B-21 Simulator – Manual

Remark : the reader must know the general working of B-21 (http://cryptomuseum.com/crypto/hagelin/b21/index.htm).

General Description

Ciphering : the user inputs the plain text on the keyboard. The ciphered letters are enlighted on the lamp panel. 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 enlighted on the lamp panel. The button on left-high corner must be on the "D" (decipher mode) position.

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

- The initial position of the two half rotors : a letter from 'A' to 'K'.
- 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 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 mode). You must set the machine in "R" (Release) mode. To do this press on the button on the left. If you want to return on the normal way (ciphering/deciphering mode), press again on this button. You will be in the "A"(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 "R" (Release) mode.

The menus

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

Reset the internal key (Wheel setting and plugboard)

[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 save 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][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 toggle. The Pin is active if the button is "flat". It is inactive if the button is "shinken".

[Internal Key][Setting key plugs]

This menu brings up a window. On this one, you can set the two 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. Each output must be different. You put/remove a plug (a square with a "O" inside) on clicking on a square.

[Internal Key][Print basic key]

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

[Internal Key][Generate new key]

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

[Internal Key][Print internal key]

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

[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)

[Debug]

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

[History]

Print the history (details of ciphering or deciphering) :

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
10	Vowel component after the plugboard (on ciphering mode)
11	Consonent component after the plugboard
12	Vowel substitution by the first half-rotor (on ciphering mode)
13	Consonent component by the second half-rotor
14	The output letter (ciphered letter or plain letter)

[Save history]

You can copy history on the clipboard.

[External Key][Ready to check]

Reinit 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 inside the clipboard is ciphered (or deciphered).

[?][Help]

This actual help.

[?][About …]

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

Example of ciphering and deciphering

Set the internal key with these values :

Plugboards : AEIOU:LNRST (default setting)

```
Wheel 23 : AB__E_G___LMN_P_R_T_VXY
Wheel 21 : A_C_E___I_LMN_P_R_T__
Wheel 19 : _BC__FG_I_LMNO_Q___
Wheel 17 : ABC____H_K_MNO__R
```

Set the external key : AARQML

Cipher this text :

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

Normally, you get this ciphered text :

```
LYSEU YKDRM APUNA WSFYP WCALL RMOIK APX
```

Remark : this benchmark is present in the book "Machine Cryptography and Modern Cryptanalysis", by C.A. Deavours and L. Kruh.

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 components of the basic key

The basic key is composed of several components :

- The keyboard matrix : it permits to split a letter in tuple of two letters. Each one is ciphered separetely.
- The letters which can be seen on the keyboard and the lamp panel. Remark : this software doesn't permit to indicate the position of a key or a lamp.
- The two groups of letters which match with the two plugboards.
- The cabling of the two half-rotors.

The files which store the basic key

All files needed are in the "rotors" directory :

- modele : It contains the model name of the machine. This name is also a file name (with .modele extension).
- *.modele : A model file. It contains several lines : The first one is the basename (without extension) of the file which contains the most part of the basic key. The second line is the basename (without .rot extension) of the file which contains the wiring of the vowel half-rotor. The third line is the basename (without .rot extension) of the file which contains the wiring of the consonant half-rotor.
- *.key : The most part of the basic 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