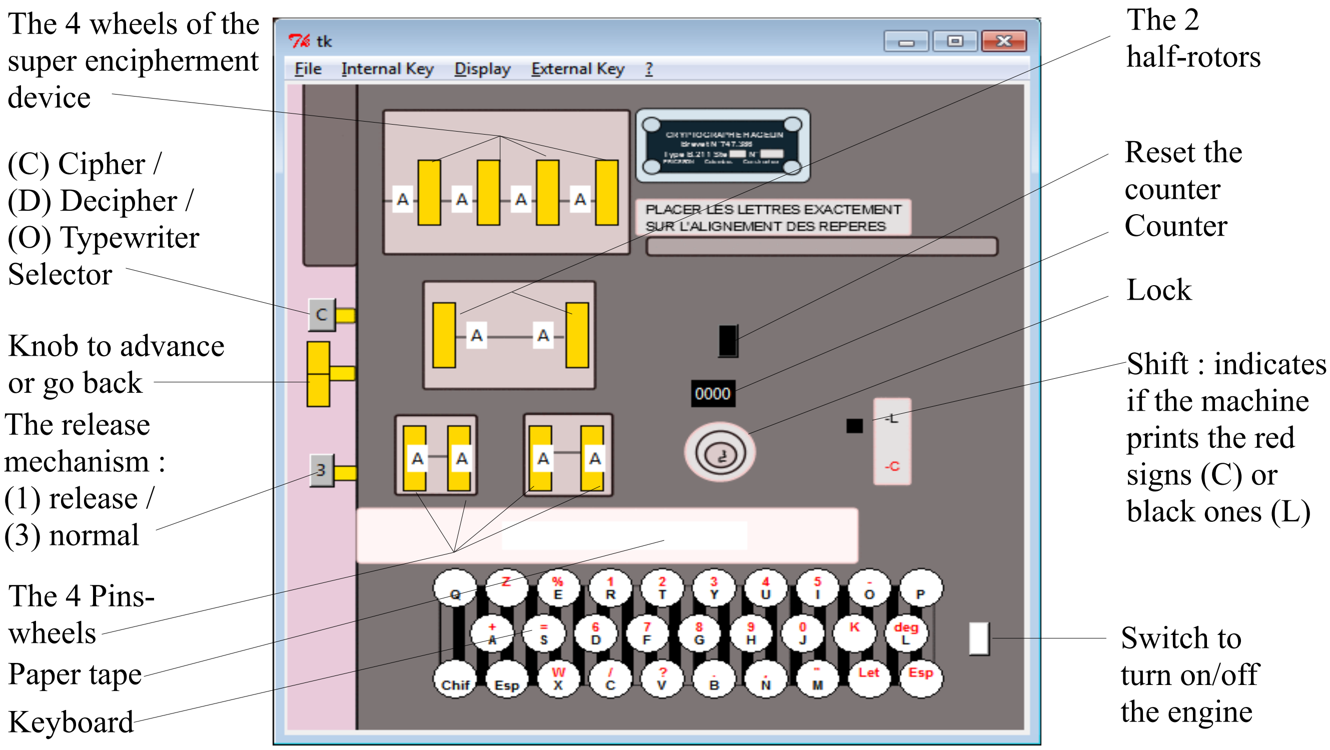
B-211 Simulator – Help

This documentation is a complement of the B-211 Manual (not the Simulator manual [it is this present document, but the genuine manual of the B-211). An exercpt of this manual is present insides the simulator (menu labeled « Manual »).


The 4 wheels of the super encipherment device
(C) Cipher / (D) Decipher / (O) Typewriter Selector
Knob to advance or go back
The release mechanism : (1) release / (3) normal
The 4 Pins-wheels
Paper tape
Keyboard
The 2 half-rotors
Reset the counter
Counter
Lock
Shift : indicates if the machine prints the red signs (C) or black ones (L)
Switch to turn on/off the engine
tk
File
Internal Key
Display
External Key
?
PLACER LES LETTRES EXACTEMENT SUR L'ALIGNEMENT DES REPERES
0000
-L
-C
Chif
Esp
Let
deg

General Description

WARNING ! Before any ciphering or deciphering operations, you need to switch on the machine!

Ciphering : the user inputs the plain text on the keyboard. The ciphered letters are printed on a paper tape. The button on the left-high corner must be on the "C" (cipher mode) position.

Deciphering : the user inputs the cryptogram on the keyboard. The plain letters are printed on a paper tape. The button on left-high corner must be on the "D" (decipher mode) position.

Remark : The machine can act as a typewriter. The button on left-high corner must be on the "O" position.

Before ciphering/deciphering, the user must set the external key :

- The initial position of the four rotors of the super encipherment device : a letter from 'A' to 'P' (ABCDEFGHIKLMNOP).
- The initial position of the two half rotors : a letter from 'A' to 'K' (ABCDEFGHIK).
- The initial position of the four wheels :
  - Wheel 23 : a letter from the set : 'ABCDEFGHIKLMNOPQRSTUVXY'
  - Wheel 21 : a letter from the set : 'ABCDEFGHIKLMNOPQRSTUV'
  - Wheel 19 : a letter from the set : 'ABCDEFGHIKLMNOPQRST'
  - Wheel 17 : a letter from the set : 'ABCDEFGHIKLMNOPQR'

To do that, you must use the yellow button near by the letter which composes the external key.
On top, you have the four buttons which manage the four rotors of the super encipherment device.
On the middle, you have the two buttons which manage the two half rotors.
Below, you have the four buttons which manage the fours wheels.

WARNING! You can't set the external key in the normal way of functionning (ciphering/deciphering/typewriter mode). You must set the machine in "1" (Release) mode. To do that, press on the button on the left. If you want to return on the normal way (ciphering / deciphering / tywriter mode), press again on this button. You will be in the "3"(Advance) mode.

A counter shows the number of the letter which is enciphered or deciphered. A button permits to go back or to advance the counter (and the components of the external key). This button is on the left at the same level than the wheels buttons. To be able to act the button, you must be in the "1" (Release) mode.

Entering a message (a plain or a cipher one)

You can click on the buttons drawn on the simulator.
You can also enter the message from the computer keyboard.
If you choose this second method, special keys have the following meanings :
« $ » The « Chif » key (to switch to red signs)
« > » The « Let » key (to switch to black signs)

The menus

[File][New] or [Internal Key][Zeroizing]

Reset the internal key (the setting of the four Pins Wheels and the four plugboards)

[File][Open]

Load an internal key (The KEYS directory is a good place to store internals keys).

[File][Save Key File as]

Store the internal key. You must name the file.

[File][Save]

If you have already saved the internal key, this menu store the internal key in the same file. If it is the first use, this menu is identical to the later one (Save Key File as)

[File][Exit]

Shut down the simulator.

[Internal Key][Zeroizing]

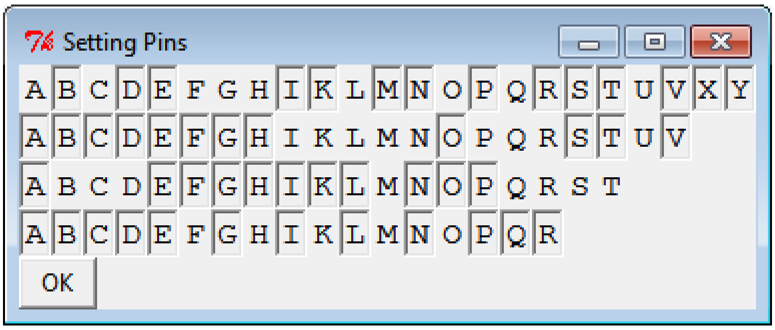
Reset the internal key (the setting of the four Pins Wheels and the four plugboards).

[Internal Key][Reset plugs]

Reset only the four plugboards.

[Internal Key][Setting key wheel Pins]

This menu brings up a window. On this one, each Pin of each wheel can be seen. If you clic on it, the value of the pin toggles. The Pin is active if the button is "flat". It is inactive if the button is "shinken".


Setting Pins

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

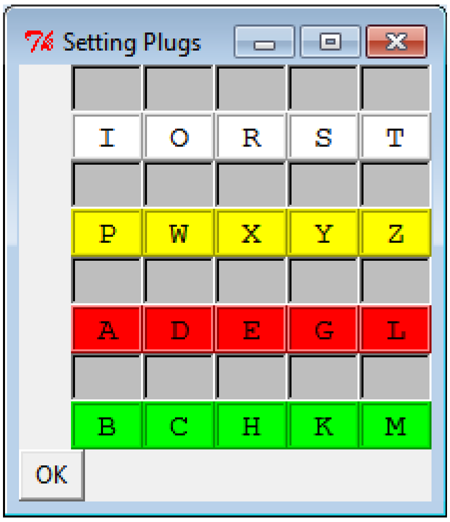
OK

[Internal Key][Setting key plugs]

This menu brings up a window. On this one, you can set the four plugboards. The electric circuits must be close to save the setting. For one plugboard, each input (represented by a letter [vowel or consonant]) must be connected with only one output. You put/remove a plug (a square with a letter inside) on clicking on a square. Then you can click on an empty square. Then you can put another plug in place of the latter one.

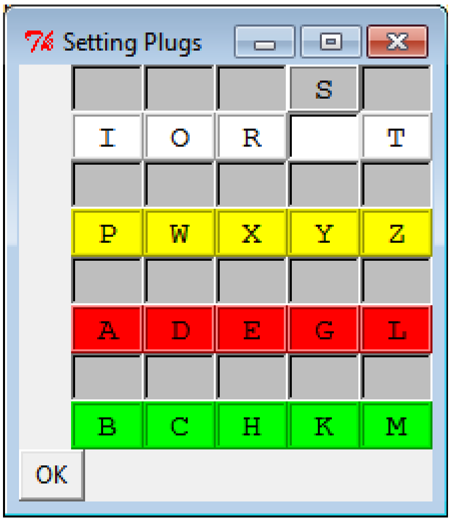
The permutation is the identity (no swapping) when the letters of a plugboard appear in alphabetical order, for example: IORST. The order OIRTS correspond to permutation10243.

Exemple : swap two plugs : You click on the first plug « S » (consequently, it desappears). Then you click on an empty box (for example one of the first row). The first plug was moved to this place (the eletric circuit is open). Then you can use the same procedure to move the second plug (« T ») in place of the first plug. Finnaly you move the first plug to the original place of the second plug (all circuits are now closed).


Setting Plugs

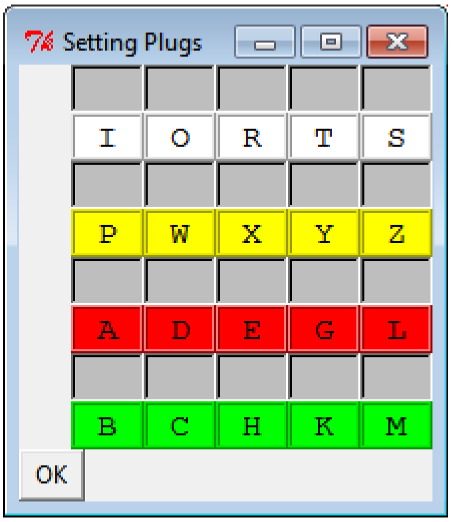
I O R S T
P W X Y Z
A D E G L
B C H K M

OK


Setting Plugs

S
I O R T
P W X Y Z
A D E G L
B C H K M

OK


Setting Plugs

I O R T S
P W X Y Z
A D E G L
B C H K M

OK

[Internal Key][Compatibility mode with M1]

This menu indicates if the simulator is (or isn't) in the compatibility mode with M1 model.

[Internal Key][Crossed mode with M1]

This menu indicates if the simulator is (or isn't) in the crossed mode with M1 model.

[Internal Key][Print internal key]

Print the current internal key. You can copy it on the clipboard.

Example :

```
Plugs : ALEDG:SOTRI
Plugs : BHCKM:PXYZW
Wheel 23 : __C__F_HI_LM_O__R____X_
Wheel 21 : ABCDE____K_M____RS___
Wheel 19 : AB_____HI__MN_PQ_S_
Wheel 17 : A_C__F__I_LMN__QR
```

[Internal Key][Generate new key]

Generate (randomly) a new internal key (Pins setting and Plugs setting).

[Internal Key][Print basic key]

Print the basic key (see later to get the basic key definition).

Example :

```
Keyboard     (black signs)(red signs)
                  OPJCN     ->0/,
                  HYB L     93.K!
                  QVXDM      ?W6"
                  U<FGR     4Z781
                  IASTE     5+=2%
> = Letters, < = Ciphers, ! = Degree

4 rotors (super encipherment) and 2 half-rotors
ABCDEFG   ABCDEFG   ABCDEFG   ABCDEFG   ABCDEFG   ABCDEFG
31240     41320     40132     43021     01243     23104
43210     14023     03124     21403     32410     34201
13042     43012     12430     24301     12304     12043
01342     02143     40213     24103     43021     23140
21043     34120     20134     03421     23410     01432
24310     24013     13240     32401     04132     12034
02314     10324     41023     30421     34021     40321
04321     30142     40231     23104     10243     01423
```

```
32041   34021   21340   13402   40132   34210
12034   42130   04123   43102   21304   40312
32104   40312   41203   20431
14302   34102   02341   23410
14230   10243   30124   20413
10432   42013   01423   43201
32410   30412   12304   23041
```

[Display][Tapes]

Print the cipher and plain texts.

[Display][Advance tapes]

Add spaces to cipher and plain texts

[Display][Cut tapes]

Delete the tapes (cipher and plain texts memorized)

[Display][Debug]

Switch to debug mode or to no-debug mode. In debug mode, the history is filled.

[Display][History]

Print the history (details of ciphering or deciphering) :

Example :

```
1    2 3 4 5    6 7   8901     2 3   4 5   6 7   8 9   0 1 2
E  : 0 0 0 1  : B F : GLAE ! K>4:4-R>0:4-P>0:0-S>4:4-P>4:1-A
N  : 1 0 1 1  : C G : GMAF ! K>0:4-R>1:1-P>4:1-S>3:1-P>3:2-F
E  : 0 1 1 0  : D H : GNAG ! K>4:4-R>1:3-P>4:2-S>1:2-P>2:3-D
M  : 0 1 0 1  : E I : GOAH ! K>2:4-R>4:0-P>3:3-S>2:4-P>1:1-Y
Y  : 1 1 1 0  : F K : GPAI ! K>1:1-R>4:0-P>3:3-S>2:4-P>1:1-Y
```

Column	Meaning
1	The input letter (plain letter or ciphered letter)
2	The current Pin of the Wheel 23 [1 = active, 0=inactive]
3	The current Pin of the Wheel 21
4	The current Pin of the Wheel 19
5	The current Pin of the Wheel 17
6	Vowel table position (of the first half-rotor)
7	Consonant table position (of the second half-rotor)
8	First super encipherment rotor position

9 Second super encipherment rotor position

10 Third super encipherment rotor position

11 Fourth super enciperment rotor poistion

12 Vowel component of fractionalization (on ciphering mode)

13 Consonant component of fractionalization (on ciphering mode)

14 Vowel substitution by the first half-rotor (on ciphering mode)
Substitution after the second vowel plugboard (on deciphering mode)

15 Consonent component by the second half-rotor (on ciphering mode)
Substitution after the second consonent plugboard (on deciphering mode)

16 Vowel substitition after the first vowel plugboard (on ciphering mode)
Vowel substitution by the first half-rotor (on deciphering mode)

17 Substitution after the first consonent plugboard (on ciphering mode)
Consonent component by the second half-rotor (on deciphering mode)

18 Substitution after the vowel two super encipherment rotors (on ciphering mode)
Substitition after the first vowel plugboard (on deciphering mode)

19 Substitution after the consonnent two super encipherment rotors (on ciphering mode)
Substitution after the first consonent plugboard (on deciphering mode)

20 Substitution after the second vowel plugboard (on ciphering mode)
Vowel substitution by the first half-rotor (on ciphering mode)

21 Substitution after the second consonnent plugboard (on ciphering mode)
Consonent component by the second half-rotor (on deciphering mode)

22 The output letter (ciphered letter or plain letter)

[Save history]

You can copy history on the clipboard.

[External Key][Ready to check]

Reset the external key and the counter.

[External Key][Come back]

Reset the counter to zero (we go back to the start: the external key is reset to its initial setting).

[To cipher from clipboard]

The text which is on the clipboard is ciphered (or deciphered).

[?][Help]

This actual help.

[?][Manual]

An exerpt of the genuine user manual of a the B-211.

[?][About …]

General information about this software (author, version, licence, …).

Example of ciphering and deciphering

Set the internal key (see this key in description of the menu [Internal Key][Print internal key])

Set the external key : GLAD BE SOCK (four super encipherment rotors, two half-rotors and the four pins-wheels)

Cipher this text :

```
ENEMY ATTACK EXPECTED ON YOUR POSITION
```

> Remark : the keying of letter « K » of the word « ATTACK » requires to switch on to the figure mode by hitting on the « Chif » button) and after hitting on the « K » letter, at last, hitting on the « Let » button to return on the letters mode (after or before the hitting on a space (black or red).

Normally, you get this ciphered text :

> AFDYY ZSJJT XQQVI DUPYJ ATLBP XQJXO QZXTN YBHOE

Changing of the basic key

With the GUI it is easy to change the external key. With the menus you can change the internal key. But you must edit files to change the basic key.

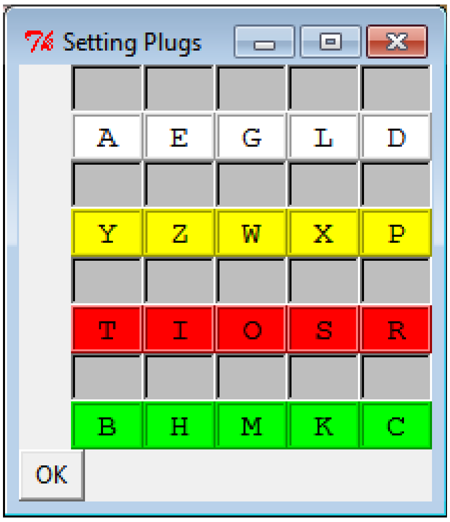
The files which store the basic key

All files needed are in the "rotors" directory :

- B211.modele : It contains several lines : The first one is the basename (without .rot extension) of the file which contains the wiring of the vowel half-rotor. The second line is the basename (without .rot extension) of the file which contains the wiring of the consonant half-rotor. The following lignes contains (without .rot extension) the name of files which contains the wiring of the four rotors of the super encipherment device.
- *.key : The most part of the internal key : first line contains the keyboard matrix. The second line contains the letters which appear on the keyboard and on the lamp panel. The third line contains the letters wich compose the vowel plugboard and its actual wiring. The fourth line contains the letters wich compose the consonant plugboard and its actual wiring. The remaining lines contains the wheel Pins setting.
- *.rot : A file which contains the wiring of an half-rotor or the wiring of a super encipherment rotor.

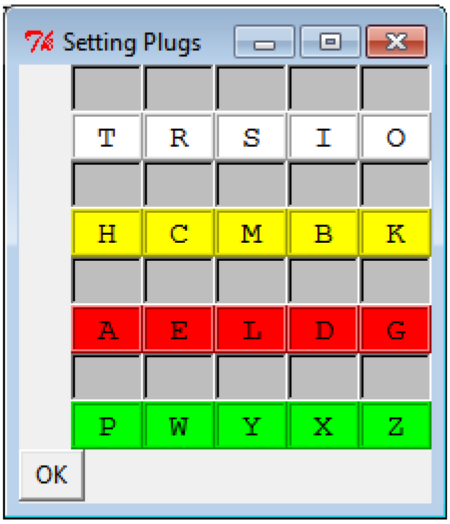
The cross-plugging configuration

With four plugboards it is possible to set two cross-plugging configurations. In the first cross-plugging configuration, the plugs of the first plugboard of the numeral channel are plugged into the sockets of the first plugboard of the letter channel and vice versa. In the second cross-plugging configuration, the plugs of the second plugboard of the numeral channel are plugged into the sockets of the seconf plugboard of the letter channel and vice versa. It is possible to apply the both cross-plugging settings, then we exchange the couple of rotors of the numeral channel with those of the letter channel.



Setting Plugs

A	E	G	L	D
Y	Z	W	X	P
T	I	O	S	R
B	H	M	K	C



Setting Plugs

T	R	S	I	O
H	C	M	B	K
A	E	L	D	G
P	W	Y	X	Z

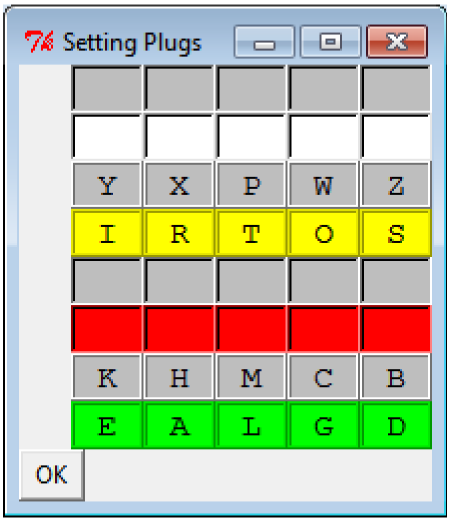
The compatibility mode

The M1 model (1937) doesn't have the super encipherment device. It haves only two plugboards (ADEGL and IORST). The M1 model acts as an ordinary B-21 machine but prints the cipher or plain text in place to enlight lamps. The M2 model (1943) uses the super encipherment device which is composed by four wheels and two another plugboards (BCHKM and PWXYZ).

You can setup the plugs to be in compatibility mode (with menu [Internal Key][Setting key plugs]), IE to have the behaviour of the M1 model. The menu [Internal Key][Compatibility mode with M1] is checked when the compatibility mode is effective. Finnaly, in debug mode, the history (menu [Display][History]) is simpler when the machine works in compatibiliy mode.

Plugs setting

To set the simulator to the compatibility mode you must set the plugs IORTS (in any order) in the Fourth row and the plugs ADEGL (in any order) in the last row.



Setting Plugs

Y	X	P	W	Z
I	R	T	O	S
K	H	M	C	B
E	A	L	G	D

History

In cipher mode [in compatibility mode]

```
1    2 3 4 5    6 7     8 9   0 1   2 3 4
E  : 1 1 0 0  : C E : K>4:4-R>4:2-P>1:4-L
```

In decipher mode [in compatibility mode]

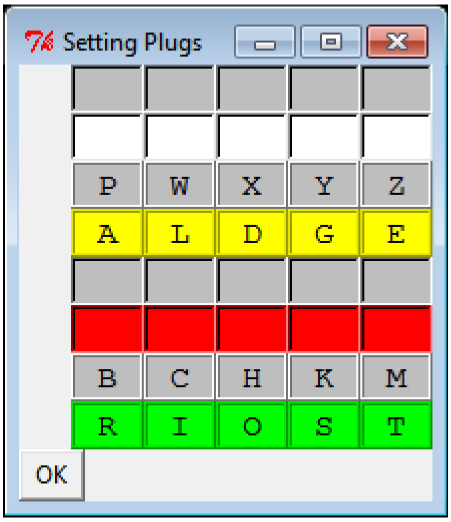
```
L  : 1 1 0 0  : C E : K>1:4-P>4:2-R>4:4-E
```

Column	Meaning
1	The input letter (plain letter or ciphered letter)
2	The current Pin of the Wheel 23 [1 = active, 0=inactive]
3	The current Pin of the Wheel 21
4	The current Pin of the Wheel 19
5	The current Pin of the Wheel 17
6	Vowel table position (of the first half-rotor)
7	Consonant table position (of the second half-rotor)
8	Vowel component of fractionalization (on ciphering mode)
9	Consonant component of fractionalization (on ciphering mode)
10	Vowel substitution by the first half-rotor (on ciphering mode) Substitution after the vowel plugboard (on deciphering mode)
11	Consonent component by the second half-rotor (on ciphering mode) Substitution after the consonent plugboard (on deciphering mode)
12	Substitution after the vowel plugboard (on ciphering mode) Vowel substitution by the first half-rotor (on deciphering mode)
13	Substitution after the consonent plugboard (on ciphering mode) Consonent component by the second half-rotor (on deciphering mode)
14	The output letter (ciphered letter or plain letter)

Crossed mode

When you press a key, two electrical signals are generated each encrypted independently. With the plugs it is possible to exchange both channels.

To set the simulator to this crossed mode you must set the plugs IORTS (in any order) in the last row and the plugs ADEGL (in any order) in the last fourth row.



P	W	X	Y	Z
A	L	D	G	E
B	C	H	K	M
R	I	O	S	T

Accuracy

In my simulator, the degree character ("°") is replaced by the exclamation mark "!". The main reason for this was my will that my graphic simulator (B-211.py) is compatible with my text simulator (B-211_tui.py). On the keyboard I replaced the degree character ("°") by the expression "deg".

Several sources describe the first model (M1) of the B-211 ([1], [4], [a]). So I think my simulator properly emulates this model.

Conversely, there are very few documents (pictures, diagrams) that describe the second model (M2). If people want to help me to validate my simulator for this model, they are welcomed.

References (Books)

[1] « Les écritures secrètes », by Adnré Muller, Presses Universitaires de France, 1971

[2] « Machine Cryptography and Modern Cryptanalysis », by Cipher A. Deavours and Louis Kruh, 1985.

[3] « Military Cryptanlytics Part II – Volume 2 », by Lambros D. Callimahos and William F. Friedman, From Aegean Park Press.

[4] « Instruction sur le fonctionnement et l'entretien de la Machine à Chiffrer Hagelin Type B-211 », N° 125 CH./CAB, 29 Mars 1943. This document was classified « Secret ». Unhappily this document doesn't explain the super-encipherment device. Only the M1 model is discribed.

References (Internet)

[a] Hagelin B-211, Crypto-Museum. http://cryptomuseum.com/crypto/hagelin/b211/index.htm
You can see pictures of the M1 model.

[b] TICOM I-58, Interview of Dr. Otto Buggisch. In 1942, He solved back trafic (two years), but he was unable to solve actual trafic. The B-211 was changed (M1 was replaced by M2).
http://cryptomuseum.com/ticom/files/i58.pdf

[c] French Hagelin cipher machines, by Christos Triantafyllopoulos,
http://chris-intel-corner.blogspot.fr/2011/12/french-hagelin-cipher-machines.html
The German called B-211 « F-20 ». American and German were able to read M1 trafic but weren't able to read the trafic from the modified machine (M2).

[d] The Hagelin B-21 and B-211, John J. G. Savard,
http://www.quadibloc.com/crypto/ro020601.htm

[e] D'Hagelin à Rita, ARCSI,
https://www.arcsi.fr/colloque-10-10-08/docs/hier-diapo.pdf
You can see a picture of a M1 model : the motor and battery is present. On the CGHQ pictures, these elements are missing.
A slide gives a description of the super-encipherment device. I'm not sure this description is completly accurate (I think the plugboards are not correctly placed).