# TSEC/KL-7 SIMULATOR 5.0 MANUAL

Ed. 501-07

## About the KL-7 Simulator

The TSEC/KL-7, codenamed ADONIS and POLLUX, is an off-line rotor cipher machine, developed in the late 1940's by the U.S. Armed Forces Security Agency (AFSA) and introduced by the newly formed National Security Agency (NSA) in 1952. It's a true Cold War era crypto machine that served in several NATO countries. The KL-7 was the first tactical cipher machine to use electronics (vacuum tubes).

This software is an accurate simulation of the KL-7 cipher machine and provides an authentic look and feel with its hands-on approach. The simulator's switches, keys and levers are operated in exactly the same way as the real machine and even produce the actual KL-7 sounds. The development of this simulator is based on the most recent declassified information and research.

The simulator is a tribute to the ASA and AFSA engineers and cryptologist who developed the KL-7 and to the men who worked with this machine. With most surviving KL-7's inaccessible or stripped from their rotor wirings, this simulator is the only remaining way to actually work with this beautiful machine, and the simulator serves as an attempt to keep the KL-7 machine and its history alive.

Image © Crypto Museum

**Important notice**: This simulation is developed for educational and historical research purposes. Today, the KL-7 is by no means a secure way to encrypt and protect information. The key settings of the simulator are saved in a small file that can be accessed and read by anyone who has access to the computer, either directly or remotely.



## Content

# 1. Operating the Simulator


The user interface of the KL-7 simulator software is developed to mimic the mechanical, electrical and cryptographic properties of the real KL-7 as much as possible. The hands-on approach gives you the chance to operate the KL-7 as an operator would do in real life. We start with a brief description of what the machine can do and then explain how to use all its nuts and bolts.

You will notice a little hand as mouse cursor when you move over switches, machine keys or places that activate some function. All functions are called with the left mouse button, but can also be performed from the PC keyboard. Once you have learned how to work with the KL-7, you can decrypt two messages, related to the Cuban missile crisis, that are found in appendix A.

### What is the KL-7

The TSEC/KL-7 is an offline electromechanical rotor cipher machine. The KL-7 encrypts (also called encode or encipher) readable plaintext into unreadable ciphertext, and decrypts (decode, decipher) the ciphertext back into plaintext. The operator keys in his plain or ciphertext on the keyboard and the result is printed on a paper tape. The encryption process is controlled by the internal settings of the KL-7. To correctly encrypt or decrypt messages, the operator has to select the appropriate rotors cores, their order, the position of the alphabet rings, the notch rings and their position on the rotors. This so-called key setting was usually performed once a day, according to a key list.

### The Simulator Window

The simulator uses a hands-on interface, allowing the user to operate the machine in exactly the same way as in real life. Of course, this virtual machine has some additional features which are not available on a real machine. There are four icons in the top-right corner of the simulator window. From left to right, these are Sound (on/off), the Help file (called with F1), the About window and the Exit icon to leave the KL7 simulator.

### The Selector


The selector or main switch is operated by clicking with your mouse on the left or right half of the selector, or by using the LEFT-ARROW or RIGHT-ARROW on the PC keyboard.

The main selector has four positions:

- **O** – Off Position: the machine is shut down completely and the keyboard keys and manual rotor movement don't function. Most features, both real life and software, are not accessible in this state.
- **P** – Plain: the keyboard and printer are activated. The text you type is printed directly onto the paper tape without encryption. The rotors don't move during typing. Only in this selector position you can manually preset the rotor positions, the so-called rotor alignment.
- **E** – Encryption: the keyboard, rotors and printer are activated. The entered text is encrypted and the ciphertext is printed in five-letter groups onto the paper tape. Note that the rotors perform one step (controlled by the notch rings) when you switch from "P" to "E" mode or from "E" to "P" mode. More about this in the chapter 2.
- **D** – Decryption: the keyboard, rotors and printer are activated. The entered text is decrypted and the plaintext is printed onto the paper tape. The Decrypt mode only accepts letters.

## The Keyboard


The keyboard contains the complete alphabet, the FIG (figures), LET (letters), RPT (repeat) and SPACE keys. You can click all these keys with the mouse. In FIG mode, the top row letters QWERTYUIOP represent the figures 1234567890. The neon indicator lamp, located just above the centre of the keyboard, will light up when the machine is in the FIG mode.

None of the keys will work when the selector is in the "O" position. In "P" and "E" position you can use letters, figures and spaces. In "D" mode you can only enter letters.

You can also use the PC keyboard to operate the KL-7. Use the **UP-ARROW** for FIG and **DOWN-ARROW** for LET or press the **SHIFT** key to switch between LET and FIG. In FIG mode, you can either use the numbers on your numeric key pad or the top row of your keyboard.

On the real KL-7, the RPT key is pressed down, together with a letter, to repeat that character. We don't have two mouse pointers on the computer screen and this function is therefore replaced by holding down the desired letter on your PC keyboard.

## The Rotor Cage – Key Settings


The rotors and notch rings inside the rotor cage control the KL-7 encryption process. It is impossible to decrypt and read a message without the proper so-called key settings or crypto key. Click on the rotor cage or use **F9** to activate the Key Settings window. The key setting comprises the following five variables:

- **8 rotor cores** - chosen from a set of 13 cores, labelled "A" through "M"
- **7 alphabet rings** - attached to the cores and set against markings 1 to 36 on the rotor core
- **7 notch rings** – attached to the cores and chosen from a set of 11, labelled "1" through "11"
- **Setting of the 7 notch rings** – set against the markings A to Z+ on the alphabet ring. 10 blanks on the alphabet ring are defined in the key sheet by the previous letter and a "+" sign (e.g. after M comes M+).
- **The wide ring** – always mounted to the 4th core and set in any of 36 positions, marked 0-36 on the core


After finishing the key settings, use the "Close" button to return to the KL-7 main screen.

With the "Zeroize" button you can erase the current key settings and clear the paper tape, KL-7 clipboard and the Auto Typing window. Note that this affects only the settings in the program and does not delete any saved files!

**Tip**: to speed up the adjustment of the key, it's not necessary to open each of the 30 drop lists. Use the **TAB** key to go to the next drop list. For letters, type that letter on the PC keyboard or, in case of a letter with a "+" sign, type the letter twice. For figures, type the number 1, 2 or 3 multiple times to get the 10s, 20s or 30s, and for the other digits, just type that digit. Use the **TAB** key to proceed to the next drop list. This way it takes only little time to set a key.

## Saving the Key Settings

You can save and open the KL-7 key settings in a small file with the ".txt" format on a location, chosen by the user. The file name appears at the top of the KL-7 and in the key settings windows once a key file has been saved or opened. The user is prompted to save any changes in the key settings when closing the program.

On start-up, the default "zeroized" settings are always loaded into the KL-7. By doing so, the location of the last saved or loaded key files is not disclosed.

### The Rotor Alignment

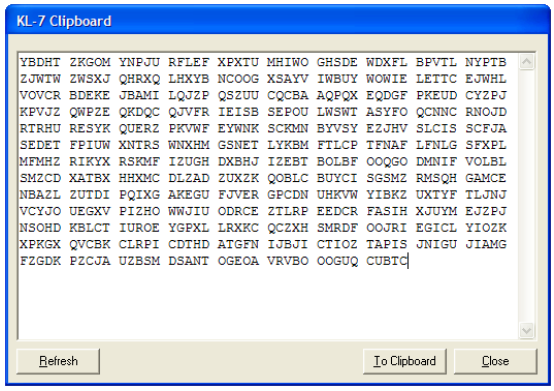

The rotor cage contains the 8 encryption rotors. The position of 7 rotors is visible in the little windows. The 4th rotor doesn't move and therefore has no window to observe its position.

Each new message requires a new random start position of the rotors, the so-called rotor alignment. This procedure is explained in chapter 2.

To adjust the rotor alignment, set the selector in the "P" position and press the **black lever** underneath the desired rotor. Click the lever once to advance the rotor one step or click and hold down the mouse button to cycle the rotor automatically. You can also use the **TAB** key to call the **Set Mode**. In Set Mode, the letter "S" will appear on top of a black lever and you can enter the desired rotor alignment on your PC keyboard. This advances the rotor directly to the desired position and the next-right rotor comes in the Set Mode. Press **TAB** multiple times to change rotor selection and use the **ESC** key to abort the Set Mode. You can memorize the current rotor alignment with the **INSERT** key and recall these settings later on with the **HOME** key. Alas for the KL-7 veterans, the practical Set Mode and memorized alignment were not available on the real KL-7.

Note: the paper tape advances one step on each movement of the rotors, during encryption and when adjusting the rotor alignment (due to the mechanical design). Therefore, the paper ribbon should be torn off (**DEL**) after finishing the rotor alignment.

### The Clipboard



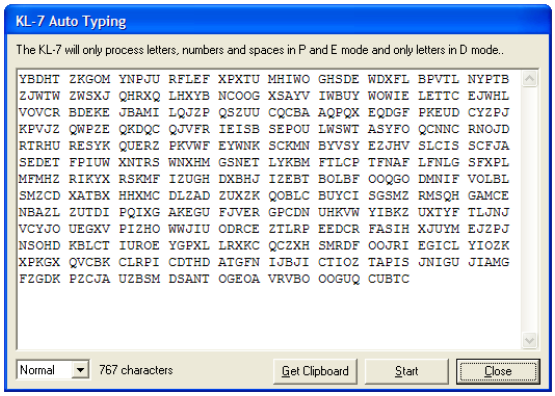

The machine output is displayed on the paper tape underneath the machine. To facilitate the reading and processing of the machine output there is a clipboard window. Click the paper tape or use the **F5 key to** call the clipboard window.

Use the "To Clipboard" button to send the text to the clipboard. You can edit the text before sending it to the clipboard. If you made a mistake during editing, you can recall the original machine output by using the "Refresh" button.

### The Auto Typing Function

To speed up the processing of large pieces of text (max 10,000 characters) you can use the Auto Typing function. Click the power cord, located at the right of the simulator keyboard or use the **F6** key to call the Auto Typing window. The Auto Typing function is not available when the KL-7 selector is in the "O" position.

You can type your text directly into the textbox or load the clipboard content with the "Get Clipboard" button. In the bottom left corner you can set the speed of the autotyping. "Slow" has a speed of 0.5 character per second, suitable for demonstration purposes. "Normal" is about 4 characters per second, which represents a very skilled operator. In KL-7 terms, this is about the speed of light (ask old KL-7 operators). "Fast" processes the text immediately without any delay function.




Auto Typing will automatically switch between LET and FIG if digits are found in the text. If your text is finished, use the "Start" button to start the Auto Typing. Don't forget to adjust the rotor alignment and to set the selector in the "E" or "D" position before using the Auto Typing function!

You can interrupt Auto Typing with the **ESC** key. If you made an error in your machine setup or want to adjust some settings, you can always close the Auto Typing window, correct the machine settings and re-open the Auto Typing window. The entered text remains in the textbox, even when the window is closed.

**Important**: In "P" and "E" mode, only letters, figures and spaces are processed. All other characters, punctuations and line feeds in the text box will be ignored. If used, they are removed and could cause words to join together. Avoid them in the text box. In "D" mode the program only processes letters.

**Letters, Figures and Spaces**

The designers devised a unique solution to encrypt 26 letters, FIG, LET and the space bar into a ciphertext that contains only 26 letters: the additional characters "piggy-back" on the least frequent letters "J", "V", "X", "Y" and "Z", meanwhile ensuring excellent readability. Nonetheless, this system has a small effect on the text after being processed.

The KL-7 test sentence shows the changes that occur. The first sentence is the text before encryption and the second sentence is the same text after it is decrypted back into plain text:

```
THE 236TH QUICK RED FOX JUMPED 780 TIMES OVER THE 1459 LAZY BROWN DOGS
THE 236 TH QUICK RED FOX YUMPED 780  TIMES OVER THE 1459  LAXY BROWN DOGS
```

Only the seldom used letters "J" and "Z" are affected and we still have an excellent readability. More about the piggy-back system is found in the technical details section later on in this paper.

Note: plaintext, encrypted by the user, may result in a slightly different ciphertext than the same text, encrypted with the Auto Typing function. The user could, for instance, type **ABC[FIG][SPACE]123** while Auto Typing always switches to FIG just before a digit and to LET just before letters, processing the same plaintext as **ABC[SPACE] [FIG]123**.

**The Counter**

The KL-7 has a character counter, located above the keyboard, that keeps track of amount of encrypted or decrypted characters. The counter does not count in Plain mode. Click the lever on the right of the counter to reset it to zero.


**Controls Overview for the KL-7 Simulator**

| Action | Simulator | PC Keyboard |
|---|---|---|
| Selector O > P > E > D | Right half selector | RIGHT-ARROW |
| Selector O < P < E < D | Left half selector | LEFT-ARROW |
| Letters | Keys A through Z | A through Z |
| Space | Space key | SPACE |
| Figures | Keys Q(1) through P(0) | 0 - 9 on num. keypad or keyboard top row keys |
| Switch LET/FIG and FIG/LET | LET and FIG keys | UP-ARROW and DOWN-ARROW or SHIFT * |
| Key Settings | Click rotor cage | F9 |
| Adjust rotor alignment | Black lever under rotor | Not available |
| Adjust rotor alignment quickly | Not available | TAB + any letter on keyboard (use ESC to quit) |
| Adjust all rotor to "A" | Not available | Open Key Settings (F9) and close Key Settings |
| Memorize rotor positions | Not available | INSERT |
| Recall rotor positions | Not available | HOME |
| Delete paper tape | Not available | DELETE |
| Reset Counter | Click counter lever | Not available |
| Clipboard | Click paper tape | F5 |
| Auto Typing | Click power cord | F6 |
| Sound On/Off | [speaker] icon | Not available |
| Help File | [?] icon | F1 |
| Exit the simulator | [x] icon | F12 |

* Depressing the SHIFT key five successive times could cause the Sticky Keys window to appear. This is a Windows™ operating system option to facilitate the use of the SHIFT and CAPS LOCK keys. Although normal use of the KL-7 simulator will never required the SHIFT key to be pressed five times in a row, you might run into this window. In such case, simply use the ESC key or select Cancel to close the Sticky Keys window.

# 2. Encryption and Decryption

We will explain the encryption and decryption procedures with the help of two easy step-by-step examples. However, before we can encrypt or decrypt messages, we must adjust the internal settings of the KL-7, the so-called crypto key. The KL-7 key sheet contains a list of keys, each valid for a period of 24 hours. The sheet lists the choice of rotor cores, the setting of the alphabet rings, the choice of notch rings and their setting.

**The Key Settings**

The ADONIS key sheet format, as documented in KAO-41C/TSEC

| POSITION IN MACHINE 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | | |
|---|---|---|---|---|---|---|---|---|---|
| D A T E | C O ALPH RING E SET | C O ALPH RING E SET | C O ALPH RING E SET | C O WIDE R RING E SET | C O ALPH RING E SET | C O ALPH RING E SET | C O ALPH RING E SET | C O ALPH RING E SET | | |
| | NOTCH RING& SET | NOTCH RING& SET | NOTCH RING& SET | | NOTCH RING& SET | NOTCH RING& SET | NOTCH RING& SET | NOTCH RING& SET | 36-45 LTR CHECK GRP | SYS INDIC |
| 31 | E 4 5-C | H 28 10-M+ | F 4 6-E | L 16 | I 9 7-B | A 32 1-E+ | G 8 8-Y | B 11 3-K | ASMTH/ISXPI | 28604 |

Since the real sheet is only readable when printed in landscape, here a more convenient format for our examples.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| ADONIS 27 OCT 1962 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| ROTOR CORE | E | H | F | L | I | A | G | B |
| ALPHABET RING SET | 04 | 28 | 04 | 16 | 09 | 32 | 08 | 11 |
| NOTCH RING | 5 | 10 | 6 | | 7 | 1 | 8 | 3 |
| NOTCH RING SET | C | M+ | E | | B | E+ | Y | K |
| 36-45 LETTER CHECK | ASMTH ISXPI | | | | | | | |
| SYSTEM INDICATOR | 28604 | | | | | | | |
| BASIC ROTOR ALIGNMENT* | X | E | G | | B | V | E | Q |

**Notes**: The ADONIS system indicator consisted of five digits or five letters, POLLUX always used letters as system indicator. POLLUX uses the letter “A” instead of “L” for the 36-45 letter check. The basic rotor alignment* is *not* used in the ADONIS or POLLUX procedures.

Click the KL-7 simulator rotor cage or use F9 to open the Key Settings window. Adjust the settings according to the key list above. The System Indicator identifies the crypto system and key, used for that particular message. This system indicator should never be encrypted and skipped during the encryption and decryption process.

With the 36-45 letter check we can verify the settings. With the machine in “P” mode, set all rotors in the “A” position (use the TAB key to enter the Set Mode). Next, switch to “E” mode, reset the counter, clear the tape (DEL) and type the letter "L" 45 times. The last two code groups should match the letter check on the key list.

**The Message Indicator**

Each new message requires a new and unique random start position of the rotors at the beginning of the encryption, the so-called message rotor alignment. This rotor alignment, visible through the little windows of the rotor cage, is crucial for the security of the message. Using the same rotor positions for different messages leads to patterns that can be exploited by codebreakers to break a message. The use of random rotor alignments creates a unique ciphertext for each message, even when key settings and plaintext are identical.

Therefore, we need a way to select a random rotor alignment and convey this secret information to the receiver. This is where we use the Message Indicator, a randomly chosen group of letters that is sent along with the message, in plain text and spelled-out. This message indicator is encrypted on the KL-7 and the resulting letters are used to set the rotor alignment prior to encryption. The receiver also encrypts the received message indicator on his machine and also uses the resulting letters to set his rotor alignment for that particular message. This way, the actual rotor alignment is never revealed in the message.

There are several methods to communicate the message indicator. We will demonstrate two different message indicator systems with two practical examples. The first method is prescribed in the recently declassified crypto document KAO-41C/TSEC “Operating Instruction for TSEC/KL-7 – ADONIS Operation” (sections 2000 to 3005). The second example uses a pre-determined basic rotor alignment to encrypt the message.

**Important**: all following examples are typed by hand. The use of Auto Typing could result in a different ciphertext (see Auto Typing section earlier in this paper). Always start in "P" before going to "E" ‘or before going to "D".

**A first example**, following KAO-41C/TSEC, uses a random five-letter message indicator. The random message indicator is encrypted and the result is used as rotor alignment, prior to the encryption of the actual message. Carefully follow the steps, shown below, to avoid compromise of the message security!

For our example message, we selected the random message indicator "ELXNO".

1. Switch the KL-7 to “P” mode
2. Set “AAA-AAAA” as rotor alignment (use the TAB key for Set Mode)
3. Switch to “E” (some rotors will move one step) and press DEL to clear the tape
4. Encrypt message indicator "ELXNO". The resulting encrypted indicator should be "BHLDO".
5. Switch back to “P” mode
6. Set "BHLDOBH" as message rotor alignment by repeating the first two letters at the end
7. Switch to “E” mode, press DEL to clear the paper tape and reset the counter
8. Encrypt the plaintext message "TOP SECRET MESSAGE 123 TEST". Any incomplete final group should be completed by one space, followed by enough random letters to complete the five-letter code group.

The result should be: `GOATJ ZPFJZ RGDET FKCSB TCMTD XTQLP`

The complete message, including the system indicator, the spelled-out (NATO alphabet) message indicator, the encrypted text and the system indicator repeated at the end:

```
28604 ECHO LIMA XRAY NOVEMBER OSCAR
GOATJ ZPFJZ RGDET FKCSB TCMTD XTQLP 28604
```

The system indicator “28604” identifies the ADONIS crypto system and used key to the receiver. He switches to "P" mode, sets "AAA-AAAA" as rotor alignment and switches to "E" mode (not “D” mode). He encrypts the spelled-out message indicator "ELXNO" and again gets "BHLDO". He switches to "P", sets "BHLDOBH" as message rotor alignment, repeating the first two letters at the end, switches to "D" and decrypts the ciphertext.

In Appendix A you will find two fascinating messages, related to the Cuban missile crisis, to practice the decryption procedure. They use the KAO-41C/TSEC procedure as described above.

**A second example** is performed with the help of a daily basic rotor alignment (*) and a random seven-letter message indicator. This method is actually cryptographically more secure because the basic rotor alignment is a secret set of seven random letters, provided in the key sheet. At the end of the procedure, all seven rotors are aligned according to their own letter, derived from the seven-letter message indicator, rather than repeating the first two letter of the five-letter method. In this example we do not use a system indicator.

In our example, we use the random message indicator "ZEHOXTA".

1. Switch the KL-7 to “P” mode
2. Set the basic rotor alignment “XEG-BVEQ” as rotor alignment (use the TAB key for Set Mode)
3. Switch to “E” (some rotors will move one step) and press DEL to clear the tape
4. Encrypt message indicator "ZEHOXTA”. The resulting encrypted indicator should be “GUZBZXN”
5. Switch back to “P” mode
6. Set “GUZBZXN” as message rotor alignment
7. Switch to “E” mode, press DEL to clear the paper tape and reset the counter
8. Encrypt the plaintext message "TOP SECRET MESSAGE 123 TEST". Any incomplete final group should be completed by one space, followed by enough random letters to complete the five-letter code group.

The result should be: `ICQBJ MHWMR AWDSQ NOUCM UZMMZ QOWZP`

The complete message, including the spelled-out message indicator:

```
ZULU ECHO HOTEL OSCAR XRAY TANGO ALFA
ICQBJ MHWMR AWDSQ NOUCM UZMMZ QOWZP
```

The receiver of the ciphertext message switches to "P" mode, sets basic rotor alignment "XEG-BVEQ" as rotor alignment and switches to "E" mode (not “D” mode). He also encrypts the spelled out message indicator "ZEHOXTA" to retrieve the result “GUZBZXN”. He switches to "P", sets “GUZBZXN” as message rotor alignment, switches to "D" and decrypts the ciphertext.

Notice that the ciphertext of both examples is completely different, although we used exactly the same key settings and exactly the same message. Thanks to the message indicator, unique for each individual message, there is no relation between the two ciphertext messages.

**Message Format**

A common format for encrypted KL-7 messages was the so-called CODRESS format, documented in the publication ACP 127 (unclassified). In such messages, the full originator, all addressees and security classification were included in the encrypted text. These messages were always unclassified, although the coded groups might well contain secret information.

The CODRESS is composed as follows:

Line 1, prosign for priority (here R for Routine) and the routing indicator(s) of the destination station(s)
Line 2, routing indicator of the sending station, its serial number and the filing time
Line 3, priority again, followed by the message Date Time Group
Line 4, groups count of ciphertext groups only
Line 5, break
Line 6, system indicator and spelled-out message indicator
Line 7, the ciphertext, followed by the repeated system indicator
Line 8, break

The complete message format for the message from the first example would be

```
RR RABCDE
DE RFGHIJ 1234 8/1400Z
R 311300 DEC
GR 6
BT
28604 ECHO LIMA XRAY NOVEMBER OSCAR
GOATJ ZPFJZ RGDET FKCSB TCMTD XTQLP 28604
BT

NNNN
```

**Other Message Indicator Systems**

Many other solutions to communicate message indicators are possible and have been applied by the different countries that used the KL-7. Any good message indicator system should provide truly random message indicators that are used only once. They are either encoded with a secret table, encrypted with an unknown daily rotor start setting or both encoded and encrypted. The message indicator may be taken from a list and crosses after one-time use.

A most secure message indicator system is to use a table with both message indicators and their according random rotor alignments. In such system, the rotor alignment is completely independent from the key settings, used for the actual message. The sender takes a message indicator and rotor alignment from the table, uses the rotor alignment directly to encrypt the message and sends the according message indicator along with the message. One cannot derive the random rotor alignment from the random message indicator. Only the receiver who has the message indicator table can set the correct rotor alignment. Even with a KL-7 and the proper key settings, but lacking the secret indicator table, there are 8,031,810,176 possible combinations to try out (a big number in the pre-digital era). The only disadvantage is that enough indicator tables must be distributes beforehand to cover the expected volume of messages for a given time period.

Note that even a single error in the message indicator will result in completely unreadable text. Care has to be taken to avoid errors in conveying the message indicator to the receiver. The most convenient ways are to spell out the indicator letters or repeating the message indicator.

**Random Letters**

If you consider generating random letters for message indicators, you should remember that humans are a very bad source of randomness. If you decide to create random letters yourself anyway, you should use the following procedure to prepare a batch of random letters:

Select at random KL-7 rotor cores and their order, and set the alphabet rings, notch rings and their setting at random. Never use key settings that are used for actual message encryption. Set the selector to P, select random rotor alignment, switch to E and type some random letters on the keyboard. Take the resulting machine output and use that as random letters. Change the machine key settings regularly. The machine output breaks up any patterns you might have created, giving good randomness. Never use the letters you typed in, only the output!

# 3. Customizing your KL-7

During its service time, the rotors of the KL-7 were recalled and rewired regularly. Some rotors were rewired on a yearly basis on national or NATO level and some were to be sent to directly to NSA and rewired by NSA personnel only.

The KL-7 simulator software also allows you to rewire (customize) each individual rotor, define the notches on each notch ring, and define the wiring of the rotor cage contact plates. You don't need to define all of them. Non-defined items keep their default simulator specifications. The custom settings are activated on each start-up. To customize your KL-7, you simply create a text file called "custom.txt" and place it in the KL-7 program folder.

The following definitions can be used:

- "A=" through "M=" for the 13 rotor cores
- "P=" for the rotor cage contact plates (left and right are identical)
- "01=" through "11=" for the 11 notch rings

In the example below, a custom title bar text, the "C" and "L" rotors, the connections to the rotor cage plates "P" and two notch rings "04" and "11" are defined:

```
T=MY CUSTOM KL-7 SETTINGS
C=JCX8OW5QTYSI3PVU60BZHER42DM9KNGF7L1A
L=T9HEMYSIOW51AUZK0BF7L2N6DJCX3PVR4QG8
P=VER24D5QT6UH8YSIOJCX7L1AW0BZ3PM9KNGF
04=00110101000101100010011001010010011
11=01000110101011010000110000011001010
```

To customize a rotor, we define it by its rotor letter. Consider the rotor in front of you, as placed in the machine, with the pins on the left side of the rotor numbered from 1 to 36 (clockwise, seen from the left). Each of these pins is connected to a pin on the right side of that rotor, as given in the rotor definition. The 36 right side pins are defined as show in the table below.

Note that these letters and digits are absolutely not related to the keyboard or any cryptographic property of the machine and is just a convenient way to describe 36 different connections. Never use spaces within a definition!

| Def | 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 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Pin | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | **16** | **17** | **18** | **19** | **20** | **21** | **22** | **23** | **24** | **25** | **26** | **27** | **28** | **29** | **30** | **31** | **32** | **33** | **34** | **35** | **36** |

In the case of the "L" rotor in the example, pin 1 on its left side is connected to "T" (pin 20) on the right side. Pin 2 is connected to "9" (pin 35) on the other side and pin 3 is connected to "H" (pin 8). Of course, it is impossible to have two identical letters in your custom string as this would short-circuit two pairs of wires.

Note that, to define the rotor cage contact plates, we use a system that differs completely from the rotor definitions. This is because we don't have a 36 pin-to-pin wiring but 26 keyboard letters to the rotors and 10 re-entry wires from left to right plate. The 26 definition letters represent the corresponding letters, coming from the keyboard. The figures represent the re-entry wires that are connected directly from left to right plate. Pin 1 is aligned with the white index line on the cage (pins are numbered clockwise, seen from the left). In the example, the letter "V" from the keyboard is wired to contact plate pin 1 (also first pin of rotor when in A position), "E" is connected to plate pin 2 and "R" to pin 3. Figure "2" connects pin 4 from the left plate to pin 4 on the right plate.

To customize one or more of the 11 notch rings, labelled "01" through "11", we define them by their number, written out in two digits, the equal sign and the 36 notch values. The rotor stepping switch is active at value "1" and inactive at value "0".

The custom title bar is defined by the letter "T". The title bar will contain all characters after the equal sign up to the next line return. If desired, you can use extra spaces to align the title at the top of the simulator.

All definitions can be placed anywhere and in any order in the file, and you may add comments and additional information wherever desired. However, it is forbidden to use the equal sign (=) on other places than inside definitions. Save the text file with the filename "custom.txt" in the KL-7 program folder (with default installation, this should be "C:\Program Files\KL-7"). To return to the default settings you delete, rename or edit the "custom.txt" file. The program verifies all custom settings and, if an error is detected, the user is notified, all custom settings are discarded and the default simulator settings are loaded.

# 4. Technical Details

The TSEC/KL-7 is a classical off-line non-reciprocal rotor cipher machine with electro-mechanical and electronic components (vacuum tubes).The machine is powered by 24 Volts DC which drives a DC motor, which in turn drives a 400 Volts AC generator. The generator provides power to the electronics. The base unit is called KLB-7. The stepping unit, on top of the base unit, is designated KLA-7 and contains the stepping mechanism, the notch switches and supports the rotor cage. The detachable rotor cage KLK-7 holds 8 rotors with 36 pins on each side. Each individual rotor performs a substitution cipher. The output of the KL-7 is printed on a paper tape.

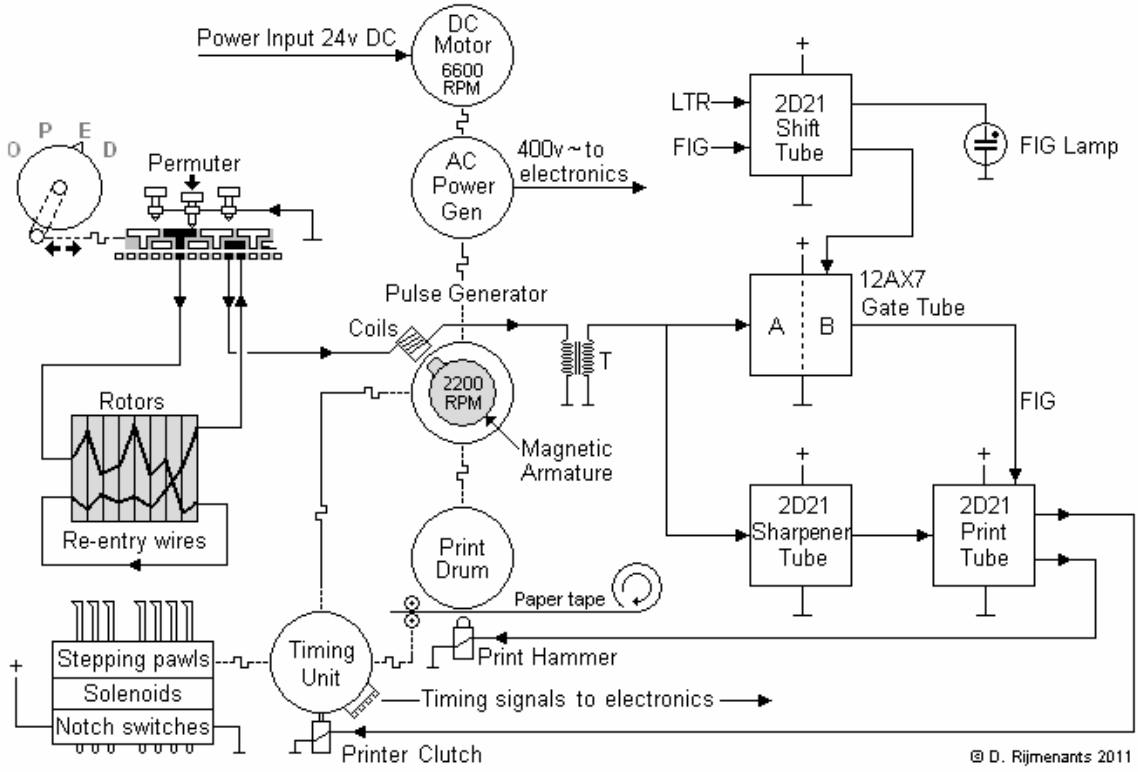
Each rotor has a wired core, an adjustable alphabet ring with and a white notch ring. The notch rings activate switches in the KLA-7 stepping unit that control the stepping of the rotors. The secret key settings comprise the selection and order of 8 cores from a set of 13, the position of the alphabet rings on the rotors, and the selection and position of 7 notch rings from a set of 11. The fourth – non-moving – rotor must be fitted with the special wide ring to fixate it in the rotor cage.

**The Signal Path**

The continuously rotating motor drives, through a 3 to 1 reduction gear, the pulse generator and print drum (both on the same axle). The pulse generator drives the timing unit through another reduction gear. The permuter board switches the direction of the keyboard signal through the rotors. The rotors scramble the signal on its way to the pulse generator. The pulse generator has a magnetic armature that rotates inside a double circle of 37 coils: 26 coils for A through Z, 10 coils for figures 1 through 0, and 1 coil for the space. All coils are arranged in a 360-degree pattern, in two separate rings. These coils produce the timing pulse for the print hammer and clutch.

Depressing a key will ground one of the pulse coils. When the rotating magnetic armature passes that grounded coil, it induces a pulse which is passed to the step-up transformer. The pulse is cleaned up by the sharpener tube and fed to the print tube, which activates the print hammer and the printer clutch. The pulse timing ensures that the print hammer hits the print drum when the proper character passes the hammer. The printer clutch causes the timing unit to perform one cycle. This cycle activates four cam switches for timing signals, advances the paper tape and provides mechanical power to step the rotors under control of the stepping logic.

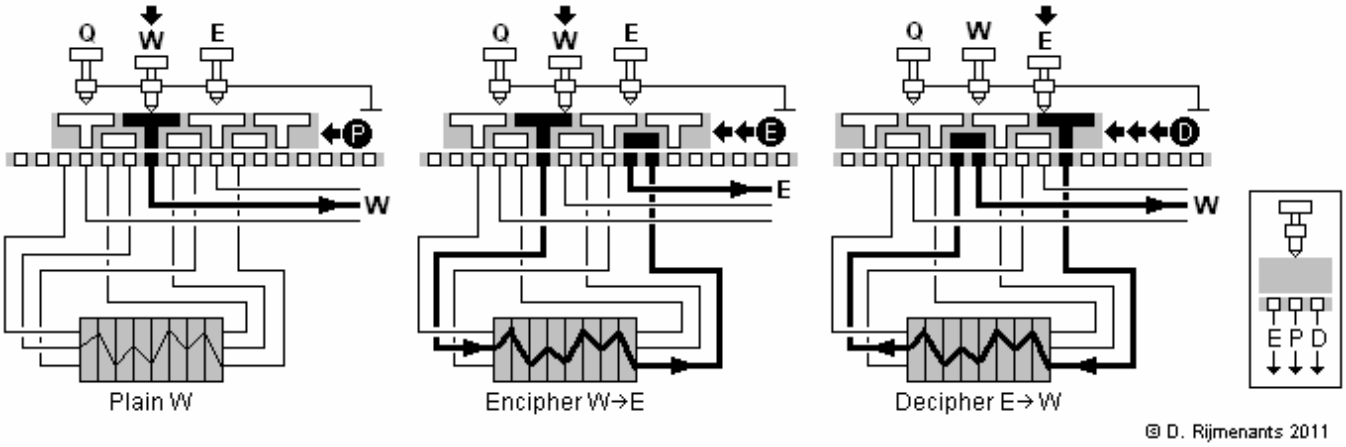
The keyboard top row letters have two pulse coils in series: a normal coil for the letter and a coil with a larger core and more windings for the corresponding figure. This combination of two coils produces a double pulse of which the second pulse has a higher amplitude. In FIG mode, the shift tube will switch the B gate of the gate tube, changing a grid on the print tube. This causes a slight delay and also requires a higher pulse to activate the print hammer, as provided by the double coils. The result is a slightly delayed activation of the print hammer, which prints the appropriate figure instead of its corresponding letter. The KL-7 holds a spare 2D21 and a 12AX7 tube.



**The Permuter Board**

The KL-7 has a simple and compact solution to swap the signal through the rotors: the complete keyboard is one large sliding selector, the so-called permuter board. The keys and wired contacts never move. Only the sliding contact board (with T-shaped contacts) moves from right to left between the keys and contacts. The spring-loaded keys are all grounded and pushing them down will ground the T-shaped contact plate at the top side of the permuter. Two rails on the permuter push the permuter board down onto the spring-loaded pins at the base of the keyboard, meanwhile ensuring easy movement of the board from right to left. The KL-7's selector has a pawl on its bottom that grasps into a vertical slot on the left of the permuter board. Turning the selector from left to right will move the permuter from right to left.

Each key has its own three connections underneath the permuter board, called (from left to right) "E", "P" and "D". In Plain, the depressed key is connected via the center of the T-shape and the "P" connection directly to the pulse generator. In Encipher mode, the depressed key is connected via the right part of the same T-shape and the "E" connection to the left side of the rotor pack. In Decipher mode, the depressed key is connected via the left part of the next-right T-shape and the "D" connection to the right side of the rotor pack. The use of two neighbouring T-shapes for each key enables the O-P-E-D sequence from right to left.




The above is a simplified example with 3-pin rotors. In reality, the KL-7 uses 36-pin rotors. Note that, to perform the piggy-back functions (see Letter and Figures section below), some E, P and D connections from “J”, “V”, “X”, “Y”, “Z”, SPACE, FIG and LET are swapped, and additional contacts on the permuter board switch some piggy-back wires and other control functions.

The permuter board also has a notched part in front of the printer mechanism. In the Encipher position, this cam pushes a pin into the printer mechanism causing the KL-7 to print a space after each fifth character.

**The Rotors**

Each rotor core has 36 contact plates on the left side that are wired in a scrambled fashion with 36 spring-loaded contacts on the right side (rotors as positioned in the rotor cage). The wiring performs a substitution encryption.

An alphabet ring, visible through the rotor cage window, is attached to the rotor core. The adjustable alphabet ring can be set by aligning it to the numbers 1 trough 36 on the side the core. This changes the position of the alphabet, relative to rotor wiring. The 36 positions on all alphabet rings are labelled as show in the table below. Note that 10 of the positions are left blank.

| Pin | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Label | **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** | |

There was a set of 12 rotors to choose from, later expanded to 13, labelled "A" through "M". The rotor core wiring is still classified and most surviving machines are either sanitized or their rotors are inaccessible. Moreover, its wiring was changed on a regular basis, in contrast to, for instance, the German Enigma where the wiring never changed during its whole service time (the cryptologists had learned their lessons).

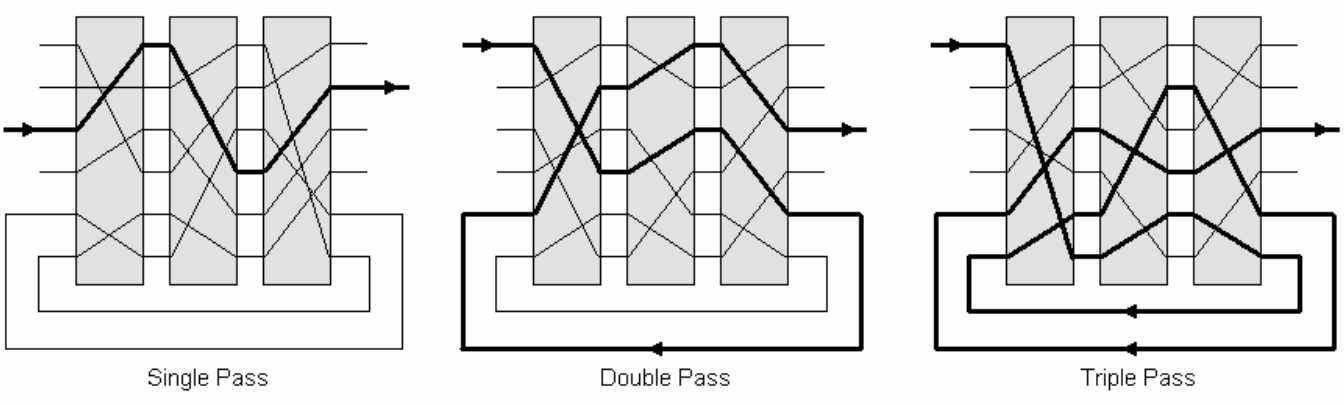
Therefore, there’s no other solution than to select our own wiring scheme for all rotors. Nonetheless, the cryptographic principles and strength of the machine are the same. The rotor wiring, as used in the KL-7 simulator, is found in Appendix B.

**The Notch Rings**

The KL-7 had a set of 11 white plastic notch rings, labelled 1 through 11. The notch rings are responsible for the highly irregular movement of the rotors. As part of the key settings, seven of them are attached to the seven moving rotors. The notch rings are aligned to one of the 36 positions of the alphabet ring. Since there are some blanks on the alphabet ring, these positions are marked with a plus sign in the key sheet (e.g. after M follows M+). The fourth (non-moving) rotor must carry the wide ring. The notches and cams on the rings control seven stepping switches in the KLA-7 stepping unit. These notch rings were also part of the key settings and still considered secret. As a result, the simulator uses its own ring settings. These are also found in Appendix B.

**The Rotor Cage**

The KLK-7 detachable rotor cage holds the eight rotors. The KL-7 uses a complex re-entry system that can cause multiple encryptions of a single character. When the signal leaves the exit rotor there are two possible situations: the signal is either passed immediately (through the permuter) to the pulse generator along one of the 26 wires, or it leaves the exit rotor on one of the 10 re-entry contacts. In the latter case, the signal is sent back to one of the 10 re-entry contacts at the entry rotor, to perform a new pass through the rotors. When the signal leaves the exit rotor again, the situation is repeated. Depending on the internal wiring and current position of the rotors, the signal performs one or more passes (theoretically up to 10 passes) through all rotors before leaving the exit rotor towards the pulse generator. This results in a most complex signal path that constantly changes in both number of passes and its way through the rotors.




Above is given a simplified example with 3 rotors with 6 wires each, of which 2 re-entry wires. In reality, we have 8 rotors with 36 wires each, of which 10 re-entry wires.

The “E and “D” connections of the 26 letters from the keyboard permuter are connected with respectively the left and right contact plates of the rotor cage. These rotor cage contact plates each have a circle of 36 pins, to connect the base with the rotors. The table below shows the wiring order between base and contact plate pins. The pins are numbered clockwise (seen from the left) and pin 1 (the permuter’s “Q” wire) is aligned with the white index stripe on the rotor cage. Both rotor contact plates are wired identically. The letter “Q” from the permuter is wired to contact plate pin 1, letter “P” to pin 2 and so on. The re-entry wires (1 through 0) are connected straightforward between left and right contact plate (1 to 1, 2 to 2, 3 to 3 ...).

| Base | **Q** | **P** | **0** | **N** | **F** | **C** | **3** | **Y** | **O** | **M** | **9** | **G** | **R** | **8** | **U** | **I** | **7** | **B** | **H** | **2** | **V** | **T** | **W** | **6** | **X** | **S** | **4** | **J** | **L** | **Z** | **5** | **D** | **K** | **E** | **A** | **1** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Plate | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 |

**The Printer Mechanism**

The KL-7 has a continuously rotating print drum, fixed on the same axle as the pulse generator. The print drum has the complete set of letters and digits on its circumference. The moment that the magnetic armature of the pulse generator passes a grounded coil, the sharpener and print tubes pass this signal to the print hammer and the printer clutch. The print hammer pushes the paper upwards against the print drum (with the inked ribbon between them) at the exact moment that the required character passes the print hammer.

The activation of the printer clutch causes the timing unit axle to perform a single cycle, providing mechanical power to advance both the paper and the rotors (adjusting the individual rotors manually also activates the clutch and therefore will also advance the paper). A pin, controlled by the permuter board, mechanically switches between continuously printing (plaintext) and five-letter groups with a space between each group (ciphertext). The paper roll is stored in the black circular casing between the motor block and the rotor cage.

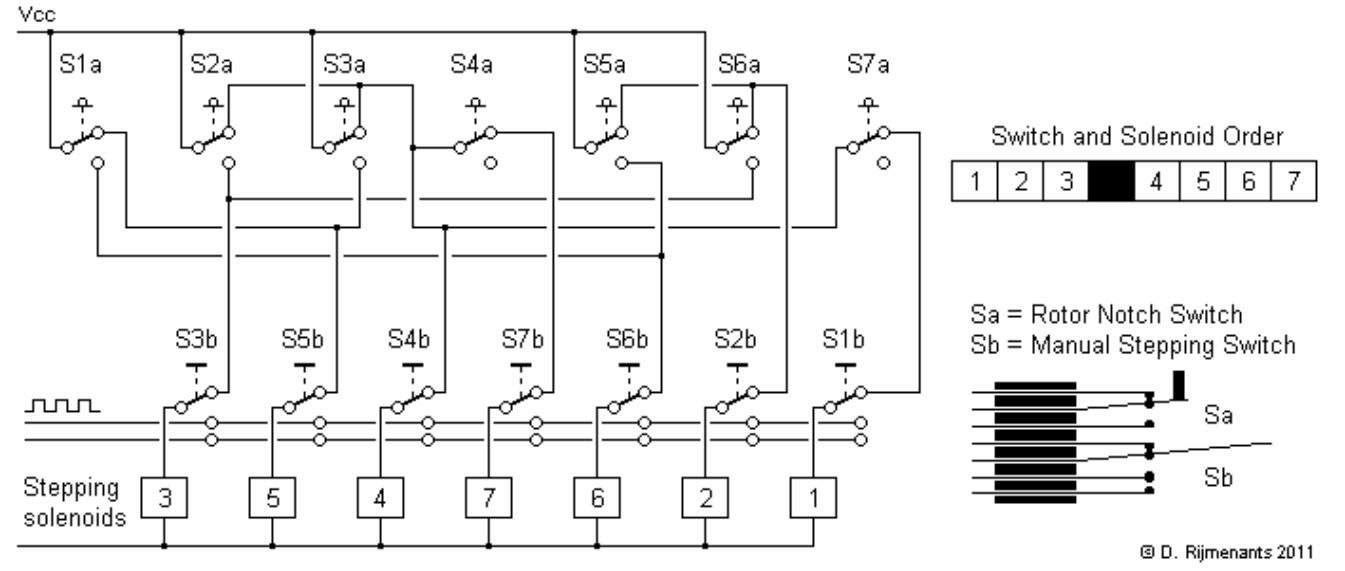
**The Stepping System**

The KLA-7 stepping unit holds the rotor cage and controls the stepping of the rotors. On the front of the cradle, there are seven levers to manually advance each individual rotor. Behind them are seven cams that read the notch rings of the rotors. These cams control the seven pile-up switches of the stepping logic, connected to the solenoids. In the middle of the cradle are the seven stepping pawls to advance the rotors. They are mechanically powered by the motor but controlled by the seven solenoids. At the rear of the cradle, there are eight locking pawls that prevent the rotors, currently not moving, from moving along with neighbouring moving rotors. The fourth locking pawl normally isn't used, but keeps the fourth rotor (with wide ring) in place when testing the rotors on a test axle without the rotor cage shell.

The stepping logic must avoid a situation where none of the rotors move, because this would cause the rotors to halt permanently. The KL-7 stepping logic ensures that at least three rotors move on each encryption cycle. When we consider the required cryptographic properties and observe the stepping of the rotors at different rotor positions, we can deduct the following logic table:

| Stepping Rotor | Notch Rings ( 0 = inactive & 1 = active ) |
|---|---|
| 1 | Ring 7 = 0 AND (Ring 2 = 0 OR Ring 3 = 0) |
| 2 | Ring 5 = 0 OR Ring 6 = 0 |
| 3 | Ring 2 = 1 OR Ring 6 = 1 |
| 4 | Ring 2 = 0 OR Ring 3 = 0 |
| 5 | Ring 1 = 0 OR Ring 3 = 1 |
| 6 | Ring 1 = 1 OR Ring 5 = 1 |
| 7 | Ring 4 = 0 AND (Ring 2 = 0 OR Ring 3 = 0) |

Knowing the operation of the machine's KLB-7 base unit and the pile-up switches, we can put this in a schematic which uses the available components:




All switches are shown inactive. Each switch is one single pile-up of the two parts Sa and Sb. Note that the order of upper switches is as actually positioned on stepping unit. The order of the lower switches and the solenoids is mixed to make the circuit diagram more readable. In reality, the lower switches and solenoids are placed from left to right according to its number. Of course, there are only 7 switches and solenoids because the fourth rotor is skipped.

Solenoids 2 through 6 are each controlled by two switches in OR logic: the solenoid is activated if at least one of the two switches has the appropriate state. Solenoids 1 and 7 are controlled by three switches and are activated if one switch is inactive AND at least one of two other switches is inactive. At least two solenoids are always active at any given moment. Switches S1b through S7b are used for the manual stepping (small levers in front of rotors).

On the KL-7, the stepping of a single rotor is controlled by two or three separate notch rings. Two notch rings can produce a maximum period (unique movement sequence) of 1,296 and three rings a theoretical maximum period of 46,656. This is for one single rotor. The combination of seven notch rings therefore provides a most complex stepping sequence.

**Letters and Figures**

The KL-7 can process 37 different characters: the letters A through Z, the figures 0 through 9 and the SPACE. The rotors, however, can only process 26 characters because 10 of the 36 connections, from and to the rotor cage, are hard-wired from output to input for the re-entry function (the 36 rotor contacts have no relation with the 36 letters and digits). Moreover, the encryption reduces the 37 characters to a 26 letters ciphertext.

To enable encryption of 37 different characters into letter-only code groups, the KL-7 uses a system, similar to the teletype code. Two signals, LET and FIG, switch the machine between letters and figures. Both character sets use the same signals and they are distinguished only by the FIG or LET mode on that particular moment. The characters “QWERTYUIOP” are processed as “1234567890” in FIG mode

This still gives 26 alpha (-numeric) keys and the additional SPACE, LET and FIG. The KL-7 must encrypt these three additional characters into a letters-only ciphertext. Therefore, the KL-7 design permits the special functions to piggy-back on some of the existing alphabet letters. The letters “J”, “V”, “X”, “Y” and “Z” were selected because they are some of the less frequently used letters.

Before encryption, the letter “Z” is changed into “X” and the SPACE key into the letter “Z”. After decrypting, “Z” is translated back into a SPACE and the letter “X” (originally the letter “Z”) remains an “X”.

Before encryption, the letter “J” is changed into “Y” and the FIG key is changed into “J”. After decrypting, the letter “J” is not printed, but causes the KL-7 to go into FIG mode. The letter “Y” remains “Y”.

Before encryption, both the letter “V” and the LET (letters) key are changed into the letter “V”. After decrypting, if the KL-7 is in LET (letters) mode at that time, the letter “V” remains “V”. If the KL-7 is in FIG mode, the letter “V” is not printed but causes the KL-7 to switch back into LET (letters) mode and also prints a SPACE.

This system of additional characters that piggy-back on normal letters is the most practical method and also the least invasive for the readability of the text. Nonetheless, the design came with a cost. The KL-7 test phrase shows the small changes that occur. The first sentence is the text before encryption and the second sentence is the same text after it is decrypted back into plain text:

```
THE 236TH QUICK RED FOX JUMPED 780 TIMES OVER THE 1459 LAZY BROWN DOGS
THE 236 TH QUICK RED FOX YUMPED 780  TIMES OVER THE 1459  LAXY BROWN DOGS
```

The seldom used letters “J” and “Z” are the only letters that are affected by the piggy-back system.

**Cryptographic Strength**

We can calculate the theoretical strength of the KL-7 by taking all cryptographic variables for a complete machine set-up, knowing the machine’s general principle of operation, but without any information on the internal wiring of the rotors and shape of the notch rings. The 8 rotor cores can be wired in $3.66^{322}$ different ways. This comprises all positions, relative to the machine, making the alphabet ring superfluous (the alphabet is only a visual representation of the rotor alignment). This also comprises all positions of the non-moving $4^{th}$ core, set by its wide ring. The notch rings can be shaped in $7.23^{75}$ different ways. This comprises all combinations of notches, relative to the stepping pawls. This gives a total of $2.65^{408}$ purely cryptographic combinations, or a 1357 bit key.

Next, we calculate all choices for the operator. He must select 8 rotors from a set of 13, giving 51,891,840 combinations. He has 78,364,164,096 ways to set 7 alphabet ring. There are 1,663,200 ways to select 7 notch rings from a set of 11. The 7 notch rings and the wide ring ($4^{th}$ rotor) can be set in 2,821,109,907,456 different ways. Finally, there are 78,364,164,096 possible rotor alignments at the start of a message. In total, this gives $1.49^{48}$ ways to adjust the key settings, both internal and external. This resembles a 161 bit key.

When the machine’s specifications are known to the adversary (espionage, capture) he has to find 8 cores from a set of 13, giving 51,891,840 combinations. There are 1,663,200 ways to combine 7 notch rings from a set of 11. There are 2,821,109,907,456 ways to set 7 notch rings and 1 wide ring. Finally, there are 78,364,164,096 ways to set all core/notch combinations, relative to the machine. The alphabet ring, only visual reference of position of core/notch combination, is disregarded. This gives the adversary a total of $1.90^{37}$ combinations or a 124 bit key.

Trying out all possible keys, a so-called brute force attack, on a 124 bit key is considered infeasible with all present and future computer power. However, cryptanalysis is more than key size, brute force attacks and theoretical security. Rotor cipher machines have proven vulnerable to certain types of cryptanalytic attacks, performed on fast computers. Therefore, the KL-7 is no longer considered secure. Nevertheless, even today, skilled cryptanalysts with current resources would still face a formidable task to mount a successful attack against the KL-7, especially when they have only a limited number of messages at their disposal.

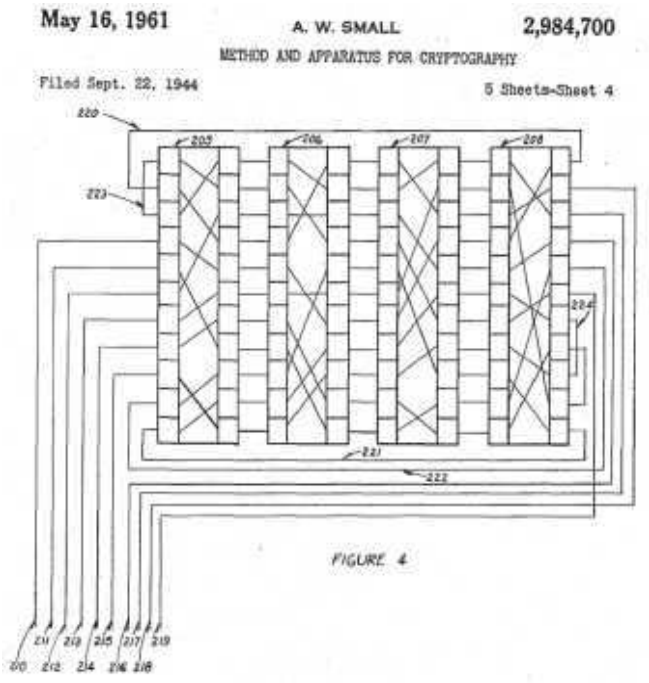
# 5. History of the TSEC/KL-7

**Development of the machine**

The roots of the KL-7 are found in the Second World War. In the 1940's, the electromechanical rotor cipher machine ECM (SIGABA) had set a new standard for secure high-level communications. At tactical level, the lightweight mechanical M-209 was widely used. By the end of the war, the M-209 was no longer considered secure and the Army expressed the need for a lightweight secure crypto machine that could replace the M-209 but that would have a cryptographic strength, comparable with cipher machines like the SIGABA. The Navy was also seeking a small cipher machine with the qualities of the ECM, with a focus on saving weight. In March 1945, the Army headquarter requested the Signal Security Service (SSS) to develop a machine that would fit their needs. Soon after, the SSS was renamed into the Army Security Agency (ASA), who initiated the research.

The project was designated MX-507 and ASA saw it as a long-range research project. The ASA researchers quickly decided to opt for a rotor-based machine. A design with 36-point rotors came on the forefront. They also had to design a completely new lightweight printing system, as the new machine was required to operate off-line and print out the messages on paper. Eventually, they were able to reduce a printer system to one quarter of its original size and weight.

ASA decided to apply a new cryptographic principle, called re-entry. The re-entry or re-flexing was invented by Albert Small, who filed it for patent in 1944. The idea was to take parts of the cipher output, re-enter the output back into the encryption process and re-encrypt it once again (see image right). In 1949, the Armed Forces Security Agency (AFSA) was created. It was the first American central cryptologic organisation and one of its goals was to provide standardization of secure communications devices and to determine a general policy for crypto equipment. The research of the ASA was transferred to AFSA in December 1949.




Meanwhile, in April 1949, the United States and its Allies had formed the North Atlantic Treaty Organisation or NATO, and deteriorating relations with the Soviet Union resulted into a grim Cold War. Secure communications between the NATO members was an important part of making a front against the USSR. An additional challenge that AFSA faced was to design a machine for themselves that could also be distributed to their NATO allies, without disclosing vital secret crypto technology that could come into Soviet hands, either directly or through infiltration of NATO members. With such a large organization as NATO, it was more than likely that this machine or its specifications would sooner or later reach Russian soil. The design had to resist by far any possible cryptanalytic attack by Soviet codebreakers, even when the technical details of the machine were disclosed. The security of the machine had to depend solely on the secrecy of the key settings, thus obeying Kerckhoffs' well known law on cryptography.

The MX-507 was renamed to AFSAM-7, which stands for Armed Forces Security Agency Machine No 7, and by September 1950, AFSA demonstrated an engineering model. The final design used 8 rotors with 36 contacts, a re-entry of ten rotor signals, and a most complex irregular stepping, electrically controlled by notch rings on the rotors. The problems with the printer timing and the shift system were solved by a clever design with vacuum tubes, making the KL-7 the first tactical cipher machine ever to use electronics.

The AFSAM-7 was approved and the Army was allowed to build prototype models. By December 1950, the Army declared the AFSAM-7 ready for production. The machine would become the first standard crypto machine in the U.S. Armed Forces. The crypto system was designated POLLUX. Contractors were selected and operational and maintenance manuals were composed. In February 1951, contracts were signed to produce 25,000 AFSAM-7's at a rate of 5,000 per year. The first repair and maintenance course for Army and Air Force personnel was scheduled in September 1951. In October 1951, AFSA announced two types of operation: the AFSAM-7 traffic for high-level communications was designated ADONIS and the traffic for the Army and Air Force was designated POLLUX. The differences between the two systems were the rotor sets and the message indicator procedure.

The final production contract was signed on February 9, 1952. The AFSAM-7 was introduced in the U.S. armed forces by the newly formed National Security Agency (NSA), and some units were also bought by the Central Intelligence Agency and the Federal Bureau of Investigation. In the early 1960's, the AFSAM-7 was renamed TSEC/KL-7, according to the new nomenclature for crypto equipment. At the moment of its release, the KL-7 was cryptographically more than capable to resist any attack.

A Baudot paper tape reader called TSEC/HL-1 was developed for the KL-7. With this HL-1, the KL-7 could directly read and decrypt five bit level punched paper tapes, received from standard teleprinters. A larger variant of the KL-7, designated KL-47, could also punch five-bit level paper tapes. Individual components of the KL-7 and KL-47 were manufactured by several different U.S. government contracted companies. After final assembly at different locations, the machines became the property of the National Security Agency and were distributed within the U.S. and to NATO members. All machines, used in other countries, were in loan from the NSA.

**The KL-7 in Service**

Despite the KL-7's extensive use within the armed forces, it wasn't always the most popular crypto machine. The KL-7 was notorious for its keyboard and rotor contact problems. The operator often had to push firmly on the keys to get the machine cycling, not allowing him to get any speed on the KL-7. To avoid contact problems, the rotors had to be cleaned regularly. The KL-7 also had a high acoustical signature. TEMPEST, the 'art' of shielding devices against eavesdropping on emitted electrical pulses and, in the case of the KL-7 also sounds, wasn't given priority during the development of the KL-7. When the machine is turned on, the motor slowly takes speed and the reduction gears produce their characteristic high pitched noise. The advancing rotors also produce their typical sound. On start-up, the KL-7's vacuum tubes need to heat up before you can type on its keyboard because the printer timing is controlled by the electronics. Usually, two rotor cages were available for each KL-7. The rotor cage of the previous day was kept on a secure location. If a message of the previous day arrived, the operator simply detached the current rotor cage and attached the old rotor cage on the KL-7 to decrypt the message with the previous key settings.

During its service time, the rotors of the KL-7 and KL-47 were rewired on a regular basis. Some rotors were rewired on a yearly basis on national or NATO level and some rotors, often referred to as the NSA rotors, were to be sent directly to NSA and were rewired by NSA personnel only. It was strictly forbidden to operators, even to the maintenance technicians with crypto clearance for KL-7, to check out the internal wiring of the rotors. The technicians were not allowed to test the rotors pin-to-pin but were instructed to place the rotor on a large conductive plate that made contact with all rotor pins at once, and then check out the connection on each pin at the other side with an Ohm meter. This way, the technician would see if a wire was broken, but didn't know to which pin it corresponded on the other side.

With its large key size (the number of possible different key settings) the KL-7 and KL-47 were considered secure against any attempt by the Soviets to decrypt the messages, even when its specifications would be compromised sooner or later. The machine was therefore certified for Top Secret messages at the start of its career. However, advances in technology and the introduction of miniature electronic components increased the computational power tremendously in the next decades. As a result, the KL-7 had become operationally insecure by the mid 1960's, and vital message traffic was often superenciphered (encrypted a second time) on other systems after being encrypted with the KL-7.

From the 1970's on, the KW-26 and KW-37 online cipher equipment largely replaced the outdated KL-7. Some KL-7's stayed in service, mostly as back-up, and retired in the 1980's. The last known recorded message, encrypted with a KL-7, was sent by the Canadian armed forces in June 1983. The fully electronic KL-51 RACE off-line cipher machine could be seen as the successor of the KL-7. The KL-7 machine itself was unclassified. However, the rotor cage wiring, the rotor entry plates and the stepping circuitry were confidential. Maintenance rotors were considered confidential and operational rotors secret. After its service time, all KL-7's, KL-47's and their rotors were recalled. All surviving KL-7's were carefully stripped from the stepping mechanism and rotor entry wiring. A process commonly denoted as 'sanitized'.

The KL-7 is a unique machine in many ways. It was the first machine to be developed under one centralized cryptologic organisation and introduced as a standard crypto device in all parts of the armed forces. At that time, the KL-7 used the latest cryptologic techniques and was the first ever cipher machine with electronics, yet its rotor based design would soon lose the battle against miniaturisation of electronics and computational power. The KL7 proved to be one of the last of a breed of true cipher machines. Many operators cursed the machine for its quirky keyboard and regular contact problems. They welcomed its electronic successors, but today they speak with sentiment about that wonderful machine and even remember vividly the typical sound of its stepping rotors. Maybe it's because of the era in which the KL-7, and the men, gave their best. Maybe it's because the KL-7 served all over the world, collecting secrets and memories about the Cold War, companionship, and even exciting stories…about treason and espionage. Because this was not the end of the KL-7 story…

### Major Security Breaches

In 1981, former U.S. Army Warrant Officer Joseph Helmich, was arrested by the FBI for the sale of critical information on the KL-7. In 1963, he served as crypto custodian in France and later at Fort Bragg, North Carolina. Being faced with financial problems, Helmich contacted the Soviet Embassy in Paris, France. He received $131,000 in return for critical information on the KL-7. At that moment, the KL-7 was the most widely used crypto machine in the U.S. military. After returning to the United States, Helmich continued to provide KL-7 key lists to the Soviets until 1966. Although already under suspicion in 1964 and admitting in 1980 to have received money from Soviet agents, it was only in early 1981 that he was observed with Soviet agents in Canada. Helmich eventually confessed and was sentenced to life imprisonment.

In 1985, the FBI received a tip from the ex-wife of John Anthony Walker, a retired U.S. Navy communications specialist. Later on, he was observed by the FBI while dropping a grocery bag alongside a road north of Washington D.C. The bag contained 129 copies of stolen secret U.S. Navy documents. At the same moment and a few miles further, a Soviet KGB agent left a grocery bag with $200,000. It was clearly a dead drop exchange to covertly exchange documents and money without meeting face-to-face. The following night, John Walker was arrested by the FBI in a motel.

The investigation shook up the military intelligence community. As later turned out, already in 1967, John Walker simply walked into the Soviet Embassy in Washington DC with a KL-47 key list and offered the Soviets to sell secret Navy documents for cash. It was the beginning of a spying career of no less than 18 years. During a search of his house after his arrest, the FBI discovered a special device, provide by the KGB, to read the internal wiring of the KL-7 rotors. During interrogations, Walker admitted providing the Soviets with complete manuals which enabled the reconstruction of a fully operational KL-7. He was also sentenced to life imprisonment.

The importance Soviet Intelligence gave to the key lists, despite possessing all technical details of the KL-7, shows they probably were unable to break the KL-7 message traffic purely by cryptanalysis, or that they had no sufficient computer power to decrypt them within reasonable time for practical use, at least in the early 1960's.

Further information and detailed images of the KL-7 are found on these excellent web pages:

http://www.cryptomuseum.com/crypto/usa/kl7 Paul Reuvers' and Marc Simons' Crypto Museum website
http://jproc.ca/crypto/kl7.html Jerry Proc's Cipher Machines website

More about the John Walker spy case:

http://www.fas.org/irp/eprint/heath.pdf U.S. Navy analysis on security weaknesses, exploited by John Walker
http://www.usni.org/magazines/navalhistory/2010-06/navys-biggest-betrayal John Walker on U.S. Naval Institute.

The KL-7 simulator website:

http://users.telenet.be/d.rijmenants Historical and technical information, and various other crypto simulators

## 6. Copyright Information & Disclaimer

### Copyright Information



### Disclaimer of Warranties



**Cipher Machines & Cryptology**
http://users.telenet.be/d.rijmenants
dr.defcom@telenet.be

## Appendix A

## The Cold War Running Hot – Cuban Missile Crisis Messages

On October 14, 1962, a U.S. Air Force U-2 plane on a photoreconnaissance mission captured photographic proof of Soviet missile bases under construction in Cuba, at the doorstep of the United States. The Kennedy administration responded with a naval blockade of Cuba to prevent the delivery of offensive nuclear weapons over sea. It was the start of the Cuban missile crisis. The truth about probably the most dangerous moment in the whole Cuban missile crisis was kept secret for many years and only surfaced a decade ago.

On October 27, 1962, after pursuing and unidentified submarine for several hours, U.S. Navy destroyers finally tightened the circle around the submarine. One of these ships, the Fletcher-class destroyer USS Beale, had tracked the submarine and dropped signalling depth charges (the size of hand grenades). Without knowing, the American warships had challenged USSR submarine B-59, a FOXTROT class submarine, armed with a 15 kiloton nuclear torpedo. Eventually, B-59 ran out of air and battery power, and desperately needed to surface

On board B-59, a fierce discussion broke out between submarine captain Valentin Savitsky, political officer Ivan Maslennikov and second captain Vasili Arkhipov. Commander Savitsky argued that “maybe the war has already started up there” and saying “we’re going to blast them now” and “we will not disgrace our Navy”. Savitsky then ordered that the nuclear torpedo on board be made combat ready. Accounts differ about what actually happened. Either Arkhipov convinced Savitsky, or Savitsky himself realized that surfacing was the only reasonable option. This decision might well have prevented an escalation of the conflict into a nuclear war. Robert McNamara, U.S. Secretary of Defense at the time of the Cuban crisis, later stated that the world was much closer to a nuclear war than people had ever thought.

Sources:

U.S. Navy, TOP SECRET/SECRET/FOR OFFICIAL USE ONLY, Charts/deck logs of anti-submarine warfare operations related to USSR submarine B-59, October 1962. U.S. National Archives, Record Group 24.

USSR, Memoir, “Recollections of Vadim Orlov (USSR Submarine B-59): We will Sink Them All, But We will Not Disgrace Our Navy,” (2002).

The National Security Archive: http://www.gwu.edu/~nsarchiv/nsa/cuba_mis_cri/docs.htm

## Decrypting the Messages

On the next page you will find two messages, containing authentic declassified deck logs from USS Beale about the challenging and surfacing of B-59, as recorded on October 27, 1962. Although the message content itself is authentic, the messages, the message encryption and its key settings are fictional and composed only as an exercise on the KL-7 simulator.

Both messages are encrypted according to the message indicator system, described in KAO-41C/TSEC, found as first example in the “Encryption and Decryption” chapter earlier in this paper: align all rotors in “A” position, re-encrypt the spelled-out message indicator and set the result as rotor alignment, repeating the first two letters at the end. Decrypt the actual message with that rotor alignment.

Optionally, once the rotor alignment is finished, you could copy and past the ciphertext into the KL-7 Auto Typing window, to avoid typing the complete ciphertext message by hand.

Note that encrypted messages always carry the security level unclassified and full addresses and security level are encrypted into the message itself. Good luck on decrypting this piece of Cold War history during the heydays of the KL-7…

| ADONIS 27 OCT 1962 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| ROTOR CORE | E | H | F | L | I | A | G | B |
| ALPHABET RING SET | 04 | 28 | 04 | 16 | 09 | 32 | 08 | 11 |
| NOTCH RING | 5 | 10 | 6 | | 7 | 1 | 8 | 3 |
| NOTCH RING SET | C | M+ | E | | B | E+ | Y | K |
| 36-45 LETTER CHECK | ASMTH ISXPI | | | | | | | |
| SYSTEM INDICATOR | 28604 | | | | | | | |

```
VZCZCBLE014     UU
OO RUCSSOZ
DE RUYNBCD 014 27/1810Z
O 271755Z OCT
GR 131
BT
28604 ECHO ZULU INDIA YANKEE WHISKEY
GNVWA WZRUO JEVCF KNDDS QCRBW MMXKS JFCFB IZKHB BPUZM HQUFL
FUXCO GRCLI UWNHD MASJI IJMSI HBNJW NZQFN LNBOM OIUEJ MUBSH
LFAJS ULJXS GKQQM QRHMW PDWAW MXXIK HPKUJ QNTOR QILSF AWEFH
ZTMDQ NFZYD FTBBH BDCJK UAXRN TDQRA QIQKN SOXRX PAVKY LQREO
CEGBE ETBUY HUAKW UUBJS VJPSR WUYYZ NEAUD MWWKM QZOZL PLTEA
YKOVY UKAEK MSZFC OUVIN MCNIQ QKNWD FDQJL HCYFP EEHDA ZHRHS
GFROI KPOYJ VPNKH JYVPL ZHPYY LJXRZ MHLAX DJIPV DWSXB RUHCA
RNFCU TGDST ZJXEE XVKAA EPDXW BHHLR EDBWC NRDIY EVOOA ACXMP
ALCIZ UTGTB VMFHD JAAFM FPMPT QTBIX EECNP RJRYK SXXTP NYPLZ
TGAOG KXZBT PYAWU UYNIP RLVPU ZMFUV UKRKA AJLOI NCERF NPXEB
XAFFZ LSAIA GAUJQ XEEVO IQZNO YIOUQ ENJNC EALIO WNOGA HHEXI
BXXBT BETNT RYCNT BNNKM IVKAP IHLPD NVMJI APEYS TCDIL BVAKW
OSEXR TQKUS JWZIR WSBJQ FVAUM YKUSF ZARQG QYBGV DJHWJ YPCRZ
CIQMW 28604
BT


NNNN
```

```
VZCZCBLE023     UU
OO RUCSSOZ
DE RUYNBCD 023 27/2325Z
O 272310Z OCT
GR 164
BT
28604 FOXTROT BRAVO NOVEMBER KILO TANGO
UJBOL DOKIM PCHZT JDQKS IQXCS YAJVP BTVSJ TQXTS DNWUS ZJPAJ
PDKHE WALLM ISIDS BSXZX PSBDX QTTSY OBEYV KYHKB TJXQO BGEJY
LFCWU WDHKV YLRNZ KZZRT GRLCX ZIVSL TRTZS MYNQP XLAIS YJQJK
KJNEV KBIMK GPDNZ FVUUA JKXNL TXLEI HEOTN CRXVG JOPYJ UHTOX
XIJSW IEWHO OMKRF XUGGC OJBTT EASHO FOQAK NVTNX WILZP YOCLK
CCWYT GOOIM WXUPI KNWLA CNTRV XCDTO LXCDP YAHJY XJKAC FGWJJ
XLBHZ AHRJP MJZBC XHTYZ SORHP DCWRI WDUJJ XRWBY ZOKJN UWLRE
RUHYV KQIYX KIJWY WHBTH UFTIM AIGLN RAKYY FFMHB OANNE FQMAQ
DBDRL HWBFW OOEYE HVQZO WQHFL SLLQH VUMJM LRBJA CRXWX LSLZH
EFKQT IERUL NZRLT SOXUJ JSMZC UHICZ QJPOK OUWXZ ETDJP DGCZK
QMVCW MRYRB QNTGZ CEOKF LNSFQ XMNGE TJHAM GHVTA VJIMW VBRAG
SFYOK ERCRC SPCBG PVVMX XQFXF JTMYU PEHMX DMZVE VCBWO IMBOZ
FCQUZ ZZSJY RTAQQ IBIKB DFALQ XMCBO CVNEE MLFFL ZDSYC VYHUI
TLVRQ PTMNN DUCDF TBJYD VRIAZ EDIPX XYLUJ IHGUL UZXQF YLHUE
UWRGA QOZSH VVWUG AESWE FNJST YMKVR MIWMN NCIDL LAWKH BEIJD
VGFJT OIURG YPSDZ KKBEY ZXHAX YFRSJ RUUKL FXEES KVQRC PTWVP
VEQEX PZFVT VUMMP QMMFR 28604
BT



NNNN
```

* Although these messages contain authentic declassified deck logs from USS Beale, the messages themselves are fictional and composed only for training purposes on the KL-7 simulator.

## Appendix B

### KL-7 Simulator Rotor Wiring

Below, the internal wiring of all 13 available rotors as used in the simulator. The left side of each column shows the left side pin numbers and the right side of the each column shows the pin number it is connected to. Note than during encryption, the signal travels from left to right through the rotors.

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 01-29 | 01-23 | 01-19 | 01-15 | 01-13 | 01-26 | 01-20 | 01-28 | 01-25 | 01-08 | 01-15 | 01-08 | 01-36 |
| 02-27 | 02-19 | 02-26 | 02-26 | 02-04 | 02-34 | 02-19 | 02-19 | 02-06 | 02-31 | 02-13 | 02-18 | 02-06 |
| 03-14 | 03-26 | 03-28 | 03-36 | 03-02 | 03-27 | 03-09 | 03-23 | 03-35 | 03-01 | 03-36 | 03-15 | 03-29 |
| 04-08 | 04-16 | 04-36 | 04-13 | 04-16 | 04-14 | 04-32 | 04-05 | 04-12 | 04-28 | 04-23 | 04-33 | 04-28 |
| 05-35 | 05-02 | 05-06 | 05-01 | 05-17 | 05-02 | 05-36 | 05-17 | 05-21 | 05-20 | 05-06 | 05-07 | 05-24 |
| 06-04 | 06-13 | 06-25 | 06-31 | 06-30 | 06-01 | 06-02 | 06-36 | 06-22 | 06-06 | 06-21 | 06-26 | 06-26 |
| 07-28 | 07-14 | 07-31 | 07-25 | 07-21 | 07-31 | 07-06 | 07-27 | 07-19 | 07-32 | 07-32 | 07-20 | 07-21 |
| 08-11 | 08-35 | 08-18 | 08-33 | 08-05 | 08-36 | 08-33 | 08-14 | 08-32 | 08-05 | 08-18 | 08-16 | 08-22 |
| 09-05 | 09-21 | 09-27 | 09-03 | 09-33 | 09-11 | 09-12 | 09-16 | 09-20 | 09-33 | 09-31 | 09-34 | 09-20 |
| 10-13 | 10-04 | 10-10 | 10-32 | 10-07 | 10-09 | 10-28 | 10-20 | 10-23 | 10-21 | 10-20 | 10-23 | 10-35 |
| 11-20 | 11-17 | 11-05 | 11-21 | 11-29 | 11-35 | 11-04 | 11-21 | 11-30 | 11-30 | 11-01 | 11-36 | 11-15 |
| 12-03 | 12-31 | 12-01 | 12-23 | 12-08 | 12-18 | 12-10 | 12-07 | 12-18 | 12-12 | 12-24 | 12-27 | 12-19 |
| 13-25 | 13-25 | 13-32 | 13-17 | 13-09 | 13-15 | 13-03 | 13-12 | 13-01 | 13-04 | 13-10 | 13-12 | 13-23 |
| 14-33 | 14-03 | 14-09 | 14-29 | 14-36 | 14-12 | 14-24 | 14-22 | 14-16 | 14-14 | 14-35 | 14-24 | 14-30 |
| 15-18 | 15-18 | 15-11 | 15-07 | 15-35 | 15-04 | 15-29 | 15-11 | 15-31 | 15-15 | 15-19 | 15-19 | 15-01 |
| 16-15 | 16-27 | 16-33 | 16-22 | 16-23 | 16-07 | 16-16 | 16-35 | 16-11 | 16-34 | 16-28 | 16-13 | 16-08 |
| 17-07 | 17-12 | 17-23 | 17-20 | 17-34 | 17-29 | 17-22 | 17-13 | 17-24 | 17-07 | 17-07 | 17-02 | 17-12 |
| 18-12 | 18-34 | 18-17 | 18-24 | 18-25 | 18-08 | 18-18 | 18-15 | 18-13 | 18-35 | 18-08 | 18-03 | 18-07 |
| 19-34 | 19-36 | 19-29 | 19-12 | 19-20 | 19-23 | 19-30 | 19-01 | 19-33 | 19-16 | 19-26 | 19-14 | 19-13 |
| 20-16 | 20-10 | 20-12 | 20-10 | 20-22 | 20-19 | 20-17 | 20-32 | 20-07 | 20-18 | 20-12 | 20-29 | 20-27 |
| 21-17 | 21-30 | 21-13 | 21-14 | 21-28 | 21-03 | 21-07 | 21-08 | 21-36 | 21-29 | 21-29 | 21-01 | 21-31 |
| 22-01 | 22-06 | 22-02 | 22-30 | 22-15 | 22-30 | 22-34 | 22-18 | 22-09 | 22-22 | 22-22 | 22-06 | 22-32 |
| 23-09 | 23-07 | 23-16 | 23-19 | 23-01 | 23-20 | 23-15 | 23-33 | 23-34 | 23-25 | 23-25 | 23-32 | 23-09 |
| 24-30 | 24-15 | 24-15 | 24-28 | 24-19 | 24-17 | 24-23 | 24-04 | 24-02 | 24-26 | 24-30 | 24-10 | 24-33 |
| 25-24 | 25-28 | 25-35 | 25-04 | 25-24 | 25-28 | 25-31 | 25-09 | 25-10 | 25-36 | 25-05 | 25-25 | 25-10 |
| 26-23 | 26-01 | 26-08 | 26-35 | 26-27 | 26-21 | 26-25 | 26-29 | 26-08 | 26-11 | 26-09 | 26-30 | 26-16 |
| 27-02 | 27-11 | 27-24 | 27-05 | 27-10 | 27-22 | 27-27 | 27-26 | 27-26 | 27-23 | 27-02 | 27-09 | 27-14 |
| 28-32 | 28-33 | 28-22 | 28-08 | 28-11 | 28-05 | 28-01 | 28-24 | 28-29 | 28-19 | 28-27 | 28-05 | 28-18 |
| 29-10 | 29-29 | 29-30 | 29-06 | 29-06 | 29-25 | 29-21 | 29-25 | 29-15 | 29-03 | 29-16 | 29-28 | 29-34 |
| 30-19 | 30-20 | 30-03 | 30-09 | 30-12 | 30-33 | 30-26 | 30-34 | 30-17 | 30-02 | 30-04 | 30-17 | 30-02 |
| 31-06 | 31-32 | 31-34 | 31-16 | 31-32 | 31-16 | 31-08 | 31-10 | 31-04 | 31-13 | 31-17 | 31-22 | 31-03 |
| 32-26 | 32-24 | 32-14 | 32-27 | 32-26 | 32-13 | 32-05 | 32-06 | 32-28 | 32-27 | 32-03 | 32-31 | 32-17 |
| 33-36 | 33-05 | 33-07 | 33-02 | 33-14 | 33-24 | 33-13 | 33-03 | 33-14 | 33-24 | 33-34 | 33-04 | 33-25 |
| 34-22 | 34-22 | 34-20 | 34-11 | 34-03 | 34-06 | 34-35 | 34-30 | 34-03 | 34-10 | 34-14 | 34-11 | 34-11 |
| 35-31 | 35-08 | 35-21 | 35-34 | 35-18 | 35-10 | 35-11 | 35-02 | 35-27 | 35-17 | 35-11 | 35-21 | 35-04 |
| 36-21 | 36-09 | 36-04 | 36-18 | 36-31 | 36-32 | 36-14 | 36-31 | 36-05 | 36-09 | 36-33 | 36-35 | 36-05 |

### KL-7 Simulator Notch Rings

Below the notch rings as used in the KL-7 simulator. Each “0” represents a notch in the ring, setting the according switch inactive. Each “1” represents a bump on the ring and will activate the according switch.

| Ring | Notch Ring Positions 1 - 36 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1<br>0 | 1 | 1<br>2 | 1 | 1<br>4 | 1<br>5 | 1<br>6 | 1<br>7 | 1<br>8 | 1<br>9 | 2<br>0 | 2<br>1 | 2<br>2 | 2<br>3 | 2<br>4 | 2<br>5 | 2<br>6 | 2<br>7 | 2<br>8 | 2<br>9 | 3<br>0 | 3<br>1 | 3<br>2 | 3<br>3 | 3<br>4 | 3<br>5 | 3<br>6 |
| 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 |
| 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 |
| 3 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 |
| 4 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 |
| 5 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 7 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| 8 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 |
| 9 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 |
| 10 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 |
| 11 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 |