l'ordre dans lequel sont branchés virtuellement les lignes, le chiffrement ne dépend que de leur combinatoire. Toutefois, si l'on désire comparer notre arrangement avec celui d'[Énigma] ce ne sera pas commode car sur cette dernière l'indication du croisement des fiches est ordonné par ordre alphabétique "sur la première lettre". C'est pour pouvoir comparer facilement l'initialisation sur les deux machines que la commande [O] a été ajoutée au **Menu de BASE**.

- 12) Tester **[O]** que l'on doit confirmer avec **OUI**. Je vous invite à ce stade à faire appel aux **Fiches n°27 à n°32** pour initialiser l'**[Énigma]** comme sur notre réplique et comparer les affichages, en particulier celui de la Fig.5 obtenue après avoir configuré la chiffreuse de référence.



REMARQUE : Le logiciel qui fournit des tables de codes telles que celles de la Fig.2 ordonne systématiquement les lignes. Toutefois on peut fort bien n'en installer que quelques-unes et les créer dans le désordre. C'est là que la commande **[O]** sera pertinente.

A chaque journée qui commence, l'opérateur radio doit changer la configuration du tableau des **Fiches croisées**. On se doute qu'il commençait par toutes les débrancher pour ensuite les installer une à une. Nous devons procéder de la même façon. Mais utiliser **[K]** vingt-six fois serait une vraie galère.

- 13) **ESC** pour revenir au mode **Menu de BASE** puis touche **[E]**.
 14) **NON** pour vérifier que l'on peut fuir. Frapper un **[L]** suivi de **ESC** pour s'assurer que rien n'a changé.
 15) **ESC** et on recommence **[E]** mais cette fois on accepte avec **OUI**.
 16) Pas besoin de **[L]** pour prouver que toutes les lignes virtuelles ont été enlevées du tableau, le programme affiche le résultat.
 17) Imposer **[L]** : La commande **[E]** enlève toutes les jonctions électriques virtuelles mais ne modifie pas le **Brouilleur**.

➤ Dernière commande pour initialiser Énigma.

Avec les chapitres précédents, nous avons entièrement configuré la machine pour la journées en cours. Toutefois, chaque fois que l'opérateur désirait envoyer ou recevoir un message, il devait réorienter les **Rotors** à l'aide des molettes spécifiquement prévues à cet effet. Nous aussi, il nous faudra le faire. Mais avoir à reprendre entièrement la commande **[I]** est totalement exclus. C'est pour cette action fréquente que la commande **[F]** a été prévue.

MANIPULATIONS :

- 18) Frapper la touche **Mode** pour passer en **CRYPTAGE**. La LED triple clignote en vert et surtout l'écran affiche **[D][G][L]**.

- 19) Par exemple proposer **[P]**, **[Y]**, **[X]**, **[C]**, **[V]**, **[B]** en regardant à chaque fois le résultat sur l'écran graphique.

On constate que pour simuler l'incrémentation des roues, chaque fois la lettre frappée au clavier s'affiche sur "le compteur" en s'incrémentant alphabétiquement chaque fois d'une position.

- 20) Sortir du **CRYPTAGE** avec **Mode** et y revenir en cliquant une deuxième fois sur cette touche. L'écran affiche toujours le triplet **[D][G][R]** car on continue à utiliser la machine sans la reconfigurer. On ajoute **[T]**, **[Z]** ou toute autre chaîne de caractères. On suppose maintenant qu'il faut transmettre un nouveau message, donc il faut réorienter les trois **Rotors**.
 21) Revenir au **Menu de BASE** avec **Mode** et recalcr le **Brouilleur** en utilisant la commande **[F]**. Accepter avec **OUI**.
 22) Il serait possible avec **[L]** de vérifier que seuls les trois **Rotors** ont été recalés, mais ce n'est pas la peine, passer directement en **CRYPTAGE** avec **Mode**, on retrouve bien le triplet **[D][G][L]**.
 23) Pour la forme proposer **[B]**, **[O]**, **[N]**, **[J]**, **[O]**, **[U]**, **[R]** puis revenir au **Menu de BASE** avec le bouton poussoir **Mode**.

Mise à part la consigne **[P]** nous avons passé en revue toutes les commandes actuellement implémentées. (Ce tutoriel a été rédigé jusqu'ici alors que le développement en était au démonstrateur **P04**.) On va pouvoir passer à la suite de l'exploitation de la machine. Mais avant je propose "d'évacuer" le dernier item possible du **menu** :

- 24) Frapper la commande **[P]** qui nous informe que l'espace disponible entre la **PILE** et le **TAS** est de 310 octets avec **P08**. C'est une information qui ne concerne que les programmeurs, et pour ce qui est de l'usage d'Énigma, on peut somptueusement oublier.

Pour celles et ceux qui désirent toutefois avoir des explications sur le sujet, aller consulter le didacticiel mentionné en début du didacticiel de ce projet que l'on trouve sur :

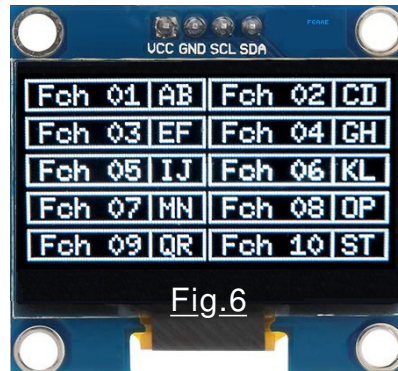
<https://www.robot-maker.com/ouvrages/00-realiser-minuscule-chiffreuse-enigma/>

Les explications relatives au problème sournois de la "collision de pile" sont fournies en Page 66, où tout y est détaillé.

- 25) Avant de continuer "votre formation", je vous propose de reprendre entièrement la configuration de la machine correspondant au 25 février 1942 par exemple.

03) Recharger une initialisation machine.

Pouvoir Sauvegarder ou Recharger une configuration d'initialisation à tout moment est un impératif d'exploitation incontournable pour la qualité opérationnelle de notre réplique. La mémoire non volatile EEPROM de l'ATmega328 est parfaitement adaptée pour agencer ces deux fonctions. Nous allons pour expérimenter ces outils commencer par le rechargement alors que nous n'avons jamais sauvegardé quoi que ce soit. En réalité, lorsque l'on loge les textes de l'interface de dialogue en mémoire EEPROM avec le logiciel P00_Textes_en_EEPROM.ino, on y inscrit aussi une configuration de base cohérente. Du reste, le programme d'exploitation recharge systématiquement la configuration EEPROM sur un RESET pour avoir ainsi une initialisation correcte.



MANIPULATIONS :

- 01) Faire un RESET pour recommencer "à froid".
- 02) Cliquer sur la touche **Mode** pour revenir en **COMMANDE**.
- 03) Touche **[L]** et **ESC** pour afficher le contenu actuel du tableau des **Fiches croisées**. On obtient la configuration de la Fig.6 qui par défaut utilise dix croisements organisés par ordre alphabétique.
- 04) Sortir avec une touche quelconque.
- 05) **[L]** montre que par défaut on a une configuration de Base.
- 06) Consigner **[E]** et accepter puis vérifier avec **[L]**.
- 07) Avec **[X]** suivi de **OUI** imposer **RX > TM > CJ** par exemple.
- 08) Quitter avec **ESC** puis **[I]** confirmé par **OUI**.
- 09) Imposer **[5] > [1] > [3] > [P] > [U] > [K]** et **ESC ESC**.
- 10) Enfin on peut tester la commande **[R]** suivie de **NON**.
- 11) La commande **[L]** prouve que rien n'a changé.
- 12) On recommence avec **[R]** accepté cette fois par **OUI**. Le programme recharge les données actuellement inscrites en EEPROM puis passe à l'affichage de l'état du **Brouilleur** qui en résulte suivi de contenu du tableau des **Fiches croisées**.

04) Sauvegarder une initialisation machine.

A tout moment il est possible avec la commande **[S]** de sauvegarder la configuration d'initialisation actuelle en mémoire non volatile EEPROM. *À chaque RESET la dernière sauvegarde effectuée sera rechargée automatiquement.*

MANIPULATIONS :

- 01) Faire un RESET suivi de **Mode** pour "repartir de zéro".
- 02) Avec **[L]** on confirme un tableau de fiches saturé.

Proposition : Dans ce qui suit nous allons initialiser la machine avec la combinaison secrète du 24 Février 1942. On note dans le tableau de la Fig.2 que les trois bagues seront respectivement indexées sur **4**, **17** et **13**. On va commencer par en déduire les lettres qu'il faudra frapper sur le clavier alphabétique. Pour mémoire la Fig.7 représente un extrait de la table complète des combinaisons secrètes limité à l'encadré vert.

Fig.7

24	B	III	V	II	04	17	13	AL	CG	DN	ES	HP	IM	OW	RT	UZ	XY	JDH
----	---	-----	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----

- 03) Cliquer sur **[C]** et noter que **04/17/13** correspondent à **D/Q/M**.
- 04) Imposer **[I]** confirmé par **OUI** pour commencer l'initialisation.
- 05) Saisir dans l'ordre **[3] > [5] > [2] > [D] > [Q] > [M]**,
- 06) Continuer avec **[J] > [D] > [H]** suivi de la lettre **[B]** et **ESC** pour terminer la configuration du **Brouilleur** de la machine simulée.
- 07) Frapper un **[E]** suivie de **OUI** pour débrancher toutes les **Fiches croisées**. C'est impératif pour pouvoir coder dix lignes, car la commande **[X]** ou la commande **[A]** ajoutent des cordons fictifs à ceux déjà présents. Il faut donc tous les éliminer pour pouvoir les remplacer intégralement.
- 08) Touche **[X]** ou **[A]** complétée par la confirmation **OUI** pour saisir en cascade les dix couples de lettres.
- 09) **AL > CG > DN > ES > HP > IM > OW > RT > UZ > XY**. Le tableau s'affiche pour que l'on vérifie. Sortir de l'affichage. *(Pour mémoire il est inutile de les ordonner, car elles sont classées directement puisque on effectue la saisie par ordre phabétique.)*
- 10) Dernière vérification avec **[L]** avant de sauvegarder avec **[S]**.
- 11) Forcer un RESET pour recharger la configuration EEPROM.
- 12) Commande **[L]** qui confirme une sauvegarde effective.


05) Utiliser la machine en (dé)chiffrage.

Fondamentalement il n'y a strictement aucune différence entre le cryptage et le décryptage. Dans le premier cas on transforme un texte en des suites de lettres "incompréhensibles" alors que dans le deuxième cas, à partir de ce charabia on retrouve du texte "en clair". Naturellement, dans les deux cas l'opérateur doit commencer par recommencer sur une configuration d'initialisation identique. Conformément aux consignes du didacticiel vous avez bien assimilé les [Fiche n°27](#) à [Fiche n°32](#).

➤ Crypter un texte le 24 Février 1942.

Puisque nous avons sauvegardé en EEPROM l'initialisation correspondant à cette date il n'y a rien à faire sur notre réplique. Par contre, pour pouvoir comparer avec [\[Enigma\]](#) il faut impérativement conditionner cette dernière. Nous allons commencer les vérifications en se simplifiant la vie, c'est à dire que l'on va utiliser le **Moniteur** de l'**IDE** à **57600 baud** pour afficher les caractères chiffrés ou décodés sans avoir à noter les lettres qui "s'illuminent" sur le tableau des ampoules. *C'est une facilité de la machine virtuelle qui en parallèle de l'allumage des ampoules affiche en parallèle le résultat d'un cryptage dans la fenêtre contextuelle du Moniteur.*

MANIPULATIONS :

- 01) Activer [\[Enigma\]](#) sur l'ordinateur.
- 02) Sur cette dernière installer le contexte du **24 Février 1942**.
- 03) Activer le **Moniteur** avec  sur l'**IDE** en ayant ouvert l'éditeur avec un programme Arduino quelconque. Cette action a pour effet d'effectuer un RESET sur [P08_EXPLOITER_Enigma.ino](#).
- 04) Frapper **[A]** sept fois sur les deux machines.

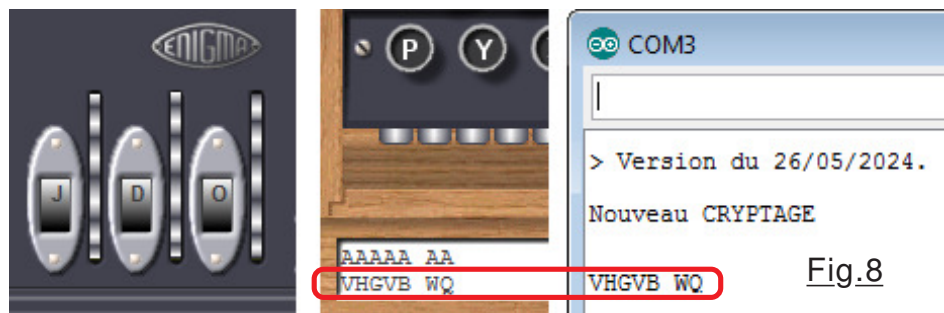


Fig.8

Comme on peut le constater sur la Fig.8 les deux machines fournissent exactement les mêmes chiffrages et les **Rotors** terminent avec des orientations identiques. *Si chez vous les résultats ne sont pas strictement conformes, c'est que forcément sur l'une au moins des deux machines l'initialisation n'est pas correcte.*

➤ Transmission en code Morse.

Pour l'ambiance nous allons "émettre" nos messages ultra secrets en **télégraphie**, le **code Morse** étant universel dans ce domaine et n'a jamais été concurrencé par d'autres standards.

MANIPULATIONS :

- 05) Touche **Mode** pour revenir en Mode **COMMANDE**.
- 06) Frapper sur **[M]** pour activer la génération de **Morse**. La petite LED jaune s'illumine pour indiquer l'activation de cette option.
- 07) Revenir en **CRYPTAGE** avec **Mode**.
- 08) Frapper cinq fois sur **[P]** par exemple. À partir de maintenant chaque caractère transmit est accompagné de son équivalent en télégraphie sonore. Revenir en **COMMANDE** avec **Mode**.
- 09) Lettre **[N]** pour passer en transmission rapide. (*Bascule de type télégraphie rapide / Normale.*)

Note : Vu la "richesse" des commandes de ce petit projet, les 26 lettres du clavier ont été affectées. Si possible le choix est lié au "verbe de l'action ou de l'option". Mais arrive un moment où la pénurie se fait sentir et il faut faire avec ce qui reste ...

- 10) Lorsque l'on clique sur **[N]** la petite LED bleue clignote durant environ une seconde, rapidement ou lentement en fonction de l'état imposé à l'option. Titiller plusieurs fois sur cette touche et *terminer sur un clignotement Rapide*.
- 11) **Mode** puis frapper quelques lettres. OUPS ... ça fonce !
- 12) Commande **Mode**. *Il est possible d'apprendre le code Morse avec notre Énigma*. Il suffit de repasser en vitesse **Normale** avec **[N]** puis de *demande de transmettre le Morse directement avec la touche [Z]*. Quand cette option est activée, *le Morse et l'ampoule orange allumée correspondent à la lettre cliquée*, alors que celle affichée dans la fenêtre du **Moniteur** reste cryptée. Quand l'option "Morse en direct" est active la LED verte clignote.
- 13) Revenir en **CRYPTAGE** et soumettre quelque lettres.



NOTE importante : Chaque fois qu'avec **Mode** on passe en mode **CRYPTAGE** on continue la même transmission, c'est à dire que l'on poursuit le chiffrement sans forcer la configuration initiale. Pour un nouveau message, il faut réinitialiser la machine. **Il suffit de replacer les trois Rotors en configuration de départ**, car le **Brouilleur** et le tableau des **Fiches croisées** virtuels restent inchangés.



- 14) Revenir en mode **COMMANDE** avec **Mode**.
- 15) Proposer **[F]** et confirmer avec **OUI** pour recalculer les **Rotors** sous la Fenêtre de la machine virtuelle.
- 16) Passer en **CRYPTAGE** et frapper frapper **[A]** sept fois. Comme la machine a été réinitialisée on retrouve le chiffrement de la Fig.8 puisqu'on obtient dans les mêmes conditions.

➤ Éteindre les LEDs du petit clavier.

Les LEDs du petit clavier constituent un artifice pour conditionner la machine. Comme ça ne correspond pas à la réalité historique, vous pouvez désirer ne plus voir le clignotement à travers les fentes de la trappe de service. La commande **[Q]**, choisie car elle est en haut à gauche donc facile à retenir, est prévue dans ce but.

- 17) Imposer la **COMMANDE [Q]** trois fois. C'est une bascule de type OUI/NON qui ne modifie pas les options. Elle se contente d'éteindre les quatre LEDs du petit clavier ou de les réactiver.
- 18) Revenir en **CRYPTAGE** et frapper quelques lettres.
- 19) Ressortir avec **Mode**. Un retour au mode **COMMANDE** rétablit automatiquement l'activité des LEDs du petit clavier.



ATTENTION : L'option **[Z]** est discrète et **reste mémorisée**. Si la télégraphie sonore en code Morse a été suspendue la LED jaune du petit clavier reste éteinte et l'on n'est plus averti que l'affichage des ampoules oranges est NON chiffré. Il sera important de penser à désactiver cette option.

- 20) Rétablir la télégraphie avec **[M]** : On constate que la petite LED verte clignote rapidement. (*Indique Morse NON crypté.*)
- 21) Frapper **[Z]** : La LED verte ne clignote plus.
- 22) Si désiré, frapper **[M]** pour annuler la télégraphie sonore.

➤ Cheminement du chiffrement.

Cette option constitue un luxe parfaitement accessoire au regard de l'usage courant de la chiffruse. Considérons le dessin de la Fig.9 qui montre le cheminement d'une lettre dans la machine et sa transformation. La commande **[J]** décrit le chiffrement à travers tous les éléments de l'électromécanique virtuelle.

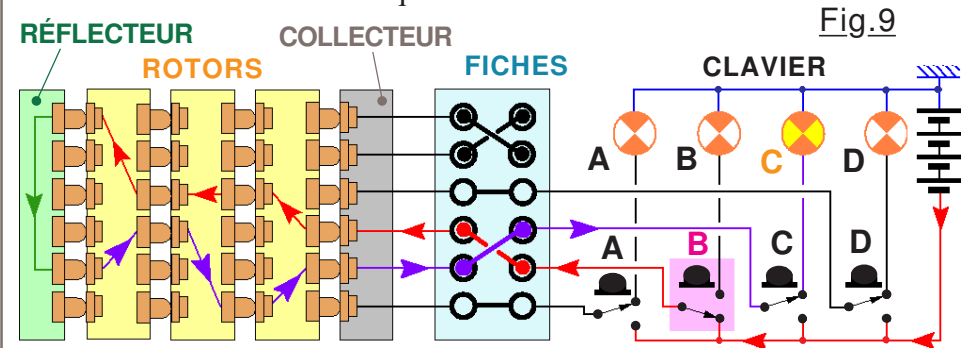


Fig.9

MANIPULATIONS :

- 23) Consigne **[J]** (*Bascule pour Jalonner.*) : La LED triple clignote durant une seconde en orange pour indiquer l'activation de ce mode. C'est une bascule de type OUI/NON. Si l'option est annulée la LED clignote alors en VERT.
- 24) Passer en **CRYPTAGE** et frapper quelques lettres. On obtient un affichage du type de celui de la Fig.10 dans lequel la traversée

U	[u < N]	[n < M]	[m < Q]	<--	B
J	[J > X]	[x > I]	[i > F]	-->	C

Fig.10

dans les deux sens du tableau des **Fiches croisées** est en bleu clair, la traversée des **Rotors** est en jaune et la transformation dans le **Réflexeur** en vert clair. Pour signaler le mode en cours la LED triple clignote en orange au lieu du vert standard.

- 25) Glups, vous avez oublié la lettre d'une commande. Soit vous consultez les fiches imprimées. Mais il est également possible et facile en **COMMANDE** d'obtenir un résumé sur l'écran graphique : **Mode** qui fait sortir du cryptage et **[H]** (*Pour Help.*) pour ouvrir l'affichage des commandes sur l'écran OLED. Cette fonction comporte plusieurs pages-écran et l'on "navigue" verticalement avec ▼ et ▲. Sortie du mode avec **NON**.

➤ Codage / Décodage.

Manipulations élémentaires, nous allons vérifier que la machine fonctionne aussi-bien en cryptage qu'en décryptage. Il suffit de coder un texte simple, noter les lettres télégraphiées. Puis recalcr les **Rotors** et soumettre le texte crypté pour retrouver le contenu initial.

MANIPULATIONS :

- 26) Provoquer un RESET pour "débuter une nouvelle journée".
- 27) **Mode** pour basculer en mode **COMMANDE**.
- 28) Soumettre la consigne **[L]** et vérifier que l'on a bien une configuration "complète" avec dix **Fiches croisées**.
- 29) Sortir avec deux **ESC** et passer en cryptage avec **Mode**.
- 30) Proposer **[B]**, **[O]**, **[N]**, **[J]**, **[O]**, **[U]**, **[R]**. La chiffreuse transforme ces sept lettres en **QJSJGRMT**.
- 31) Retourner en mode **COMMANDE**.
- 32) Frapper un **[F]** et accepter pour recalcr les **Rotors** en **[JDH]** sous la fenêtre virtuelle de la machine.
- 33) Reprendre le cryptage avec **Mode**.
- 34) Frapper dans l'ordre les lettres **[Q]**, **[S]**, **[J]**, **[G]**, **[R]**, **[M]**, **[T]**. La chiffreuse retransforme ces sept lettres en **BONJOUR**, confirmant le fait que l'Énigma historique fonctionnait aussi-bien en cryptage qu'en décodage

NOTE : Typiquement les messages étaient envoyés par groupes de cinq lettres comme montré sur la Fig.11 sachant que sur cet exemple la transmission a été terminée. **P08** précise alors la position des **Rotors** en fin du cryptage. (*On en verra l'utilité dans le chapitre*

Nouveau CRYPTAGE

BONJO URBZDZ WCLXT KSBTM CDLPB MUQOF XYHCX TGYJF LINHN XSHIU NTHEO RXPQP
BUBTZ SZSOO STGOT FSODB BZZLX LCYZX IFGNF DZEEQ IBMGF JBWZF CKPFM GBXQC
IVIBB RNCOC JUVYD KMWJP FMDRM TGLWF OZLXG JEYYQ PVPBW NCKVK LZTCE DLDCT
FENETRE = [BIB]

Fig.11

qui suit.) Pour des raisons évidentes de respect des protocoles de l'époque, quand on réalise un codage long, cette présentation est respectée dans la fenêtre du **Moniteur**. Soumettre à la machine des textes longs peut s'avérer un tantinet indigeste, comme c'était le cas du reste sur l'Énigma réelle sur laquelle chaque enfoncement d'une touche devait contrer l'effort qui servait à actionner le ou les **Rotors**.

06) Coder rapidement des textes longs.

Précisé dans la page précédente, on peut fort bien *désirer crypter un texte long* sans pour autant y passer trop de temps. Dans ce cadre, pouvoir effectuer des Copier/Coller sur l'ordinateur va se montrer particulièrement agréable à l'usage. C'est dans ce but que le Mode **TEXTE** a été ajouté aux **COMMANDES**.

MANIPULATIONS :

01) REESET puis replacer la machine en mode **COMMANDE**.

02) Consigne **[T]** et accepter avec **OUI**.

La machine passe automatiquement en **CRYPTAGE**, et la LED triple s'illumine en continu avec ses trois composantes activées. (*Lumière proche du blanc.*) **Les deux claviers sont maintenant ignorés** et les frappes doivent être effectuées sur celui de l'ordinateur, la saisie se faisant dans la fenêtre contextuelle du **Moniteur** de l'**IDE**. La seule façon de revenir en mode **COMMANDE** consistera à frapper '&'.



Important : Le maximum de caractères accepté par **P08** est de soixante en saisie sur le **Moniteur**. Toute suite dépassant cette limite sera purement ignorée. **Le logiciel d'exploitation réalise un filtrage des données :** Les accentués seront remplacés par leurs équivalents simples. La ponctuation est ignorée et Tout autre caractère que ceux valides sera ignoré. Les lettres frappées en minuscules seront automatiquement traduites en équivalent majuscule.

Voici le long message à transmettre :

Bonjour les amis, il importe de noter que le maximum de caractères est de soixante en saisie sur le Moniteur. Tout autre caractère que ceux valides sera ignoré. (Les espaces et la ponctuation seront ignorés.) Les accentués seront remplacés par leurs équivalents simples. Ce texte est volontairement repéré par des couleurs pour délimiter des blocs de soixante caractères pour ne pas déborder l'éditeur. Si le texte saisi dépasse soixante, ce qui suit sera ignoré.

01) Avec la souris sélectionner la ligne de **texte rose**.

02) **Ctrl c** pour la **copier** dans la mémoire tampon de WINDOW'S.

03) **Ctrl v** pour la **coller** dans la fenêtre de saisie du **Moniteur**.



Note : L'ouverture de ce mode suspend les options 'B' et 'M'. C'est la raison pour laquelle à l'ouverture du mode TEXTE les trois petites LEDs du clavier s'éteignent et le reste au retour dans le mode COMMANDES.



(ATTENTION : L'option 'Z' reste mémorisée.)

Le comportement de notre machine ressemble assez à celui d'[Enigma] en mode Auto Typing avec une vitesse de codage sélectionnée à Normal. Ce qui ralentit notre machine virtuelle c'est l'affichage sur l'écran graphique du mouvement des Rotors. Pour obtenir un codage ultra rapide il suffit de "cacher" ces rotations :

- 04) RESET et **Mode** pour tout recommencer.
- 05) Consigne [T] et accepter avec **OUI**.
- 06) Si vous consultez avec attention les fiches résumant les commandes, vous allez constater qu'en Mode TEXTE on dispose de six commandes regroupées sur le "pavé numérique de l'ordinateur. Frapper un '9' pour passer en cadence ultra rapide. Quand on valide le '9' en apparence il ne se passe rien.
- 07) Avec la souris sélectionner la ligne de **texte rose**.
- 08) **Ctrl c** pour la **copier** dans la mémoire tampon de WINDOW'S.
- 09) **Ctrl v** pour la **coller** dans la fenêtre de saisie du Moniteur. Cette fois "ça fonce" et les LEDs des ampoules ne font que scintiller.

Note : Le message complet a été fractionné en plusieurs groupes de 60 caractères pour rester dans la marge limitée par le Moniteur de l'IDE. Il suffit de placer autant de "morceaux" de textes dans la fenêtre de saisie sans sortir du cryptage avec '&'. Il y a continuité du listage correctement formaté. On peut par cette technique transmettre des messages aussi longs que désiré.

- 10) Maintenant **copier** la ligne de **texte bleu**.
- 11) La **coller** dans la fenêtre de saisie du Moniteur : On constate que *tant que l'on ne quitte pas la transmission avec '&' le texte continue d'être correctement formaté.*
- 12) **Sans vous tromper**, recommencer cette procédure avec toutes les autres lignes de ce long texte.
- 13) Sortir du Mode TEXTE avec la ligne presque vide '&'.
14) Réinitialiser les Rotors avec [F] et accepter avec **OUI**.

➤ Décrypter rapidement des textes longs.

C'est strictement la même procédure que celle précédente sauf que pour cette dernière le contenu initial était dans le fichier texte du didacticiel, alors que pour cet exercice il se trouve dans la fenêtre contextuelle du Moniteur ce qui en principe est exactement pareil ... ou presque :

Différence : Chaque ligne affichée dans le formatage ne comporte que $12 \times 5 = 60$ lettres. Mais si l'on sélectionne toute la ligne, en réalité on va copier 60 lettres et 11 espaces. On dépassera ainsi la limite des 60 et chaque fois dix lettres du message seront perdues.

Conclusion : On ne va copier que 10 regroupements à la fois entre chaque **copier / coller**.

- 15) Consigne [T] et accepter avec **OUI** pour commencer le décodage.
- 16) Frapper un '9' puis *sélectionner les dix premiers groupes* dans la fenêtre d'affichage du Moniteur à l'aide de la souris.
- 17) **Copier** ce texte et le **coller** dans la ligne de saisie.
- 18) Recommencer avec *les dix groupes suivants*.
- 19) Continuer ainsi jusqu'à la fin ... n'est fastoche qu'en théorie !

Le risque de se tromper ne serait-ce que d'un caractère est considérable et Paffff il faut tout recommencer, car avec une seule lettre oubliée, les Rotors ont tourné et le décodage ne sera plus correct. Je suis presque certain que vous avez galéré et que l'ordinateur est passé par la fenêtre !

Il existe dans un tel contexte une procédure bien plus simple :

- 20) **Copier** l'intégralité du texte encodé et le **coller** dans un éditeur de texte. Par exemple le Bloc notes.exe est idéal parce que *tous les caractère de sa police ont une largeur identique* et sont alignés.
- 21) Supprimer un à un les espaces comme ceux montrés en rouge sur la Fig.12 avec la ligne jaune ajoutée pour que vous puissiez vérifier que l'on obtient bien des lignes de 60 lettres. Pour la dernière ligne ce n'est pas la peine puisqu'elle est courte.

```

-----*****-----*****-----*****
QSJGRMTAWAQXXGLBMWLRXINRNCAOKXZIIISDQJZKAONXTGIDCIXILXZIOUFW
ESWLFFQBKHXYRZDWQNSHOLGPBUTOCUICBCCUPXVTCUPVHGJHPWSPTYEFAULM
AYSMCFKSQOUWPILZPVGKDDGKBMUJBVUCAKORNCDWLDBIEPCIVAMJKLUUDFSC
XVWUGGBVEKECEKRLLTQYTPNWOIUGLZGWZLNHDBVRAMBMYRQDFBXPJRYBZUQB
NOBAXTFCOWCOHUKRNGHIPMZQTSVWKZGUTZWVDEQADWCNQFCIGULNZWJDQLT
UPQWXIHABIONCLBUSFLCXLSUFYYYIWALTOVDNWXZOTYTLYOUZZBRQGNXAVX
NNVKB DLTYX KAQZE SBNY
FENETRE = [JRW]

```

Fig.12

- 22) Maintenant on se contente de sélectionner une ligne dans le **Bloc notes.exe** et de la **copier**.
- 23) On recommence avec toutes les autres lignes. C'est d'autant plus facile que *la dernière ligne sélectionnée reste en bleu*, on ne peut donc pas se tromper et en sauter ou en cloner une.

Nouveau CRYPTAGE

BONJO URLES AMISI LIMPO RTEDE NOTER QUELE MAXIM UMDEC ARACT ERESE STDES
OIXAN TEENS AISIE SURLE MONIT EURTO UTAUT RECAR ACTER EQUEC EUXVA LIDES
SERAI GNORE LESES PACES ETLAP ONCTU ATION SERON TIGNO RESLE SACCE NTUES
SERON TREMP LACES PARLE URSEQ UIVAL ENTSS IMPL SCETE XTEES TVOLO NTAIR
EMENT REPER EPARD ESCOU LEURS POURD ELIMI TERDE SBLOC SDES O IXANT ECARA
CTERE SPOUR NEPAS DEBOR DERLE DITEU RSILE TEXTE SAISI DEPAS SESOI XANTE
CEQUI SUITS ERAIG NORE
FENETRE = [JRW]

Fig.13

On peut vérifier sur la Fig.13 que l'on retrouve bien le texte initial forcé en majuscules, avec des accentués remplacés par leurs équivalents simples et débarrassé de toute la ponctuation.

- 24) Poursuivre avec '0' pour rétablir "Rotors" : En apparence (*seulement.*) il ne s'est rien passé.
- 25) Frapper la chaîne 't', 'e', 's', 't' : L'afficheur est à nouveau activé.
- 26) Proposer la suite '*', '-', 'a', 'B', 'c', 'D' : Toutes les lettres sont en majuscules, la télégraphie est activée à vitesse lente.
- 27) Continuer avec '+', 'e', 'f', 'g', 'h' : Le Morse est passé en vitesse rapide ce qui ralentit malgré tout la cadence de la transmission.
- 28) Caractère '/' pour stopper la télégraphie, puis 'a', 'a', 'a', '&', 'a', 'a', 'a', 'a' : Seules les trois premières lettres sont encodées, puis le '&' est rencontré et l'on revient au mode **COMMANDE**.
- 29) Cliquer sur [T] acceptée avec **OUI** pour reprendre le mode **TEXTE**.
- 30) Saisir '9', 'a', 'a' pour chiffrer en cadence rapide.
- 31) Sortir du mode avec 'a', 'a', 'a', '&', 'a', 'a', 'a'. Seuls les trois premiers 'a' sont codés, mais ce n'est pas nouveau.
- 32) Répéter [T] avec **OUI** pour persister en mode **TEXTE**.
- 31) Tester la chaîne 'a', 'z', 'e', 'r', 't', 'y' : On constate que le mode rapide '9' reste mémorisé quand on quitte le mode **TEXTE**. Il est donc fortement conseillé de terminer ce type de transmission avec '0' avant le '&' pour replacer l'ensemble en "standard". Bien entendu tout RESET rétablira une configuration banale.

➤ Afficher le texte frappé dans le Moniteur.

Lorsqu'une saisie se fait dans la fenêtre contextuelle du **Moniteur** de l'**IDE**, dès que l'on valide la ligne elle s'efface ce qui peut présenter un inconvénient important. En effet, si l'on saisit en direct une ligne trop longue, on perd des caractères, et il est difficile de continuer correctement la transmission. La commande [W] a été prévue pour palier ce risque.

- 32) Consigner '0' suivi de '&'.

- 33) [D] avec **OUI** pour avoir une configuration commune.

(Une coupure secteur intempestive a brouillé la configuration de ma machine, donc pour recommencer on réinitialise.)

- 34) Touche [W] confirmée par **OUI**.

- 35) Frapper [T] activé avec **OUI**.

- 36) **Copier** la chaîne de caractères "Information : En 1945 on entre en guerre, et c'est à cette époque que l'Enigma a été utilisée pour les transmissions dans les armées."

[INFORMATIONENONENTREENGUERREETCESTACETTEE] Fig.14
HQUME CCRJS ETTCO NMISP YVYIC JSKXJ RYTGF MSWXT W

La Fig.14 présente le résultat obtenu. La longueur de texte retenue colorisée en rose ne fait que 41 caractères alors que la zone saisie en fait 60. Le filtrage a éliminé les caractères interdits : Les quatre chiffres, les espaces, l'apostrophe, la virgule et le ':'. Les accentués ont été remplacés par des lettres simples et toutes les lettres ont été "clonées" en majuscules. On va transmettre la suite du message :

- 37) **Copier** la suite "poque que l'Enigma a été utilisée pour les transmissions dans les armées." : Seul le début en rose est crypté correspondant à 60 caractères.

- 38) Terminer avec "s les armées." qui cette fois ne déborde pas.

Le mode [T] surtout en option '0' permet un cryptage ou un décodage ultra rapide. Il présente de surcroît un texte formaté par groupe de cinq lettres comme c'était le cas à l'époque de l'utilisation de cette machine dans les armées. **L'option [W] est bien commode pour voir ce qui a été réellement transmit si l'on déborde la limite des 60 caractères.** Cette option dégrade toutefois le formatage du texte chiffré car on perd la continuité des groupes d'affichage.

07) Coder avec les protocoles de 1939 à 1945.

L'Énigma ne pouvant traiter que des lettres non accentuées avec exclusion de toute ponctuation et chiffres, des conventions étaient imposées dans les armées pour "uniformiser" les transmissions. La **Fiche** non numérotée et intitulée **Protocoles de cryptage en 1939/1945** résume les conventions de l'époque. Bien qu'en français le **ä**, le **ö** et le **ü** restent rares, vous pouvez désirer respecter les contraintes pour "le plaisir historique". Vous allez vous rendre compte que c'est une opération infiniment plus indigeste que l'on pourrait le penser. Pour vous aider dans ce "petit délire", je vous propose la commande **[U]** qui transforme un texte quelconque dans la fenêtre du **Moniteur** en son équivalent respectant les protocoles imposées dans les armées allemandes.

MANIPULATIONS :

- 01) Frapper **'&'** pour revenir au mode **COMMANDE**.
- 02) Cliquer sur **[U]** et accepter avec **ROI**. La LED triple ne clignote plus et éclaire en "violet" constant pour signaler le mode.
- 03) **Copier** la chaîne de caractères "Il fait chaud à Paris. A, B, C, H, ä ö ü. 1234". Après affichage on revient en **COMMANDE**.

```
Nouveau CRYPTAGE
>>> Respecter les PROTOCOLES <<<
Frapper le texte original :
[IL FAIT CHAUD A PARIS. A, B, C, H, ä ö ü. 1234]
Texte traduité :
[ILFAITQAUDAPARISXAYBYCYHYAEUEUX]
Nouveau CRYPTAGE
```

Fig.15

Le traitement de ce texte montre sur la Fig.15 que le **'ä'** continue à se voir converti en majuscule non accentuée. Les espaces sont éliminés. Contrairement au protocole le nom propre PARIS n'a pas été doublé, car le logiciel ne détecte pas les noms propres. Les chiffres ont été éliminés car non présent sur le clavier d'Énigma. Le **ch** de Chaud a bien été remplacé par **'Q'** alors que le **C** et le **H** isolés ne sont pas modifiés. Les virgules sont remplacées par des **Y** et le point final par un **X**. En résumé, le texte traduité et placé entre crochets est celui qu'il faut crypter en doublant PARIS et avec 1234 en lettres.

[ILFAITQAUDAPARISXAYBYCYHYAEUEUX]

08) Commandes diverses.

Quelques commandes viennent enrichir la liste des possibilités, certaines restant des petits plus "gratuits" possibles car le logiciel ayant été optimisé à outrance il restait quelques octets à logger dans la mémoire réservée au programme.

➤ Test du tableau des ampoules.

Cette commande relève directement d'un "luxe" et n'a strictement rien d'historique. La commande **[Y]** est de type bascule OUI/NON. Si l'option est active, les 26 LEDs oranges du tableau des ampoules virtuelles s'illuminent simultanément. Cette option d'une valeur opérationnelle très faible sert à vérifier l'ensemble lors du câblage initial, car vu la fiabilité des LEDs, avant que l'un de ces témoins lumineux soit en panne il va couler pas mal d'eau sous les ponts ... et la guerre sera de loin terminée ! En fonctionnement autonome sur accumulateur, il ne faudra pas abuser de cette possibilité durant de trop longues périodes, car c'est la configuration de la machine virtuelle qui consomme le plus. *(J'avoue que c'est aussi pour consommer les 26 touches possibles comme commande que j'ai ajouté en fin de développement ce petit plaisir.)*

➤ Mesure de la tension sur le +5Vcc.

Que la petite carte Arduino NANO soit alimentée par sa prise mini-USB de téléversement, ou directement sur le **+5Vcc** par un accumulateur rechargeable de type "bloc USB", en mesurer la tension n'est pas forcément inutile. Sur accumulateur, lorsque cette tension diminue nettement en dessous de +5V, c'est que la décharge est bien avancée et que bientôt le dispositif va passer en dessous du fonctionnement correct du microcontrôleur.

MANIPULATIONS :

- 01) **'&'** pour revenir au mode **COMMANDE**.
- 02) Tester **[Y]** quatre ou six fois pour en observer l'effet.
- 03) Frapper **[V]** pour faire afficher la valeur de la tension sur le **+5Vcc**. La petite LED bleue en standard attend de nous la frappe d'une touche quelconque pour sortir de l'affichage temporaire.

Lorsque l'on alimente avec la prise USB de l'ordinateur la tension est généralement d'environ 4,8V à 4,9V ce qui n'a strictement rien d'anormal sur tout si la ligne USB est longue voir avec plusieurs raccords.