

Hagelin BC-52 Simulator v4.1

About the BC-52 Crypto Machine

After the success of the C-38 and M-209 as tactical cipher devices Hagelin Cryptos (Crypto AG) developed a cipher machine for high level military and diplomatic encryption. In 1952 the C-52 was introduced and, as Devours and Kruh wrote, 'caused ripples throughout the cryptanalytic community'. The C-52 raised the security of drum-and-lug devices to another level. The machine had 6 irregular moving pinwheels, selected from a set of 12, and the number of drum bars was extended to 32, of which 5 were also used to advance the wheels. When lugs and pins are selected carefully the C-52 provides even in this computer era a powerful encryption. The combination of C-52 and the keyboard, denoted B-52, was named BC-52. Within short time the BC-52 was purchased by more than 60 countries and remained popular until today.

This program is an accurate simulation of the Hagelin BC-52. The user can select between the C-52 and CX-52 model, both with the B-52 keyboard attachment. The machine can be customized and different wheel and drum bar configurations are possible.

Special thanks to John Alexander, David Ross and Klaus Kopacz for providing me with information that enabled me to create this simulator.

© Dirk Rijmenants 2006

mailto: dr.defcom@telenet.be

Website: <http://users.telenet.be/d.rijmenants>

How to use the simulator

The **BC-52 simulator** is designed to encrypt messages in a realistic and accurate way, as you would with the real BC-52. Move the mouse over the motor cage on the left of the machine to call the simulator menu. All these menus are also available by Function Keys. All objects such as buttons, wheels and other machine parts will show a little hand as icon.

You can always call the help file by pressing **F1** or by clicking the Help icon in the upper right corner of the program. There you will also find the speaker icon to enable or disable the sound effects, the information and exit button.

Key Settings

Both sender and receiver must set their BC-52 in exactly the same way. The key setting consists of five parts. The selection and order of the pinwheels, adjusting the pins on the wheels, the lugs, the print wheel offset and the initial start position of the pinwheels. To set the key you must click on the cover from the BC-52, above the pinwheels.

For more details on how to create quality keys please read the Key Settings section.

Pinwheel selection and settings

The wheel selection depends on the selected model. The **C-52** uses 6 wheels, selected from 12 different wheels with 25 up to 47 pins. The **CX-52** uses 6 identical wheels with 47 pins each. The model can be selected in the Customizing window (**F10**). When changing the model all pins and lugs are cleared.

The C-52 Model

The user must select a set of 6 different pinwheels. Each wheel is designated by a number between 25 and 47 which is also the number of pins on that wheel. In the key settings window you can see the 6 wheels that are currently set in the machine.

Click on one of the 6 wheels to extract it from the BC-52. The wheel is now shown in the middle of the window and all its pin settings are visible. You can adjust the pin settings of that wheel by clicking a pin number to **activate (red)** or **deactivate (white)** the pin. An extracted wheel can either be placed in the wheel box below or in an empty place in the BC-52. Other wheels can be selected from the wheel box and placed in the BC-52 after adjusting the pins.

The CX-52 Model

The CX-52 has 6 pinwheels with 47 pins each. Click on one of the 6 wheels to extract it from the BC-52. The wheel is now shown in the middle of the window and all its pin settings are visible. You can adjust the pin settings of that wheel by clicking a pin number to activate (red) or deactivate (white) the pin. When all pins are adjusted the wheel is placed back in the BC-52.

Setting the Lugs

The BC-52 has 32 sliding bars on the drum. 27 of these bars are used for enciphering only, and 5 bars are used to advance wheels 2,3,4,5 and 6 (numbered from left to right, and wheel 1 always steps). All the bars on the drum will pass the pin levers once on a full cycle of the drum.

A lug on one of the 27 bars will push or 'slide' that bar to the left if the current wheel pin in front of the lug is active. If more than one lug is on a given bar, for instance lug 2 and 3, they will act as OR function. The bar will go to the left if a pin is active on wheel 2 or wheel 3. Use the scroll bar to go through the 32 bars, and click on the lugs to place (red) or remove (white) a lug. In general 1 or 2 lug are used on the same bar, but some key setting use up to 3 lugs.

Setting the movement bars

There are 5 special bars that will advance the wheels in an irregular fashion. Each bar is designated to one of the wheels, except for the first wheel, which moves always. If for example a lug is placed on the 2nd position of the bar that is responsible for moving wheel 5, this bar will go to the left and move wheel 5 one step further if the current pin on the 2nd wheel is active.

In the early CX-52 setup these special bars also were also used for enciphering. However, due to complications in preparation of acceptable lug patterns later CX-52 models use the special movement bars only for stepping and not for enciphering. To see which bars are responsible for movement, and whether they also are used for enciphering, please check the BC-52 setup with **F10**.

The lugs on these bars are critical for the cryptographic security of the machine. Below is given a normal setup where bar 1 moves wheel 2, 2 moves 3 and so on.

B									
A			LUGS						
R	1	2	3	4	5	6			

1	1	-	-	-	-	-	moves	wheel	2
2	1	2	-	-	-	-	moves	wheel	3
3	1	2	3	-	-	-	moves	wheel	4
4	1	2	3	4	-	-	moves	wheel	5
5	1	2	3	4	5	-	moves	wheel	6

In this setup, a pin on wheel 1, in front of lug 1, will move wheels 2, 3, 4, 5 and 6 when respectively bars 1, 2, 3, 4 and 5 pass that pin. A pin on wheel 2 will move wheels 3, 4, 5 and 6, a pin on wheel 3 will move wheels 4, 5 and 6, and so on. This way, all wheels will move most of the time and will stop once in a while, depending on the pins on the wheels. This creates a highly irregular wheel movement sequence.

Load and Save Key settings

You can save the current key settings or load existing key settings through the simulator menu. These files are saved with the **.C52** extension. When starting the simulator the last used key setting is loaded automatically. On exit you will be asked whether you want to save changes or not.

Printwheel Offset Selection

To add a complication to the encryption it is possible to use an offset on the print wheel. This is normally done by pulling the dial knob away from the machine, thus disconnecting plain and cipher print wheels from each other, and turn the dial a given number of steps. When for example enciphering the letter **H** with an offset of 2 letters the machine will actually encipher the letter **F**. Both sender and receiver of a message must agree on what offset is used.

In the BC-52 Simulator the offset is adjusted by clicking the upper or lower half of the alphabet knob. When the label shows **A=A** there is no offset. By default there is no offset, and changes are not saved. The offset must be set each time the simulator is started.

Customizing the BC-52

Hagelin produced several different versions of the C-52 and CX-52. Therefore the program has a customizing option. You can call it by pressing the **F10** key.

Machine type: You can select between the C-52 model with 6 different pinwheels and the CX-52 with 6 wheels with 47 pins each. Be aware that change the machine model will clear all pins and plugs. Please set new pins and lugs before using the BC-52!

Wheel labeling Setup: Here you can select another offset for the alphanumeric labeling of the pinwheels. This is the label that is visible through the cover window when pin number 01 is aligned with the pin reading pawl inside the machine.

Wheel Advancing and Pin Reading Methode: In this frame you can select which bar on the drum is used to move a particular wheel. There are different version of the BC-52. The default way of wheel movement is that the first 5 bars are used to advance wheel 2,3,4,5 and 6. However, there are version where these bars are placed between the 27 normal bars, and even detachable bars are developed. Therefore the user can select which bars are responsible for moving the wheels.

You can select the type of bar that is used for a particular wheel. There are bars that will move the wheel if they are slided to the left (1), bars that move wheels if they are not slided to the left (3) and bars that will always move a wheel (3). A normal machine setup uses option 1.

You can also select whether the 5 special movement bars are also used for enciphering or only for movement (by default only for movement) and determine whether the pin pawls are kept in position during the cycling of the drum or that the pins change when wheels are advanced during the drum cycling.

Space Letter: Select the letter that will represent a space during enciphering. When during deciphering this letter is decrypted, it will be replaced by a space.

Program Speed: The program delays some operation to make the simulator realistic. Disable the graphics delay to increase the encryption process of the machine and disable some sound effects.

Create key settings

The selection and arrangement of the variable elements of the BC-52 is called the key settings. In order to obtain a quality encryption and high level of security there are some rules that have to be followed. In this section we will give some recommendations to create good key settings.

Pin Settings

On the pin settings the manufacturer advises the following: The experts recommend that in choosing a pattern for setting the pins a method be used that is statistically random. A simple way is flipping a coin and write down the result (obverse = active pin, reverse = inactive pin). For an even distribution you should never allow more than 3 successive pins on any wheel to have the same state and try to have close to 50 percent of the pins on a wheel in the active position.

The lugging

To create the lug settings we start with selecting 6 numbers between 1 and 14 whose sum is 27. Assign each of these numbers to one of the 6 pins. Write down all 64 possible combinations of six pins. The easiest way to do so is writing them down in binary order (1 = 000001, 2 = 000010, 3 = 000011 and so on). For each possible combination of pins, find the sum of numbers which have an active pin. Write this sum to the right of that combination. If a sum is greater than 25, subtract 26 from it. Continue until you have all sums for all possible pin combinations. Finally, check whether the 64 sums include all possible numbers from 0 to 25. If this is not the case, discard the lugging set and make a new one. With a little experience you will be able to correct bad luggings by changing only a few lugs.

Example of a Lugging check table:

	13	07	03	02	01	01	SUM
00:	0	0	0	0	0	0	= 0
01:	0	0	0	0	0	1	= 1
02:	0	0	0	0	1	0	= 1
03:	0	0	0	0	1	1	= 2
04:	0	0	0	1	0	0	= 2
05:	0	0	0	1	0	1	= 3
06:	0	0	0	1	1	0	= 3
07:	0	0	0	1	1	1	= 4
...							
...							
64:	1	1	1	1	1	1	= 27

Once a good lugging is found, we can start placing the lugs on the slide-bars. Start with the first of the 6 selected numbers. In our example from above this is 13. Place a lug on the first position of the first bar (disregard the movement bars!) and continue until you placed 13 lugs in the first position of the first 13 slide-bars. Proceed with placing 7 lugs in the seconde position of the next 7 slide-bars and so on.

Include or exclude movement bars

In the early CX-52 setup the special wheel movement bars also were also used for enciphering. When using the movement bars also for enciphering the lugs one must follow the rules as explained above, but also be sure to create a good stepping cycle for the wheels. Therefore, due to complications in preparation of acceptable lug patterns later CX-52 models use the special movement bars exclusively for stepping and not for enciphering.

To see which bars are responsible for movement, and whether they also are used for enciphering, please check the BC-52 setup with **F10**.

Lugs for Movement

Apart from setting the lugs for enciphering the user must also set the lugs on the special movement bars and make sure that there is a good variation in the stepping of the wheels. More on this can be read in the how to use section.

Enciphering with the BC-52

Before enciphering you must set the initial start position of the 6 wheels, also called message key (see enciphering procedures section). Change the position of the pinwheels by clicking the upper or lower half of that wheel. Select the **Cipher (C)** or **Decipher (D)** mode by clicking the handle on the left of the machine. In Cipher mode the output cipher text is printed in groups of 5 letters. Use the letter **X** as replacement for a space (can be changed with **F10**). In Decipher mode the output plain text is printed without groups and a deciphered **X** is replaced by a space.

To enter text on the C-52 the operator would turn the knob on the left of the alphabet dial to select the letter, and push down the handle on the right of the C-52. On the BC-52 configuration this process is done by the B-52 electric keyboard attachment.

You can click the paper advance knob to create spaces on the paper ribbon and press the **DEL** key to clear the ribbon. Use the **INS** key to memorize the current wheel positions and **HOME** to retrieve these wheel positions. To reset the counter, click the counter reset knob on the left of the counter.

The Clipboard Function

If you click on the paper ribbon or press **F5**, the Smart Clipboard Window appears. You can select how to format and transfer text to the clipboard.

Using the Auto Typing option

If you have a large amount of plain text or code that needs to be typed, you can use the Auto Typing Window. This window will appear if you press **F6**. In this window you can type, edit or paste pieces of text, or retrieve the content of the clipboard. You can select three different speeds of typing. Select 'Start' to begin processing the text. During the Auto Typing you can abort by pressing **ESC**. Make sure that all machine settings are completed and the external message indicator is in the correct position before starting the Auto Typing. Auto Typing will only process letters, and in Cipher mode also spaces, and will ignore all other characters.

The Key Sheet

You can view the current key settings by pressing **F8**

Exiting the simulator

To exit the BC-52 simulator, just click on the Exit symbol in the top right corner of the machine or use the menu. If desired, you can save the current machine settings, keep the previous settings, or erase all settings.

Shortcut Keys

F5 Show Clipboard
F6 Show Autotyping Window
F8 Show the current Key Settings
F10 Customizing the BC-52

Enciphering Procedures

In this section we will explain the procedures to encipher and decipher messages

To encipher and decipher messages correctly both sender and receiver must have identical key settings, agree a procedure to exchange the initial position of the wheels and compose the message. Crypto AG never wrote a standard procedure, but provided expertise to the customer on the functioning of the machine and advice to create secure keying and message procedures. Therefore different procedures were implemented by different customers to use the C-52 and CX-52. We will describe one procedure as example.

Note that this example is created with the default setting on the C-52 model. Please check your machine setup with F10. The key settings for this example are available in the installation folder of the program and can be loaded through the simulator menu. Also make sure that there's no printwheel offset ($A = A$).

First of all we need to set the BC-52 according to the given key settings. On the left of the key sheet are the selected wheels and their pin settings. On the right are the Lugs on the drum. Note that the first five bars on the drum are used to advance the wheels. At the bottom of the key sheet there is a checksum to verify your settings. These are 25 A's, enciphered with the machine in AAAAAA start position. In the enciphering example we will use the following settings for the machine:

```

-----
                    BC-52 KEY SETTINGS
-----
41 37 43 47 31 29  NR  1 2 3 4 5 6
-----
01 01 -- -- -- 01  01  1 - - - - -
02 -- -- 02 02 02  02  1 2 - - - -
-- -- 03 03 -- --  03  1 2 3 - - -
04 04 -- -- 04 04  04  1 2 3 4 - -
-- -- 05 05 -- --  05  1 2 3 4 5 -
-- -- -- -- -- --  06  1 - - - - -
07 -- 07 07 -- --  07  1 - - - - -
08 08 -- -- 08 08  08  1 - - - - -
-- -- 09 -- 09 09  09  1 - - - 5 -
10 10 10 -- -- --  10  1 - 3 - - -
11 11 11 -- 11 --  11  1 2 - - - -
-- 12 -- 12 -- 12  12  - 2 - - - -
13 -- -- 13 -- 13  13  - 2 - - - -
-- -- 14 -- 14 --  14  - 2 3 - - -
15 15 -- 15 -- 15  15  - 2 3 - - -
16 -- 16 -- -- 16  16  - - 3 - - -
-- 17 -- 17 17 --  17  - - 3 - - -
18 18 -- 18 -- 18  18  - - 3 - - 6
-- -- -- -- -- --  19  - - 3 - 5 6
20 -- -- 20 20 --  20  - - - - - 6
-- -- -- -- 21 --  21  - - - - - 6
22 22 22 -- 22 --  22  - - - - - 6
-- -- 23 23 -- 23  23  - - - - 5 6
-- -- -- -- 24 --  24  - - - - 5 6
25 25 25 25 -- 25  25  - - - - 5 6
26 26 -- -- -- 26  26  - - - - 5 -
-- -- 27 27 27 --  27  - - - 4 5 -
28 -- 28 -- -- 28  28  - - - 4 5 -
29 29 -- 29 29 --  29  - - - 4 - -
-- -- -- -- --  30  - - - 4 - -
-- -- 31 -- --  31  - - - 4 - -
32 -- -- --  32  - - - 4 - -
-- 33 -- --  33
34 -- 34 --  34
-- -- -- 35  35
-- 36 36 --  36
37 -- -- 37  37
-- -- --  38
39 -- 39  39
-- 40 --  40
41 -- --  41
    42 --  42
    43 43  43
        --  44
        45  45
        --  46
        47  47
-----
IUBFF RRLDR MBMLH RLMDI GFTEN
-----

```

Note that in this example we use the default machine setup (check with **F10**) with default wheel labeling, wheels 2 to 6 advanced by resp bar 1 to 5, both options checked, and letter **X** as replacement for a space.

The key settings are the internal pin and lug settings of the BC-52. These are changed normally every 24 hours. The position of the six wheels at the beginning of the message is called the message key. This message key is a

crucial part of the cryptographic settings of the machine and must be unique for each encrypted message, to make optimal use of the key variations. If the same message key is used for many different messages this increases the amount of statistical information for a cryptanalytic attack on the message. We must encipher the message key for each message in order to transmit it in a secure way.

Selecting the Message Key and Trigram

We start by creating 12 random letters. People tend to create patterns when they select random letters. They may select neighboring keys on the keyboard, repeat sequences or use initials. Therefore a little procedure is used to ensure the randomness of the letters.

Make sure the BC-52 is in Cipher mode. The start position of the 6 wheels are set to a random position and 12 random letters are entered on the keyboard. The resulting output are 12 good random letters which are splitted in 2 groups of 6 letters.

For our example we assume the random sequence is DKNWQL MOXZVT XXH

The first group of 6 letters is used as start position to encipher the second group, which is the actual message key for the message. After these groups an indicator of 3 letters, also called trigram, is given. This trigram refers to a secret table or indicated a special procedure. There are many different ways to use this trigram. It can be used to set the offset of the printwheels, identify the enciphering method and/or used key. In our example we use the trigram XXH to indicate a printwheel offset H.

Note on the message key: the procedure with the enciphered message key, as described above depends entirely on the secrecy of the machine settings. If these settings are compromised unauthorized persons can decipher the message. Some procedures use a second secret table with message keys. Both sender and receiver use a system to agree on one of the message keys of the table. This can be done by transmitting a random selected number that corresponds with a message key, or in a small message center by using the message keys one by one. If the machine settings are compromised and the message key table is kept secret, there are still 10,779,215,329 possible startpositions (on the CX model) unknown to the attacker.

Enciphering the Message Key and Trigram

We set the 6 wheels of the BC-52 from left to right in the positions D, K, N, W, Q and L. (if a given letter is not available on the wheel labeling we set that wheel in the first following position). Make sure that there's no printwheel offset (A=A).

Next, we encipher the second group of 6 letters and the trigram. With the given key settings this should result in ODUMIQ MIB.

Finally we can encipher the complete message with the message key MOXZVT, being the second groups of 6 letters, as start position of the wheels and printwheel offset H (click upper or lower half of the alphabet knob until A=H is displayed). In our example we must encipher this message:

ENEMY TANK DIVISIONS ARE MOVING TOWARDS BORDER X TAKE DEFENSIVE ACTION

With the given internal settings, the message key MOXZVT and printwheel offset A=H this results in:

XKHLB LIEMO CCSGW OPXHJ XXRWP
LRBXP CEEKB LIUTD FWKEU TIWED
TBVDX QDUYE KRNNE QTFJT

Message Format

We can now start composing our message. The first 6 letters are the 6 letters, used as start position to encipher the message key. The next 6 letters are the enciphered version of the message key. After these groups the enciphered trigram is given. The result is arranged in groups of 5 letters and followed by the actual message.

The complete message:

DKNWQ LODUM IQMIB XKHLB LIEMO
CCSGW OPXHJ XXRWP LRBXP CEEKB
LIUTD FWKEU TIWED TBVDX QDUYE
KRNNE QTFJT

Deciphering the message

To decipher the message the receiver must first retrieve the message key and trigram. He sets the 6 wheels of his BC-52 in the startpositions **DKNWQL**, the first 6 letters of the message. The BC-52 must be in Cipher mode and not Decipher mode (otherwise an **X** in the message key would be replace by a space)! Next, he keys in the next 9 letters **ODUMIQ MIB** to retrieve the message key **MOXZVT** and the trigram **XXH** which indicates the offset in our example. Finally he can set the retrieved message key **MOXZVT** as start position, adjusts the printwheel offset to **H**, and sets the machine in Decipher mode to decipher the rest of the message. Note that without the correct key settings on his BC-52 he will never be able to retrieve the message key nor trigram.

Congratulations on enciphering and deciphering your first message with the BC-52 cipher machine!

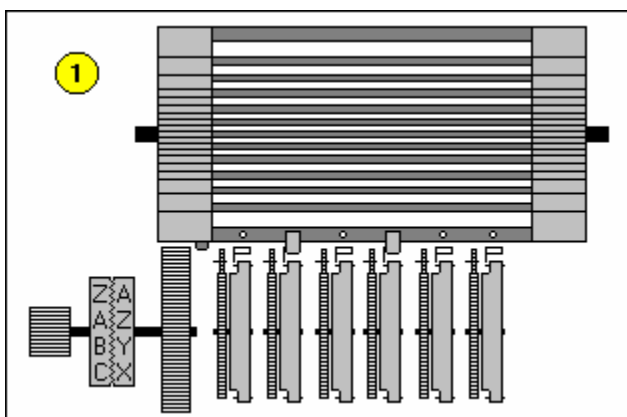
Technical details on the BC-52

General Description

The Hagelin BC-52 is a combination of the C-52 with the B-52 electrical keyboard. This machine, developed and manufactured by Hagelin Cryptos (Crypto AG), is an all mechanical drum-and-lug cipher machine. Both plain and cipher text are printed on a gummed paper ribbon. The C-52 is detachable from the keyboard base and can be operated manually. In that case the operator turns the letter knob until the desired letter appears on the letter dial and pushes the handle on the right downwards. The Cipher mode enciphers the letters in groups of five letters. In Decipher mode there are no groups and deciphered letters **X** are replaced by spaces. When the counter is reset, this also will reset the group counting of the print mechanism.

Encryption Principle

A double printing wheel has one normal and one reciprocal alphabet. Encryption is performed by setting the normal alphabet wheel to a plain letter and than add a number of steps. In the new position of the print wheel the cipher text is printed with the reciprocal print wheel. The pseudo random number of steps is determined by the settings of the lugs on the drum and the pins on the wheels (see fig 1).

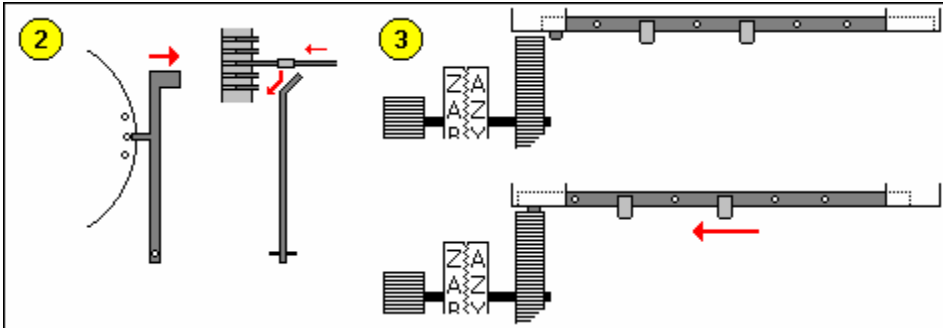


The Drum and Lugs

Inside the BC-52 there is a drum that contains 32 bars. Small lugs can be affixed on one or more of the six positions on each of these drum. When the operator turns the handle or uses the keyboard the drum will make a complete revolution.

In front of the drum there are 6 pinwheels, all having a small pin for each position of the wheel. This pin can be positioned to the left or the right. Each wheel has a guide arm with a slope end that will move towards the drum if activated by a pin.

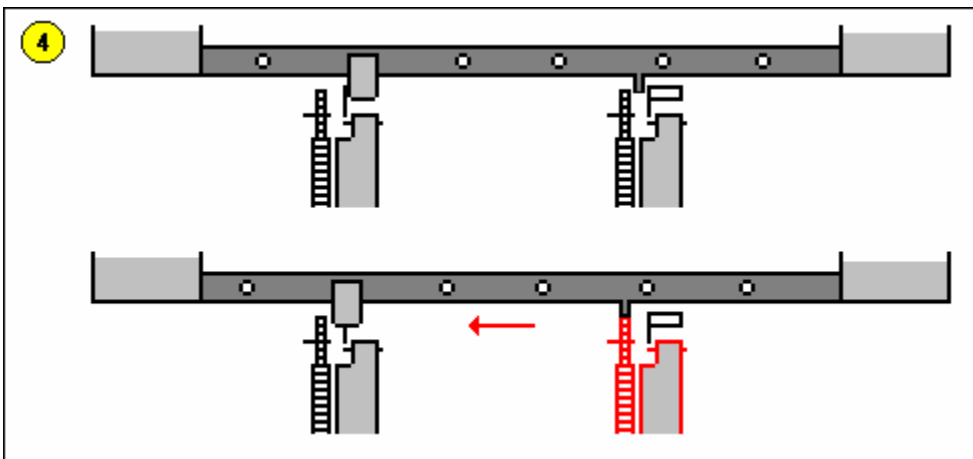
During the revolution of the drum some of the lugs on the bars will contact an active guide arm. These bars are forced to slide to the left (see fig 2). The left side of the drum works as a variable toothed gear. Each bar that is slid to the left is one more theet on the drum (see fig 3). The drum will turn the gear from the printing wheel. Therefore, the number of steps that are added to the plain letter is the number of teeth on the drum.



Wheel movement

The movement of the 6 wheels also depends on the settings of the lugs on the drum and the pins on the wheels. If we number the wheels from left to right the first wheel steps on each cycle of the drum. The other 5 wheels are moved by 5 special advance bars. Each of these bars are identical to the other bars but also have small fixed pins. If a lug on such bar contact an active guide arm it will be forced to slide to the left, just as a normal bar. However, in the case of advance bars, the little fixed pin will now be positioned right in front of a small gear wheel, which steps the pinwheel one step further.

An example (see fig 4): The current pin on wheel 2 is in the active position and on the drum the advance bar for wheel 5 has a lug in position 2. The moment the drum revolves, that lug will contact the guide arm from wheel 2, pushes the bar to the left and lets the small fixed pin advance wheel 5.



The advance bars are responsible for the irregular movement of the wheels and are critical for the cryptographic security of the machine. When in the following example setup all 5 bars have passed the guide arms, an active pin on wheel 1 will move wheels 2, 3, 4, 5 and 6, because there is a lug in position 1 on each of the 5 bars. A pin on wheel 2 will move wheels 3, 4, 5 and 6. A pin on wheel 3 will move wheels 4, 5 and 6, and so on. This way, all wheels will move most of the time and will stop once in a while, depending on the pins on the wheels. This creates a highly irregular wheel movement sequence.

```

B
A      LUGS
R  1  2  3  4  5  6
-----
1  1  -  -  -  -  -  moves wheel 2
2  1  2  -  -  -  -  moves wheel 3
3  1  2  3  -  -  -  moves wheel 4
4  1  2  3  4  -  -  moves wheel 5
5  1  2  3  4  5  -  moves wheel 6

```

To show the importance of the selection of lugs on the advance bars we will give below an example of bad lug setting. The problems are obvious. Wheel 2 will only move if there is an active pin on wheel 1. Wheel 3 only moves if there is an active pin on wheel 3 and so on. This results in very slow rotation of the last wheels, limiting the pin variation and therefore weakening the security.

```

B
A      LUGS
R  1  2  3  4  5  6
-----
1  1  -  -  -  -  -  moves wheel 2
2  -  2  -  -  -  -  moves wheel 3
3  -  -  3  -  -  -  moves wheel 4
4  -  -  -  4  -  -  moves wheel 5
5  -  -  -  -  5  -  moves wheel 6

```

There are different versions of the C-52. Some have fixed advance bars, spread all over the drum instead of the normal first 5 bars. On some machine versions the advance bars are detachable and their order can be changed.

Printwheel Offset

To add a complication to the encryption it is possible to use an offset on the printwheel. This is done by pulling the dial knob away from the machine, thus disconnecting plain and cipher print wheels from each other, and then turn the dial a given number of steps. When for example enciphering the letter H with an offset of 2 letters the machine will actually encipher the letter F.

Copyright

THIS PROGRAM IS FREWARE AND CAN BE USED AND DISTRIBUTED UNDER THE FOLLOWING RESTRICTIONS: IT IS STRICTLY FORBIDDEN TO USE THIS SOFTWARE OR COPIES OR PARTS OF IT FOR COMMERCIAL PURPOSES, OR TO SELL, TO LEASE OR TO MAKE PROFIT FROM THIS PROGRAM BY ANY MEANS. THIS SOFTWARE MAY ONLY BE USED IF YOU AGREE TO THESE CONDITIONS.

DISCLAIMER OF WARRANTIES

THIS SOFTWARE AND THE ACCOMPANYING FILES ARE SUPPLIED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, WITH RESPECT TO THIS PRODUCT, ITS QUALITY, PERFORMANCE, MERCHANTABILITY, OR FITNESS FOR ANY PARTICULAR PURPOSE. THE ENTIRE RISK AS TO IT'S QUALITY AND PERFORMANCE IS WITH THE USER. IN NO EVENT WILL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES RESULTING OUT OF THE USE OF OR INABILITY TO USE THIS PRODUCT.