

KL-7 Cipher Machine Simulator

Version 5.0

© 2012-2013 Uri Blumenthal

Overview

This program emulates *TSEC/KL-7* offline non-reciprocal rotor-based cipher machine developed by the National Security Agency (NSA) in the US.

This simulator is patterned after and uses GUI, sound files and Help file of the KL-7 Simulator v4.1.2 written for MS Windows by Dirk Rijmenants:

*Source: © Rijmenants, Dirk. Cipher Machines & Cryptology,
<http://users.telenet.be/d.rijmenants>.
All rights reserved*

This program uses information, audio and photos from Crypto Museum under license CM-500384. See more details at:

<http://www.cryptomuseum.com/crypto/usa/kl7/>

This program includes three components:

KL7Sim

is the actual simulator of the KL-7 machine;

KL7Rewire

generates new wiring for the rotors and the baseplate, and new shapes for the notch rings;

KL7Codebook

generates new codebooks containing daily keys (single key, monthly key-sheet, key-sheets for the entire year) for KL-7 networks.

Usage is granted on the following terms:

This program is written for educational and historical research purposes and is provided as freeware. It can be used under the following conditions:

It is strictly forbidden to use software or copies or parts of it for commercial purposes or sell or lease this software, or to make profit from this software by any means.

(C) Dirk Rijmenants 2011

Contents

Additions to and changes from Dirk's version 4.1.2	4
Controls Overview	5
Copyright Information and Disclaimer	6
<i>Copyright Information</i>	<i>6</i>
<i>Disclaimer of Warranties</i>	<i>6</i>
About the KL-7 Simulator	6
Operating the Simulator	7
<i>What is the KL-7</i>	<i>7</i>
<i>The Simulator Window</i>	<i>7</i>
<i>The Main Switch</i>	<i>7</i>
<i>Letters, Figures and Spaces</i>	<i>9</i>
<i>The Counter</i>	<i>9</i>
<i>The Rotor Cage</i>	<i>9</i>
<i>The Rotors – Setting the Key</i>	<i>9</i>
<i>Codebook</i>	<i>11</i>
<i>Rewire</i>	<i>12</i>
<i>The Clipboard</i>	<i>12</i>
<i>The Auto Typing Function</i>	<i>12</i>
Enciphering and Deciphering	13
<i>The Key Settings</i>	<i>13</i>
<i>Enciphering</i>	<i>14</i>
<i>Deciphering</i>	<i>14</i>
<i>The Message Indicator and Rotor Alignment</i>	<i>14</i>
<i>Message Format</i>	<i>18</i>
<i>Other Message Indicator Systems</i>	<i>19</i>
<i>Random Letters</i>	<i>19</i>

<i>Security of the above methods</i>	19
Customizing your KL-7	20
Technical details from Crypto Museum	22
<i>Block Diagram</i>	22
<i>Rotors (KLK-7)</i>	23
<i>Rotor wiring</i>	24
<i>Gear box</i>	24
<i>Stepping Unit (KLA-7)</i>	25
<i>Rotor movement</i>	25
<i>Keyboard</i>	25
<i>Mode switch</i>	26
<i>Pulse Generator</i>	26
<i>Printer</i>	27
<i>Classified</i>	27
Technical details from Dirk Rijmenants	28
<i>The Signal Path</i>	28
<i>The Permuter Board</i>	29
<i>The Rotors</i>	30
<i>The Rotor Cage</i>	30
<i>The Notch Rings</i>	31
<i>The Stepping System</i>	31
<i>Letters and Figures</i>	31
<i>Cryptographic Strength</i>	33
Appendix A	34
<i>Simulator Rotor Wiring</i>	34
<i>Simulator Notch Rings</i>	34
<i>Base Plate Wiring</i>	34

Additions to and changes from Dirk's version 4.1.2

- A. M-rotor is added. It was introduced in 1975 and rewired monthly.
- B. Complete customization is supported. Multiple customization files can be generated by the *Rewire* component. `kl7-custom.txt` is loaded automatically when the simulator starts, other customization files can be selected and loaded by pressing F7 key. Customization can be removed by pressing F8 key. You can apply and remove various customization files on the fly as the simulator runs.
- C. INSERT and END keys both save the entire state of the machine (rotors and their positions, machine mode and register). Adding END key is useful because Macs don't have INSERT key.
- D. UP-Arrow shifts to FIGURES, DOWN-Arrow shifts back to LETTERS. SHIFT key behaves as the Help file describes.
- E. This version supports multiple key files (*.txt format). It also parses automatically all the key file formats that the *Codebook* component generates. Click on *Codebook* to generate new keys - a single day key, a monthly key-sheet, or a set of the monthly key-sheets for the entire year.
- F. Click on the rotor cage for rotor configuration and to load or save the key, and on the black levers underneath the cage window to set rotor starting position (message key). Note that when the key is loaded from the key-sheet, it validates the key by its LETTER CHECK and sets the initial (daily) starting position for the rotors. Note that even if the LETTER CHECK fails, the key is still loaded because it may be that the LETTER CHECK was computed on rotors that were wired differently. So the user is informed of the check failure and can make an informed decision. Note: *Codebook* generates LETTER CHECK for the current machine wiring (i.e., for customized rotors and cage).
- G. This version allows to save output to and/or load input from text files.
- H. Counter counts only enciphered and deciphered characters, and does not get incremented for symbols typed when the machine is in the *Plaintext* mode (marked **P** on the main switch). Note that the space character produced when the mode is switched between **P** and **E** does increase the counter.
- I. Keyboard keys (letters, figures, space) auto-repeat when pressed and held (of course, until released). You can disable (and re-enable) auto-repeat by pressing F3 key.
- J. On soft keyboard, click on RPT key first, then click mouse (but don't release!) on the character you want to auto-repeat. To stop auto-repeating, just release the mouse. RPT functionality can be disabled/enabled (toggled) by pressing F3 key (applies to the keyboard as well, see above).
- K. Original Help file and Manual can be displayed by pressing F2 key.
- L. **Important update!** Based on [KAO-41C/TSEC](#) that was declassified on 28-Apr-2011, any rotor can be placed in 4th slot. In that case, the wide ring is attached to it instead of the notch ring. We now support this. Also, cryptographic procedures have been updated, following this manual.

Controls Overview

Action	Simulator (mouse click on)	Keyboard key	
Switch O > P > E > D	Right half of the switch	RIGHT Arrow	
Switch O < P < E < D	Left half of the switch	LEFT Arrow	
Letters	Keys A to Z	A through Z	
Space	Space key	SPACE	
Figures	Keys Q(1) through P(0)	0 - 9 on keyboard	
Switch LET/FIG and back	LET and FIG keys	SHIFT, or	UP-Arrow to FIG
			DOWN-Arrow to LET
Adjust rotor positions	Black levers under rotors	Function key F8	
Save entire state of machine	Not available	INSERT or END	
Restore machine state	Not available	HOME	
Reset counter	Click counter lever	Function key F4	
Delete (erase) paper tape	Click on Paper tape and click Clear	DELETE or Backspace	
Sound On/Off	[speaker] icon	Not available	
Display Help file for this version	[?] icon	Function key F1	
Display original Help file from Dirk	Not available	Function key F2	
Clipboard	Click Paper tape	Function key F5	
Auto Typing	Click power cord	Function key F6	
Load customization file	Not available	Function key F7	
Remove customization (restore original settings of Dirk Rijmenants' sim)	Not available	Function key F8	
Key settings	Click rotor cage	Function key F9	
Toggle RPT enabled/disabled	Not available	Function key F3	
Exit the simulator	[X] icon	Command-Q (Mac)	

Copyright Information and Disclaimer

Copyright Information

This program is provided as freeware and can be used and distributed under the following conditions: it is strictly forbidden to use this software or copies or parts of it for commercial purposes or to sell or lease this software, or to make profit from this program by any means. You are allowed to use this software only 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, or fitness for any particular purpose. The entire risk as to its quality and performance is with the user. In no event will the author of this software be liable for any direct, indirect or consequential damages, resulting out of the use or inability to use this software.

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 also 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 is operated in exactly the same way as the real KL-7, with all switches, keys and levers, and even the actual KL-7 sounds. The development of this simulator is based on publicly available information and research. The principles of operation and technical details are known, but the internal wiring of the ciphering rotors, which is considered part of the secret key settings, is still classified. Most available machines are sanitized and the rotors are either removed from the rotor cage, stripped of their wiring, or the rotor cage has been sealed. Therefore, it is impossible to make a fully compatible simulation, as there is no fully functional machine with an accessible rotor wiring to be compatible with. The KL-7 simulator operates cryptographically in exactly the same way as the real KL-7, but consequently uses its own rotor wiring and notch rings. Keying and operating procedures have been verified against the recently declassified AFSAG 1236 and KAO-41C/TSEC manuals. On KL-7 base, two systems were deployed: POLLUX and ADONIS. Both had tactical applications and employment, but ADONIS was typically used for higher-level communications including strategic...

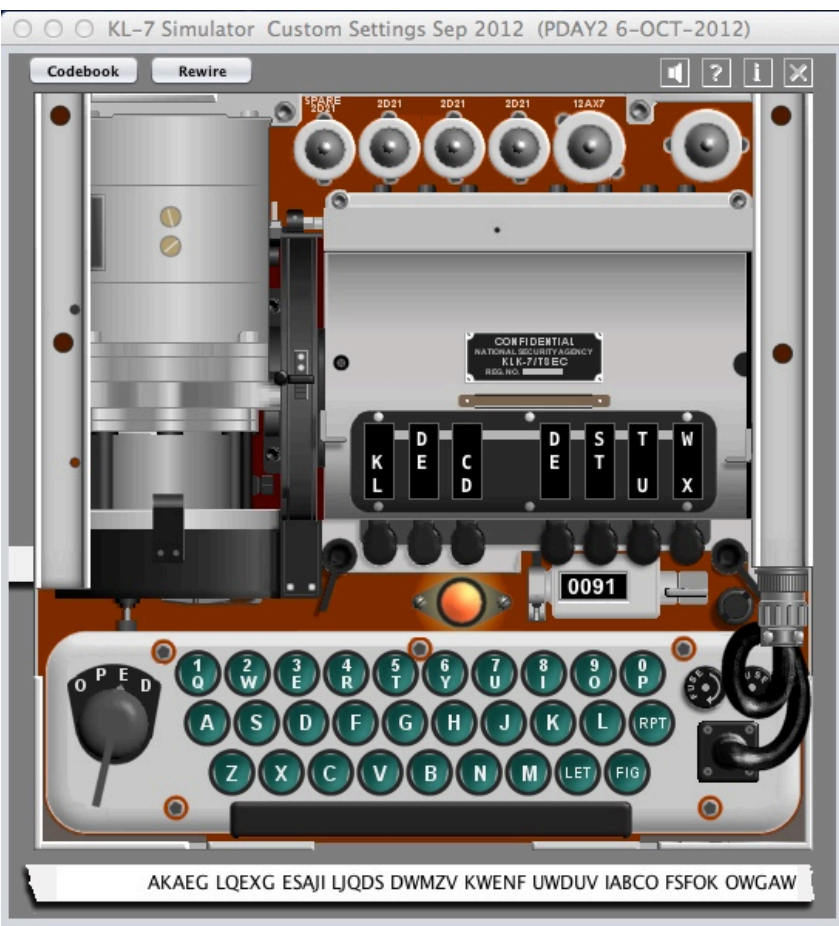
This simulator is a tribute to the ASA and AFSA engineers and cryptologists who developed the KL-7, and to the men who worked with this wonderful machine. With most surviving KL-7's sanitized, this simulator is the only remaining way to actually work with this beautiful machine, and the simulator serves as an attempt to keep the KL-7 machine and its history alive.

Important notice: This simulation is developed for educational and historical research purposes. Today, the KL-7 is by no means a secure way to encipher and protect information. When the key settings of the simulator are saved in a file - that file is not protected and can be accessed and read by anyone who has access to the computer, either directly or remotely.



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. After you have learned how to work with the KL-7, you can decipher two messages, related to the Cuban missile crisis, that are found in Appendix B.



What is the KL-7

The TSEC/KL-7 is an offline electromechanical rotor cipher machine. The KL-7 can encipher readable plaintext into unreadable ciphertext or 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 encipher or decipher a message, the operator had to select the appropriate ciphering rotors, their order, the position of the alphabet ring, select notch rings for each rotor and set the notch rings in the correct position on the rotors. This so-called key setting was usually performed once a day, according to a key list. For each individual message on a particular day, the operator used a unique starting position of the ciphering rotors, known as the message key. This machine has been deployed under the code names POLLUX and ADONIS.

The Simulator Window

In the top-right corner of the simulator window there are four icons. From left to right, these are sound (on/off), this help file, the about window and the exit button to leave the KL7 simulator.

In the top-left corner there are two buttons "Codebook" and "Rewire" that invoke the Codebook-generating and new wiring-generating modules.

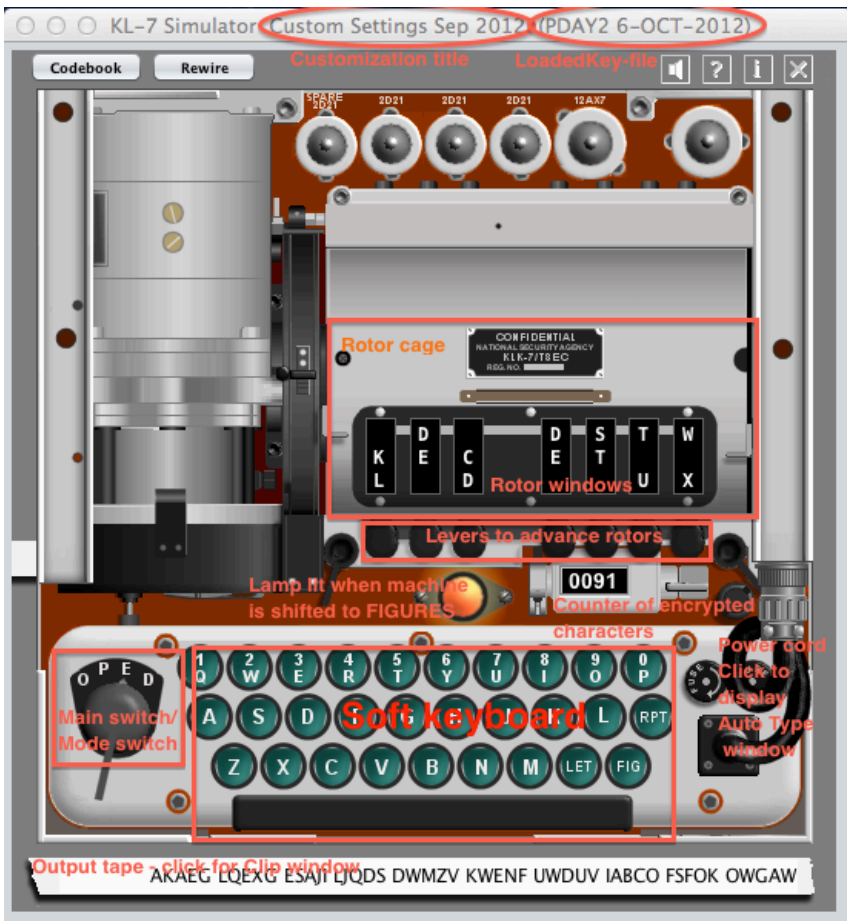
The Main Switch

When you start the KL-7 simulator for the first time, the default key settings are loaded and the machine is in the O (off) position. Turn on the machine by selecting the P position on the switch, located at the left of the keyboard.

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

The main switch has four positions:

- O** – Off Position: the machine is shut down completely and the keyboard keys and manual rotor movement don't function.
- P** – Plaintext: the keyboard and printer are activated. The text you type on the keyboard is printed directly onto the paper tape without encryption. The rotors do not move.
- E** – Encipher: the keyboard, rotors and printer are activated. Machine enciphers every character typed and prints the result in five-letter groups onto the paper tape. Note that the rotors perform one step cycle (controlled by the notch rings) when you switch from "P" to "E" mode or from "E" to "P" mode.
- D** – Decipher: the keyboard, rotors and printer are activated. The entered text is deciphered and the plaintext is printed onto the paper tape. The Decipher mode only accepts letters.



The Keyboard

The keyboard contains the complete alphabet, and the FIG (figures), LET (letters), RPT (repeat) and SPACE keys. In FIG mode, the top row letters QWERTYUIOP represent the figures 1234567890. You can click all these keys with the mouse. These keys do not work when the main switch is in the "O" (off) position. You can enter letters and figures in "P" and "E" mode and only letters in "D" mode. Use the FIG key to switch to figures and LET to switch back to letters. The figures lamp, located just above the centre of the keyboard, will light up when the machine is in the FIG mode.

You can also use your PC keyboard to operate the KL-7 keyboard. All letters are automatically converted into capital letters. Use 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, therefore this function has been modified:

- on the computer keyboard just hold down the desired letter, and it will be auto-repeated until you release the key.

- on the simulator keyboard (the “soft” keyboard) click the mouse on the RPT button, then click (press and hold) the mouse on the letter you want to auto-repeat. It will auto-repeat until you release the mouse.

You can disable (and re-enable) the auto-repeat by pressing F3 function key.

Letters, Figures and Spaces

Because we have to encipher 26 letters, FIG, LET and the space bar into a ciphertext that contains only 26 letters, the designers devised a unique solution: 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 small changes that occur. The first sentence is the text before enciphering and the second sentence is the same text after it is deciphered 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. Punctuation marks are usually omitted, or when required for clarity - spelled out. It is recommended to use X in place of a period, e.g., PICKUP ARRANGED X SAME PLACE TOMORROW X

The Counter

The KL-7 has a character counter, located above the keyboard, that keeps track of the enciphered or deciphered characters. The counter does not count in Plain mode. Click the lever on the right of the counter (or press function key F4) to reset it to zero.

The Rotor Cage

The rotors and notch rings inside the rotor cage control the KL-7 encryption process. The rotor cage contains 8 ciphering rotors. Positions of 7 rotors is visible in the little windows. The top letter in each window, marked by the white index, is called the current position. After enciphering or deciphering a character, the rotors are stepped to the next position. On each cycle, multiple rotors will step. This is controlled by the notch rings on the rotors. These notch rings cause the rotors to step in a highly irregular and complex fashion through the KLA-7 switch-pileups. The 4th rotor doesn't move and therefore has no window to observe its position. All the rotors have alphabet rings and notch rings each. Rotor that goes into the 4th slot in the cage (stationary position), gets a wide ring instead of a notch ring. All the other rotors get a notch ring each that controls rotor stepping mechanism.

Each message requires a new random start position of the rotors, the so-called message indicator (or message key, this procedure is explained later). To adjust the rotor positions, set the main switch in the P position and mouse-click on the black lever underneath the desired rotor. The popup for setting the rotor starting positions will appear. You can memorize the current rotor positions with the INSERT or END key. Use the HOME key to recall the memorized rotor positions.

Note that INSERT (or END) stores the entire configuration of the machine in the file “k17-savedstate.dat”: rotors and their positions, notch rings and their positions, current position (visible through the cage window) of the rotors, machine mode (O, P, E, D) and register (LETTERS or FIGURES). Pressing the HOME key restores the machine state from this file.

The Rotors – Setting the Key

The rotors control the Encipher and Decipher process. This is called the machine's key setting. It is impossible to decipher and read a message without the correct key settings. The rotor cage has 8 rotor slots. Each rotor must be assembled and set prior to going into its designated slot.

POLLUX and ADONIS were similar. The distinctions are: each POLLUX rotor set had 8 rotor cores identified by numbers from “1” to “8”, 7 alphabet rings, 1 stationary wide ring, and 7 notch rings identified by numbers from “1” to “7”. Each ADONIS set had 13 rotor cores with alphabet rings

permanently attached, 1 stationary wide ring, and 11 notch rings. When a rotor is assembled, a notch ring (or a stationary wide ring) is locked on the rotor core in accordance with instructions.

The operator must select the proper rotors and position of the alphabet ring, the notch rings and their position on the rotor. The stationary wide ring gets attached instead of a notch ring to the rotor that goes to 4th slot in the cage. That rotor will be stationary (because unlike other rotors it does not step). Click on the rotor cage (or select F9 on the PC keyboard) to activate the Key Settings window and select and adjust the rotors and notch rings.

The key setting for ADONIS system comprises the following variables:

- **8 rotor cores** chosen from a set of 13, labelled "A" through "M" (M-rotor has been added in 1975).
- **alphabet rings** permanently mounted on the cores and set in any of 36 positions marked on the side from "01" to "36".
- **7 notch rings** chosen from a set of 11 and labelled "1" through "11". These are mounted on the core on the side, next to alphabet ring.
- **position of the notch rings** in any of the 36 position. Notch rings each have two "bracketing marks", which are supposed to bracket a position on the top surface of the alphabet ring. Positions between letters, e.g., between "B" and "C", are given in the key list as "B+".
- **the wide ring** is placed on the rotor that goes to the 4th slot, and it is treated exactly as the alphabet ring (except that it does not have letter markings on the top surface, because it never moves, and is never visible outside the cage). In the menu above, the setting of the wide ring for the 4th rotor is in the *Alphabet Position* column with the rest of alphabet rings.

	Rotor Selection	Alphabet Position	Notched Ring Selection	Notched Ring Position
1	E	04	5	C
2	H	28	10	Y
3	F	04	6	R+
4	L	16	none	none
5	I	09	7	G
6	A	32	1	B+
7	G	08	8	T
8	B	11	3	J+

Buttons: Zeroize, Load key, Set Key, Set & Save, Cancel

These settings are picked according to the daily key setting. Of course, you can use each rotor only once, and the program will refuse any double use of a rotor. Select for each rotor the position of the alphabet ring (labelled from "01" to "36"), and the wide ring position of the 4th rotor (labelled same as alphabet ring). There are 11 notch rings, labelled "1" through "11". Select a notch ring for each individual rotor according to the key sheet and set the position of that notch ring on its rotor with the "Set" button. With the "Set & Save" button you will both set the cage configuration and save the key settings in a file of your choice. Use the "Zeroize" button to reset the rotor cage to default (note that the key files that are stored on your disk are not deleted - to remove them from your system you would have to use File Explorer or the appropriate system command).

SECRET CRYPTO									ARIEL 8036 CRSJH									MAY 2013		
DAY	ROTORS								NOTCH RINGS								DAILY ROTOR	36-45 LTR	SYSTEM	
	1	2	3	4	5	6	7	8	1	2	3	5	6	7	8	ALIGNMENT	CHECK	GRP	INDICATOR	
31	J	F	C	M	D	H	K	I	4	9	5	6	10	7	3	GCN	NDKC	HJIEO	SNKGN	HIVGG
	14	24	02	25	30	20	13	35	Z+	E	C	V	Q	O	Z					1589
30	H	D	M	I	F	A	B	C	1	2	5	3	11	4	6	PHV	NONY	SKACZ	UVBOS	AMMNS
	23	34	22	21	21	27	19	34	E+	L	V	V	R	H	I					2298
29	B	G	E	I	M	L	C	A	10	4	5	11	7	1	9	OIC	WDQS	WQBRW	FPAAB	EIQNM
	34	20	03	20	12	21	07	08	H	C	W	A	W+	D	E					6577
28	F	I	M	D	H	C	J	K	7	1	2	3	4	5	6	MKA	FIFU	HJOXZ	TTEQQ	EJQQA
	21	10	19	26	18	04	27	26	P	B	V	L	Z+	G+	L					4921
27	A	F	D	M	B	E	C	G	4	7	9	11	10	1	2	GDU	QMGN	GFDHE	LCHRX	XYZGF
	04	02	09	14	29	04	18	04	C	D	O+	O	L	T	I					1190
26	G	L	A	B	D	C	I	M	2	5	1	3	6	4	7	NYO	YMCS	VALGV	HQTXZ	MDIUN
	14	10	35	21	15	36	01	08	O	C	Q	I	T	H	E					6754
25	D	F	I	E	G	L	H	B	10	1	7	4	2	8	11	JHE	JBRA	VEEKW	ELJXG	XHVCJ
	25	02	23	08	09	26	11	35	O+	I	B	V	Z+	P	E					1706
24	F	L	B	D	I	G	A	C	1	2	8	6	3	9	4	GGW	HYOT	AGAAQ	XGBGJ	THQNC
	03	04	32	30	27	31	13	33	C	J	T+	G	O	G+	O+					9266
23	D	J	L	M	A	B	G	C	10	11	2	6	7	4	8	BQR	FROG	ZLVVV	CYREU	VBPSJ
	24	34	12	08	11	32	30	06	O	L	J+	W+	E+	E+	B					1723
22	K	E	A	F	M	D	B	C	1	2	8	6	10	9	5	QGL	SBUB	POYDM	CBHMF	KOKJO
	24	09	07	16	21	04	11	11	E	W	L	I	R	T+	M+					9039
21	M	I	J	E	A	B	K	C	9	7	6	10	5	3	8	DSC	GLQO	LEARU	ILVNS	VHRKT
	25	26	10	12	18	23	20	28	C	R+	C	O+	Z+	T+	W					4626
20	L	C	F	J	I	K	E	B	11	1	2	9	6	7	10	FAG	WENZ	ELLIO	UILVU	RZFTV
	29	08	13	27	11	11	06	33	N	E	B+	Z+	Y	O	G					2536
19	F	H	K	J	M	B	L	A	11	10	6	1	7	8	9	ZFR	DXLQ	RYKCB	GRYCU	GBUWQ
	23	11	21	33	25	01	29	32	I	G+	Q	F	J+	J	P					1804

To set their machine with the required identical crypto variables, sender and receiver used a key list (such as shown above, which was generated by the *Codebook* component). Each key list entry for a given date contains the list and order of the selected rotors with alphabet ring positions

marked directly underneath the corresponding rotor, selected notch rings and their positions marked underneath, and a daily rotor alignment (basic start position). The basic start position is used to encipher the message indicators for the individual messages. A key list was distributed with a "36-45 Letter Check" to verify the key settings. To perform this check, all rotors are set in the "A" position with the machine in 'P' mode. Next, the machine is switched to "E" mode and the letter "L" is repeated 45 times. The last two code groups, letters 36 to 45, should match the letter check on the key list. The last column comprises *system indicators* for the individual keys. At the top of the list there are:

- **Classification** from CONFIDENTIAL to TOP SECRET with CRYPTO marking.
- **Codename** of the net.
- Two **system indicators** for this key list - 4-digit group, and 5-letter group.

Only one *system indicator* (SI) is used with a message. For ADONIS it can be a 4-digit group, or a 5-letter group. One can select the SI from the header of the key list, or pick the one for the given date and key.

Clicking on the "Load Key" button opens the File Chooser dialog that allows to select a key file in one of the three formats (the program automatically recognizes each of them):

- Key file created by the "Set & Save" button of the "KL-7 Key Settings" menu. It contains everything that this menu allows to set (rotor selection, alphabet ring positions, notch rings and their positions), but not the basic start positions for the rotors.
- Single Key file created by the *Codebook*. It contains all the above settings plus the basic start position for the rotors. It also provides the LETTER CHECK, which is automatically verified when this key is loaded.
- Monthly Key-sheet created by the *Codebook*, such as shown above. In this case when loading the key, the user is prompted to enter the day of the month for which the key should be loaded.

Clicking on the "Set & Save" saves the settings displayed in the "KL-7 Key Settings" menu in a file of user's choice.

Codebook

The *Codebook* component is activated by clicking on the *Codebook* button. It will generate keys for a single day, for a month, or for the entire year. It supports both random key generation, and generation based on the seed derived from the user-provided pass-phrase.

The simulator can automatically parse the key-sheets generated by *Codebook*, and load the daily key of your choice. This key is validated by comparing the code groups (letters 36 to 45) generated by the Letter Check procedures (performed automatically) with the LETTER CHECK groups given in the key-sheet. The *Codename Net* determines the filename that the generated key-sheet will be written to. You will be prompted where to store the generated key-sheet files.

It is possible to generate the key-sheet from a user-supplied password. This allows two distant users exchange a single password/passphrase and generate the same key-sheets from it. This method is weaker than generating key-sheets based on *Random*, but convenience or inability to securely exchange entire key-sheets may force one to resort to the *From password* method.

Note that *Codebook* takes into account customization, so when a key-sheet has been generated on a machine, its LETTER CHECK was computed using customized rotors, etc. If your machine is customized, but you want to generate key-sheets for the original (default) rotor wirings - press function key F8 to remove customization before invoking *Codebook*.

Rewire

This component generates new rotor wirings, new shapes of notch rings that control rotor stepping, and new base plate. It is not known if in the course of use of KL-7 notch rings were ever updated, nor whether the base plate was ever rewired. But it has been published that in Denmark all the rotors were rewired annually at NATO Maintenance and Supply Agency (NAMSA), the L-rotor was rewired annually at AMSA (Allied Military Security Agency), and the M-rotor was rewired monthly at the crypto center (see <http://jproc.ca/crypto/kl7.html>).

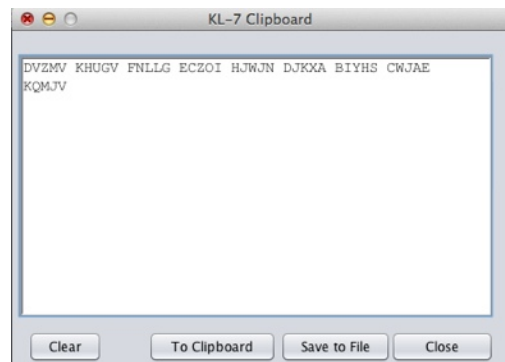
The original rotor wirings and notch rings are still classified. More so, no KL-7 machine with the original rotors currently exists. And those rotors were wired differently for different countries, maybe for different users as well. That means it would be pointless to copy original rotors even if they were known, because there is nothing now to be compatible or interoperate with (no real working KL-7 exists, as far as we know).

This simulator is compatible with the excellent [KL-7 simulator written by Dirk Rijmenants](#), which is not surprising considering that this simulator was written using specifications collected by Dirk, and tested on his example ciphertexts. You can exchange encrypted texts, saved keys and customization files between the two programs. Note that both programs allow users to have their own "personal" wirings - and increase security at the cost of potentially lesser interoperability. Use of this component is straightforward: just select what (which rotors, and/or notch rings, and/or base plate) to rewire, and click *Generate*. You will be prompted for the file name and directory where to save the newly generated wiring data, which you could then exchange (off-line!) with your correspondents. Like the *Codebook* component, *Rewire* supports generating the new wirings based on a user-provided password. This is less secure than generating from *Random*. But if exchanging the customization files themselves is not feasible, generating two identical customization sets at remote places from a pre-shared password may be the only option.



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. You can call the clipboard window by clicking the paper tape or by using the F5 key. The window shown on the right will pop up. Use the "To Clipboard" button to send the text to the clipboard. Use "Save to File" button to save this text in a file of your choice. You can edit the text before sending it to the clipboard or saving. The purpose of "Clear" and "Close" buttons is self-evident. :-)



The Auto Typing Function

To speed up the processing of large pieces of text, you can use the Auto Typing function. To call the Auto Typing window, you either click on the power cord, located at the right of the keyboard, or use the F6 key. The window shown below will pop up. Don't forget to set the main switch in the appropriate position and to preset the correct rotor positions (message key) before using the Auto Typing function for encryption or decryption!

You can type your text directly into the text box, load the clipboard content with the "Get Clipboard" button, or load the text (e.g., plaintext to be encrypted, or ciphertext to be decrypted) from a file by clicking on the "Get File" button. In the bottom left corner you can set the speed of the auto-typing. "Slow" has a speed of 0.5 character per second, suitable for demonstrations purposes or observation of the ciphering cycles. "Normal" is 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 op-

erators). "Fast" processes the text immediately without any delay function. This enables quick processing of large pieces of text in a blink of an eye. "Save" button allows you to save your edited text to a file of your choice and location. Note, that if you edit text in this window and, e.g., add carriage returns for better readability, save this edited text in a file, and then bring it back into this window via "Clear" and "Get File" - you won't see those carriage returns (the text will be as shown in the picture above), but the saved file will be properly formatted.

If your text is finished, use the "Start" button to start the Auto Typing. You can interrupt the Auto Typing with the ESC key. If you made an error in your machine setup, 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 text box, even when the window is closed. Of course, in P and E mode, only letters, figures and spaces are processed (there's automatic switching between LET and FIG) and in D mode only letters.

Note: you cannot paste into Auto Typing window, but you can copy text to the Clipboard and import from there. The Auto Typing function is not available when the KL-7 main switch is in the "O" position.

Important notice: it is possible that a ciphertext, entered by the user on the keyboard, differs from the same text, entered with Auto Typing. Auto Typing always switches to FIG or LET just before figures replace letters or vs versa (space does not force register change), for instance ABC [SPACE] [FIG] 123, while the user could type ABC [FIG] [SPACE] 123.

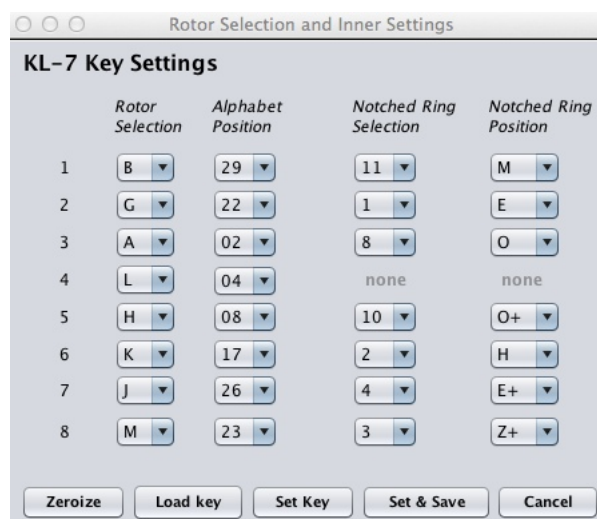
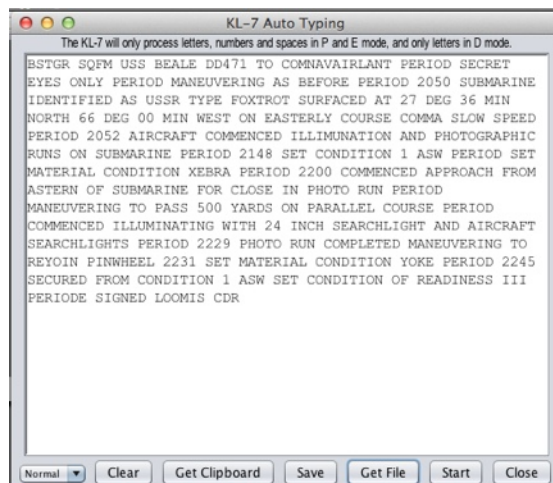
Enciphering and Deciphering

We will explain the encryption and decryption procedures with the help of a few step-by-step examples. However, before we can encrypt or decrypt messages, we must adjust the internal settings of the KL-7 machine, the so-called cryptographic key. Cryptographic keys were distributed via *key lists*. Each list was printed on a key sheet (see above for an example) that usually contained keys for a month.

The Key Settings

To correctly encipher and decipher a message, both sender and receiver must use identical key settings. This key setting is distributed on a key list beforehand. Once the key is set on the machine and the 36-45 Letter Check was successful, you can encipher or decipher messages. A key setting was generally valid for 24 hours. The key must contain the rotors to use and their order in the cage, the position of the alphabet ring of each rotor, the notch rings for each of the seven rotors (except for the 4th one, which doesn't step), the notch ring positions, and one single basic start position of the rotors (a seven letters group) for each day.

Prior to enciphering or deciphering a message, the cage must be configured for the daily key. To set the daily key click on the rotor cage or press F9 function key. The above menu will pop up. Clicking "Default" sets each rotor to the default starting position "A". After that rotors must be set in the proper start position. The rotor positions for each individual message are called message rotor



alignment, and must be unique for each message. In the [Message Indicator](#) section below is explained how you can tell the receiver of the message which message key is used.

Since usually more than one cryptographic system is employed, it is important to be able to determine, which system to use to decrypt the arriving encrypted message. System indicator that is included in the plaintext header of the encrypted message conveys this information. It points at the system, and at the appropriate key list that should be used to decrypt this message.

Enciphering

It is important that the main switch is always in the "P" Plain position when the rotor alignment is set and before the enciphering is started! Once the KL-7 is prepared to start enciphering, the main switch is turned from "P" to "E". At that moment, some rotors will advance one cycle. How many and which rotors will cycle, depends on the current notch positions on the rotors. This procedure provides an additional limited scramble of the rotor positions, prior to enciphering the first character of the message. To set the starting positions for the rotors click on the black levers underneath the rotor cage (the machine must be in "P" mode). The "Message Rotor Alignment" menu will pop up.

To encipher text we use the following sequence:

1. Set the main switch in "P" position
2. Set the Message Key as start position on the rotors
3. Turn the main switch in "E" position
4. Tear off the paper tape (DEL) and zero the counter
5. Encipher your message



Never reuse a message key to encipher other messages!

Deciphering

As with enciphering, we also prepare the machine in "P" position and then turn the machine (via "E") to the "D" position. Again, this causes the message key to be scrambled according to the current notch positions.

To decipher text we use the following sequence

1. Set the main switch in "P" position
2. Set the Message Key as start position on the rotors
3. Turn the main switch in "D" position
4. Tear off the paper tape (DEL) and zero the counter
5. Decipher your message

Don't forget to tear off the paper ribbon with DEL after presetting the rotors and prior to enciphering or deciphering, to avoid numerous leading spaces on the message. Always break up the rotor alignment after finishing a message and never leave these positions unattended on the machine! A good way to break up the keys is to click "Zeroize" button in "KL-7 Key Settings", and "Default" button in "Message Rotor Alignment" windows. This will reset the rotors to ABCDEFG, and the key to AAAAAAA.

The Message Indicator and Rotor Alignment

Each individual message must have its own unique random start position of the rotors, the so-called *message rotor alignment* (individual unique message key). This rotor alignment, visible through the little windows of the rotor cage, is crucial for the security of the message. Using the same message key for different messages leads to patterns that can be exploited by codebreakers to decipher a message. The use of random different rotor alignments creates a unique ciphertext for each message, even when their key settings and plaintexts are identical.

Therefore we need a way to select a random rotor alignment, and to convey it to the recipient. This is where we use *message indicator* - a randomly chosen group of letters that is sent along with the message, unencrypted and spelled-out phonetically. This message indicator is encrypted on the KL-7, and the resulting letters are used to set the rotor alignment prior to encryption. The recipient also encrypts the received message indicator on his machine, and uses the result to set his rotor alignment for decryption of this message. This way, the actual rotor alignment is never revealed in the message.

On the right the pop-up menu “Message Rotor Alignment” is shown, that is used to set the message key. One brings this menu up by mouse-clicking on the black levers underneath the rotor cage. Message rotor alignment is determined by applying a cryptographic procedure to the *message indicator*. The official procedure, as well as several useful ones, are described below. Usually random letters are selected as *message indicator*, and encrypted message indicator is used as *message rotor alignment*.



For user convenience, an option is available to set all the seven starting positions for the movable rotors from one 7-characters long string typed or pasted into the text field right of the “Set from string:” button. Clicking on the “Set from string:” button tells the program to take that given string and apply it as a message rotor alignment.

SECRET	POLLUX	4-OCT-2012	1	2	3	4	5	6	7	8
ROTOR			B	G	A	L	H	K	J	M
ROTOR ALPHABET POSITION			29	22	02	04	08	17	26	23
NOTCH RING			11	1	8		10	2	4	3
NOTCH RING POSITION			M	E	O		O+	H	E+	Z+
DAILY ROTOR ALIGNMENT			X	Y	E		I	P	E	Q
SYSTEM INDICATOR			HRCGQ	3	7	1	3			
36-45 LETTER CHECK			SDYZH	K	B	B	M	T		

Note: The ADONIS system indicator consisted of four digits, or five letters, POLLUX always used five letters as system indicator. Digital system indicators for ADONIS were encrypted with a different system provided with the key lists, often PALLAS SQUARE (somewhat similar to German Rasterschlüssel 44). System indicator for POLLUX were never encrypted (always accompanied the message in the clear). POLLUX used the letter “A” instead of “L” (like ADONIS) for the 36-45 letter check. Finally, the daily rotor alignment was not used in either ADONIS or POLLUX procedures.

Letter check. With the 36-45 letter check we can verify the settings. With the machine in “P” mode, set all rotors in the “A” position. 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.

There are several ways to communicate the message indicator. The first and second example make use of the daily rotor alignment. The third example uses an encrypted random message key without the use of a daily rotor alignment. The fourth example uses the official message indicator prescribed by *KAO-41C/TSEC KL-7 ADONIS Operating Instructions*.

We will demonstrate these methods with practical examples. Select the key settings for your KL-7 by clicking on the rotor cage or pressing F9 to call the key settings window. Adjust the settings according to the key list above (if these settings are in a file, you can just point the simulator at

that file via the "Load File" button of that menu). On the key list you see the daily basic start position, which we will use later on. One selects the daily key based on the key *cryptoperiod* (time period when this key is valid or allowed for use), and the external (unencrypted) *DTG* group (Date-and-Time Group) that was assigned to the message (using GMT time). In our examples we implicitly set cryptoperiod of each key as 24 hours starting at 0:00 Z (Zulu time = UTC = Universal Standard Time = Military Time) and ending at 23:59 Z. Other manuals and documents may specify cryptoperiod explicitly, e.g., 051140Z May 64 means 05-May-1964 11:40 UTC.

Important: all 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 is the procedure defined in *KAO-41C/TSEC* for ADONIS system. It uses a random 5-letter message indicator (rather than 7-letter), and it always uses "AAAAAAA" instead of the daily rotor alignment. For our example message, we select the random *message indicator* "KBYRD".

1. Switch the KL-7 to "P" mode.
2. Set AAAAAAA as start position on the rotors.
3. Turn the selector handle (switch mode) to "E" position (some rotors will advance one step).
4. Encipher KBYRD, the five random letters. The result should be PBWWX - the form the first five letters of the message rotor alignment (actual message key).
5. Switch the KL-7 to "P" mode. Set rotors in slots 1,2,3,5,6 to these letters. Repeat (re-use) the first two letters PB to set the remaining two rotors in slots 7 and 8. In other words, the complete message rotor alignment would be PBWWXPB.
6. Switch to "E" mode, reset the counter and press DEL to clear the paper tape.
7. Encipher the 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 OWLSU GDATE MRNIX JLLUA WYZUV IGMLN (output 30 characters)

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

```
3713 KIL0 BRAVO YANKEE ROMEO DELTA
OWLSU GDATE MRNIX JLLUA WYZUV IGMLN 3713
```

The receiving operator would observe from the system indicator 3713 that the arrived message is for ADONIS KL-7, and will select the appropriate (identified by 3713) key list. He would configure the rotor cage as prescribed by the key from this list for the given DTG, switch to "P" mode, align the rotors in the cage windows to "AAAAAAA", switch to "E" and encrypt letters "KBYRD", getting "PBWWX". He would switch to "P" again, and use "PBWWXPB" as message rotor alignment. He'd then switch to "D" and decrypt the ciphertext.

A second method is also performed with the daily rotor alignment and seven random letters. This could be done from the head (which is not recommended as humans are all but random), from a list where the used combination is stroked through, or a roll of random letters, torn off when used. Any system is good, as long as the letters are truly random and never reused. These random letters are enciphered and the result is used as message key. In our example, we have torn off the random letters RJDALPE from a roll of paper tape.

1. Switch the KL-7 to "P" mode.
2. Set XYEIQEQ, the daily basic start position from the keys sheet, as start position on the rotors.

3. Switch to "E" (some rotors will move one step).
4. Encipher RJDALPE, the seven random letters. The result should be IQWZH RQ.
5. Switch back to "P" mode
6. Set IQWZHRQ as message key on the rotors
7. Switch to "E" mode, reset the counter and press DEL to clear the paper tape
8. Encipher the message TOP SECRET MESSAGE 123 TEST

The result should be TUYGG LVNMC DGWRA LSZUF WIWPI VXCQQ

The message is sent along with the original random letters RJDALPE. You could again spell out the letters, but another way to exclude errors is to repeat the random letters. This will give:

```
3713 RJDALPE RJDALPE
TUYGG LVNMC DGWRA LSZUF WIWPI VXCQQ 3713
```

The receiver switches to "P" mode, sets the daily start position XYEIPEQ on his rotors and switches to "E" mode (NOT the "D" mode, but "E" mode as he must get the same result as the sender!). He enciphers the same random letters RJDALPE and also gets the result DHVZWNH. He switches to "P", sets his rotors according to the result letters DHVZWNH, switches to "D" and decipher the rest of the message.

A third method, without daily rotor alignment, is to take 14 random letters, for instance GEFLDHA and JALEIFG. The first group is set as a start position for the rotors. Next, the second group is enciphered and the result is used as message key.

1. Switch the KL-7 to "P" mode.
2. Set GEFLDHA, the first part of the 14 letters, as start position on the rotors.
3. Switch to "E" position (some rotors will move one step).
4. Encipher JALEIFG, the second part of 14 letters. The result should be DTVIF VU
5. Switch back to "P" mode.
6. Set the resulting DTVIFVU as message key on the rotors.
7. Switch to "E" mode, reset the counter and press DEL to clear the paper tape.
8. Encipher the message TOP SECRET MESSAGE 123 TEST

The result should be IZMBM XLXJA GLYXS USTHP LKBRL VKFTZ (output 30 characters)

Together with the message indicator, the complete message is:

```
3713 GEFLDHA JALEIFG
IZMBM XLXJA GLYXS USTHP LKBRL VKFTZ 3713
```

The receiving operator starts with exactly the same procedure to retrieve the message. He switches his machine in "P" mode, sets GEFLDHA, the first part of the 14 first message letters, as start position on his rotors, switches to "E" mode (NOT "D", as he must get the same result as the sender!) and enciphers JALEIFG, the second part of first 14 letters, which should again result in DTVIF VU. He switches back to "P" mode, sets the resulting DTVIFVU as message key on his rotors, switches to "D" and deciphers the rest of the ciphertext.

This method is very practical as it does not require a secret message key table or a list with message keys, distributed beforehand, along with the key list. A downside is that the adversary doesn't need to find out any secret start position for the rotors once he has the general key settings. This reduces his search for the correct settings with a factor 8×10^9 (7 rotors, labelled with 26 letters).

As you will have noticed, the ciphertext of all these examples is completely different, although we used exactly the same keys settings on exactly the same message. Thanks to the message key, which must be unique for each individual message, there is no relation between the three 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, as serial number and the filing time (DE = from)
Line 3, priority again, followed by the message Date Time Group (DTG)
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
3713 KILO BRAVO YANKEE ROMEO DELTA
OWLSU GDATE MRNIX JLLUA WYZUV IGMLN 3713
BT

NNNN
```

One message is allowed to contain up to 1200 encrypted 5-letter groups. If the message text is longer, it must be divided between words into parts so that no part exceeds the 1200 groups limitation. Each part must be encrypted with a different rotor alignment! Prefix plaintext to the message indicator, for example:

```
PART TWO OF FOUR KILO DELTA CHARLIE WHISKEY ZULU
```

If a message needs to be re-encrypted, it must go under a different message indicator and a different DTG. If the original DTG must accompany the message, it has to be encrypted inside the message body.

Punctuation marks are omitted or spelled out, however it is customary to use the letter X surrounded by whitespaces as period. Since KL-7 causes J to be decrypted as Y, and Z as X - letters J, Y, X, Z must be phoneticized when encrypting text such as callsigns, proper names, etc.

If a mistake has been made (e.g., a typo), type the word ERASE preceded and followed by a space, repeat the last correct word (not a number!) and continue the message from that point.

In Appendix B of the [KL-7 Help file](#) (on Dirk's Web site), you will find an exercise to decipher two messages, related to the Cuban missile crisis.

Other Message Indicator Systems

Many other solutions to communicate message keys are possible. Any good message key system should provide truly random message keys that are used only once. They are either encoded with a secret table, encrypted with an unknown daily rotor alignment setting, or both encoded and encrypted.

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 distributed beforehand to cover the expected volume of messages for a given time period.

Note that an error on one single letter of 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 letters, or to repeat the indicator groups.

Random Letters

If you consider selecting random letters for message keys, you should remember that humans are a very bad source of randomness. When keying in random letters on a keyboard, they always tend to create patterns. If you decide to select random letters manually anyway, you should use the following procedure:

Set the machine switch to P, select random start positions for all rotors, switch to E and type some random letters on the keyboard. Take the resulting machine output and use that as random letters. The machine output breaks up any patterns you might have created, giving good randomness. Never use the letters you typed in!

Security of the above methods

If the attacker dedicates efforts to break one message, then it does not matter which of the above methods is used, as the attacker would have to spend the same amount of resources regardless. The difference starts to manifest itself when secrecy of multiple messages is at stake.

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, such as the special non-moving "L" rotor, 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 settings. The default settings (rotors and base plate wiring, and shapes of the notch rings) are the same as in Dirk Rijmenants' simulator (listed in the Appendix A), so the two are interoperable.

There are two ways to provide customization:

- Use the *Rewire* command to generate new wirings for any subset of components (rotors, notch rings, base plate) either completely random or based on a provided password.
- Manually create and/or customization file, following the description below.

There are two ways to load a customization file:

- Upon each startup, the simulator looks for a file named "kl7-custom.txt" in its current/working directory. If it finds such a file, it is loaded prior to further operations.
- At any time user can press function key F7 and force the simulator to load a customization file that user selects. It can have any name.

To remove customization and revert to the original default wiring of the components (regardless of how the customization file was loaded), press function key F8. Note, that the format of customization file is the same, and it matches the format used by Dirk Rijmenants in his simulator - making these files interchangeable.

The following definitions can be used:

- "A=" through "M=" for the 13 rotors
- "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", "I", "K", "L" and "M" rotors, the connections to the rotor cage plates "P" and two notch rings "03" and "11" are defined:

```
T=Custom Settings (Test)
C=OMJ5KVVNEXFYLGBOPlQ2SR3T4UZ67C89ADHI
I=J45TF8UE7C9DW60NHKLMRIXAG1VBOPQYSZ23
K=2FZ0HG91ARL7X3MI4S6JTUOQKVWEBY5C8DNP
L=YSEQKZM5R10BNWAHVOCGXIFJ23DLPT46U789
M=BWCDZ6NM4KE827I9FG3VX0OHJLPAQRSTYU15
P=P9QNZ8LXRHIKV5AOUSCD1JM0W6T23Y47BEFG
03=110101001000101000001000001001110010
11=111011100100100111011101000000011010
```

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 "I" rotor in the example, pin 1 on its left side is connected to "J" (pin 10) on the right side. Pin 2 is connected to "4" (pin 30) on the other side, and pin 3 is connected to "5" (pin 31). 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 customization example above, the letter "P" from the keyboard is wired to contact plate pin 1 (also first pin of rotor when in A position), figure "9" connects pin 2 from the left plate to pin 2 from the right plate, "Q" from the keyboard is connected to plate pin 3 and "N" to pin 4. Standard (default) base plate (contact plate) wiring is shown below.

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

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. If you save the text file with the filename "kl7-custom.txt" in the KL-7 program folder, it will load automatically when the simulator starts. To return to the default settings for rotor, ring and cage contact plate, delete, rename or edit the "kl7-custom.txt" file, or press function key F8. By pressing F7, you can choose and load any customization file, regardless of what it is named.

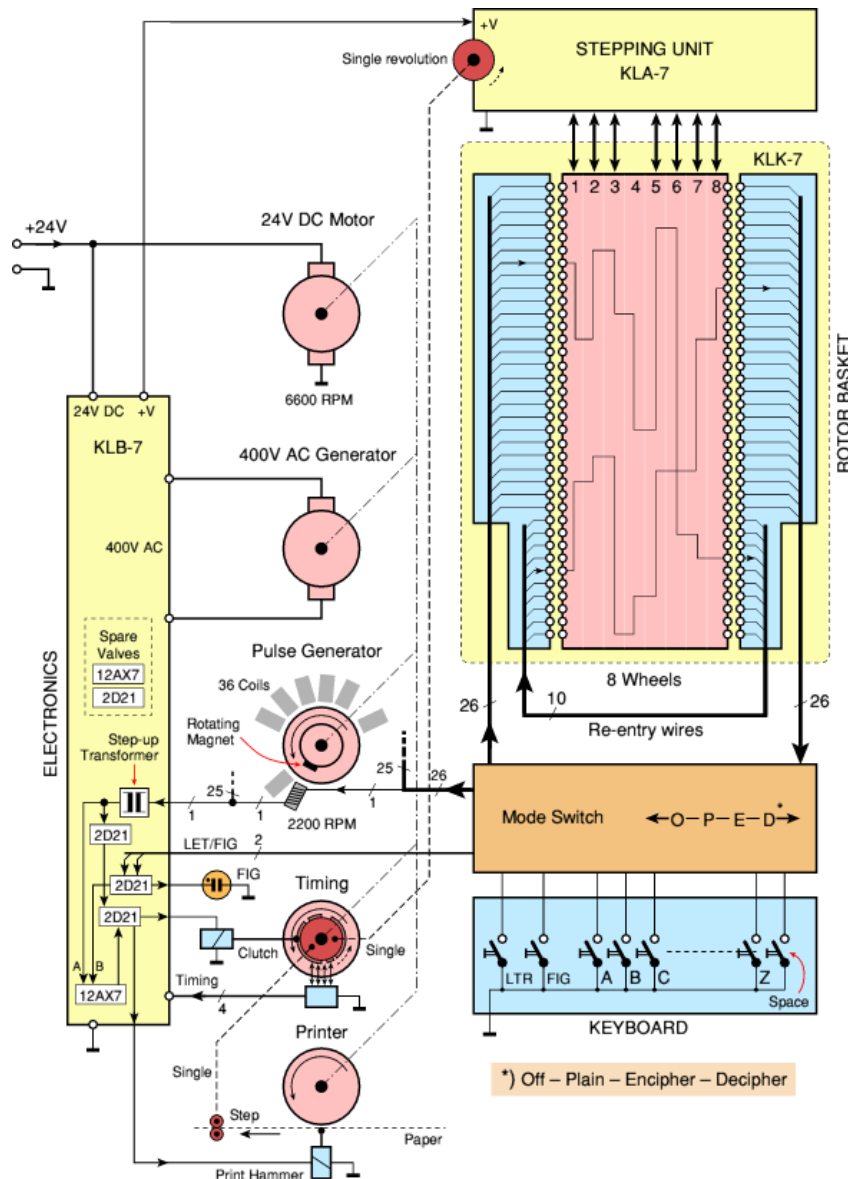
The program verifies all custom settings and, if an error is detected, the user is notified, all custom settings are discarded and the default simulator settings are loaded.

Technical details from Crypto Museum

The following data (text and drawings) are copied from the following [Web page of Crypto Museum](#) that was created and copyrighted by Paul Reuvers, all rights reserved. All the links within that text are pointing back at the original Web site.

Block Diagram

KL-7 was an electro-mechanical rotor-based cipher machine driven by electronic circuits with valves (vacuum tubes). The machine is powered by an external 24V DC source, such as a PSU or the battery of, say, a truck. Timing of the machine is provided by a [complex mechanical unit](#) with several rotating parts coupled by a common axle. The block diagram below shows how this is done. The main 24V motor runs at 6600 RPM. It drives the mechanical parts as well as an AC generator that provides the 400V to drive the valves.



Pressing a key on the [keyboard](#), grounds one of 26 lines that is routed via the [mode-switch](#), through the [coding wheels](#), to one of the 26 coils of the pulse generator. The pulses from the pulse generator are used to drive the printer. As all rotating parts (DC motor, AC generator, pulse generator, printer and stepping unit) are coupled, timing is guaranteed.

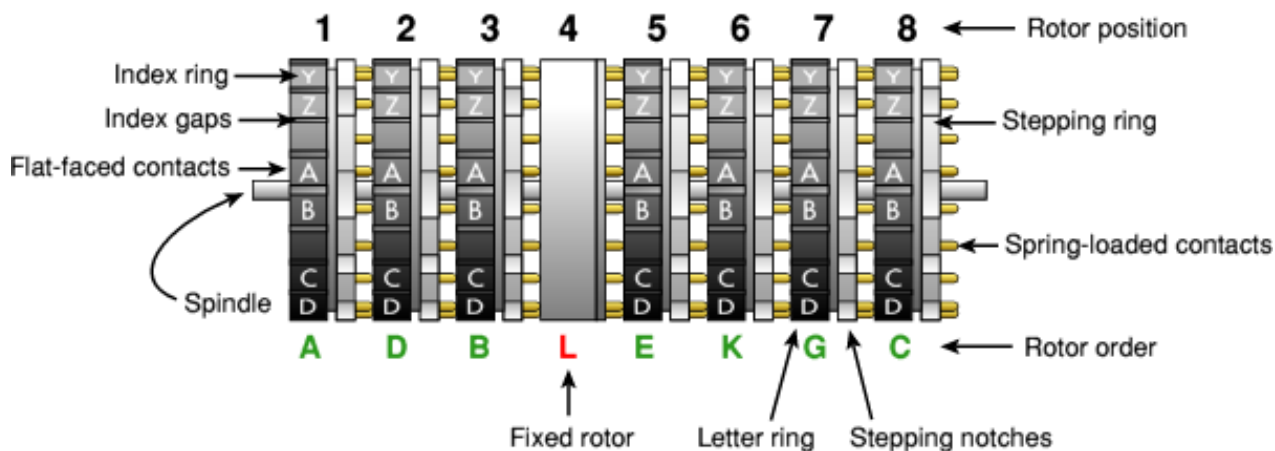
Rotors (KLK-7)

The rotors of the KL-7 resemble those of the famous German [Enigma machine](#). Each rotor has a series of flat-faced contacts on the right side, and the same number of spring-loaded contacts on the left. It also has an adjustable index ring with the letters of the alphabet on it, and an inner core which connects the contacts on one side with the contacts on the other side. There are however, some significant differences.

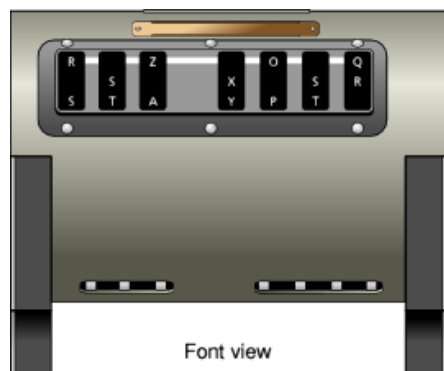
First of all, a KL-7 rotor has 36 contacts, whereas an Enigma wheel has 26 contacts. Of the 36 contacts, 26 are used for the encryption of the 26 letters of the alphabet. The remaining 10 contacts are looped back to the input (see below). This results in a re-encipherment of part of the text. Each wheel has an index ring with 36 positions, each separated by a narrow gap. Only 26 positions are identified with one of the letters of the alphabet. The rest is empty. When unfolded, the index ring looks like this:



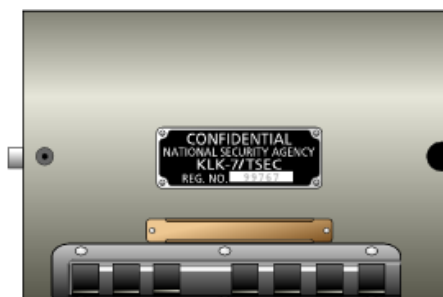
Another important difference, is the omission of the reflector (Umkehrwalze). In encoding mode, one side of the rotor basket is the input and the other side is the output. In decoding mode, all contacts are swapped, so that the output becomes input and vice versa. This has the advantage that, unlike on Enigma, a letter can become itself on a KL-7. Swapping all contacts however, does involve a rather complex multi-contact switch, which is integrated with the KL-7 keyboard.



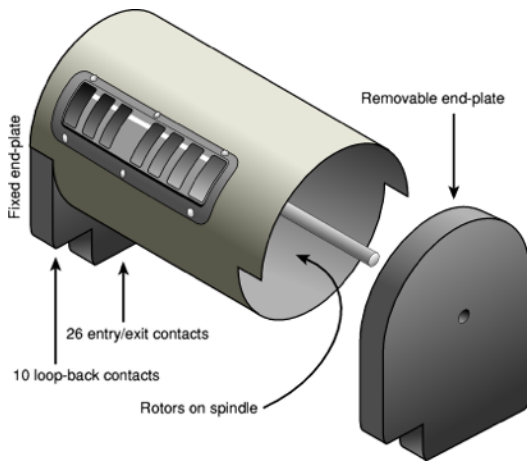
The **Drum** or Rotor Basket of the KL-7 consists of a metal cage with 8 wheels on a spindle (KLK-7). The fourth wheel from the left is fixed in position. It never rotates and hence does not have a window to show its setting. This wheel is sometimes referred to as the **NSA rotor**. For each of the other 7 wheels, a window is present in the cage. Through this window, three successive letters of the wheel are visible. The topmost letter visible through the window, represents the current setting. This position is indicated by a white line from left to right.



Front view



Top view



Each KL-7 machine was originally supplied with 12 rotors, marked **A-L**, in a metal box. In 1975 the 13th one - the **M**-rotor was added. The L-rotor was the so-called stationary¹ NSA wheel, that was used in position 4. Of the remaining 12 rotors (A-K and M), 7 would be placed in the rotor basket on a given day, in a particular order, as per cipher instructions (codebook).

The user would remove the rotor basket from the machine by releasing two levers; one at either side of the basket. Once removed, the rightmost end-plate of the basket can be removed by releasing a pawl that locks it on the spindle. After removing the rightmost end-plate, the rotors can be taken from the spindle. The spindle itself stays in the basket as it is fixed to the leftmost end-plate, that in turn is fixed to the cylindrical basket (see image above).

Rotor wiring

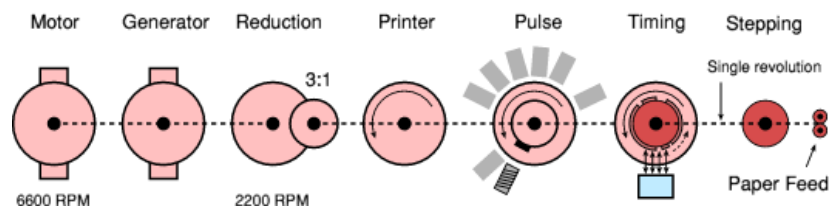
Each KL-7 wheel contains 36 wires which connect the flat-faced contacts from one side with the spring-loaded contacts at the other side, in a seemingly 'random' fashion. The wiring of the KL-7 rotors has always been kept secret, but whether or not this makes sense, remains to be seen.

According to security instructions, it was forbidden to trace the wheel wiring of the KL-7. Even technical repair personnel was not allowed to trace each individual contact for a faulty connection. They were only allowed to place the spring-loaded contacts on a metal surface and test each flat-faced contact for continuity only. This way, the wiring would not be revealed. Faulty rotors had to be sent in for repair.

If you would happen to find a KL-7 now and trace the rotor wiring, it wouldn't be of much use, as the rotor wiring was different for many of its users. Furthermore, the wiring was changed frequently for safety reasons. Nevertheless, the Russians managed to read a significant part of the US Navy Submarine Command KL-7 traffic for many years. Go to the [Web site](#) for the details.

Gear box

At the heart of the KL-7 is a very compact, yet complex, mechanical unit. It consists of a DC motor, and AC high-voltage generator, a printer, a pulse generator and a timing unit. All components are driven by the DC motor, either directly, or through a 3:1 cog-wheel reduction.



The motor and the generator are mounted on the same axle, rotating at 6600 RPM (rotations per minute). Through a 3:1 reduction, the pulse generator and printer are driven, making them rotate at 2200 RPM. Using a further cog-wheel reduction, the Timing Unit is driven.

Unlike the other components, the Timing Unit does not rotate continuously. Instead, a clutch, driven by the electronics, is used to couple it to the main axle, after which it will complete one full revolution. Whilst doing this, a set of 4 cam-controlled switches provide the timing signals for

¹ Recently declassified KAO-41C/TSEC states that the 4th slot is "stationary" (rotor in it does not step), but any rotor can be placed in the 4th slot. Instead of a notch ring, that rotor would be paired with the wide ring. Likewise, L-rotor can receive a notch ring instead of the wide ring and go to another slot (not slot 4).

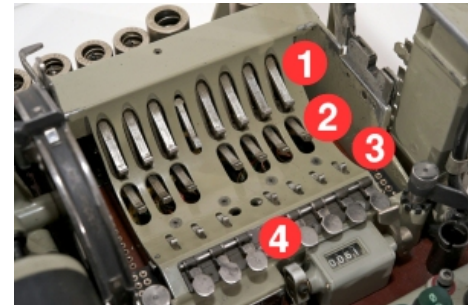
the electronics. The Timing Unit also drives the KLA-7 Stepping Unit (and hence the rotors), and the paper feed. On each revolution, the rotors can be advanced by one position.

The complex unit is housed in the left half of the KL-7, as shown in the image on the right. The motor is at the rear of the unit (at the right in the image). Immediately before the motor is the generator (sometimes called inverter), with two large bolts at the top.

The printer is the the other end of the unit (left in the picture). The black cap protects the print head and the ink ribbon against dust.

Stepping Unit (KLA-7)

The rotors are held in position by a locking lever (1). This is a spring-loaded arm that reaches under the wheel from the rear. At the end of the arm is a small sharp notch, that locks into a narrow rig (gap) between the index letters on the circumference of the wheel. Further towards the front, at the bottom of the rotor basket, is the transport notch (2). These notches are driven by the main gear and lock into the same gaps on the index ring. They move forward to rotate the wheel to the next position. On each key-press a rotor can only make a single step.



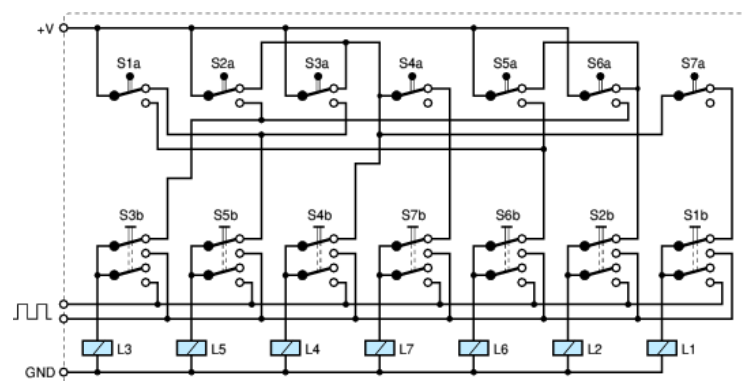
Whether or not a rotor moves when a key is pressed, depends on the presence or absence of a notch on the stepping ring of one of the other rotors. The stepping ring of each rotor is sensed by a switch (3) towards the front of the basket.

Please note that the switches sense the stepping ring 10 positions further on the circumference of the rotor. In other words: when the rotor is at **A** (visible in the window at the white line), the notch of position **H** is sensed. The switch in turn activates a solenoid (L1 thru L7) that allows the rotor to be moved by the main gear.

When setting the daily key, the starting position of the rotors can be changed manually by pressing the keys (4) whilst in plain-text mode (**P**). When the key is pressed briefly, the rotor advances a single step. Holding the key down, makes the rotor step continuously.

Rotor movement

Rotor movement control is complex, but is fixed by the internal wiring. Although details about the rotor stepping mechanism have never been published, it is possible to deduce the wiring of the switches, simply from observing rotor movement. Two European researchers who wish to remain anonymous, recently sent us a table with rotor movements as they have observed them. From this table, we have been able to reconstruct a possible wiring of the switches, which is given in the diagram on the right.



Please note that the sensing switches at the top are in the proper order (1 thru 7), but that the order of the manual stepping switches and the solenoids is mixed. This is done to make the circuit diagram less cluttered. At present, we are uncertain whether this circuit diagram is correct or not, as we have not been able to compare it with a working machine.

Keyboard

The keyboard of the KL-7 is part of the KLB-7 base unit. It consists of 29 green keys and a black space bar. It has the standard QWERTY layout divided over three rows. The numbers are shared with the top row. At the bottom right are 3 special keys marked **LET**, **FIG** and **RPT**.

Each key is in fact an electric switch, consisting of a contact and a spring, mounted below the key. Whenever a key is pressed, the contact is grounded (i.e. connected to the 0V rail), allowing the [pulse-generator](#) to issue a pulse.

When entering numbers, the user first needs to press the **FIG**-key (figures). This acts like some kind of shift-key. As long as the machine is in numbers-shift mode, a large neon lamp behind the keyboard is lit. When reverting to letters, the **LET**-key has to be pressed first.



Mode switch

A coded KL-7 message consists only of the 26 letters of the Latin alphabet. In order to allow the source text to contain letters, numbers and spaces, special tricks have to be used. This is done by surrendering a couple of letters and using them for SPACE, Letter-shift (LET) and Figures-shift (FIG). The surrendered letters are then no longer available and must be replaced by another one.

Furthermore, the operation has to be reversed when switching from encoding to decoding. All this is done with the MODE-switch that is hidden under the keyboard. The MODE-switch consists of a large pertinax board with contacts at either side, much like a PCB (but thicker).

It is controlled with a simple knob to the left of the keyboard. The image on the right shows the MODE-switch being operated. It has 4 settings: Off (O), plaintext (P), encoding (E) and decoding (D). In the picture, it is set to encoding (E). The MODE-switch also acts as the power switch.



The MODE-switch is in fact a big slide-switch. By rotating the knob, the large brown pertinax board is moved from right to left. It has 4 different positions. When pressing a key, a spring-loaded contact is pushed down onto one of the oval contact on the top side of the board. The oval contacts on the top side are connected to a different set of contacts at the bottom. The contacts at the bottom, are in turn connected with a set of fixed spring-loaded contacts in the base unit.

Pulse Generator

The timing for the printer is delivered by a pulse generator that is coupled to all other rotating parts by the main gear. The pulse generator consists of 36 coils divided over two rings, with a rotating magnet at the center. 26 coils are used for the 26 letters of the alphabet. The remaining 10 coils are for the numbers. They are each connected in series with one of the letters, but are mounted on the ring at a slightly different angle. This causes a short delay when in numbers-mode (FIG), just enough to select the next character on the printing wheel.

Printer

The KL-7 has a built-in printer with a continuously rotating print head. The output is printed on a narrow paper strip, similar to the American [M-209](#) and the Russian [Fialka](#). The printer is part of the main gear assembly on the left. The paper roll is located to the right of the printer.

The letters and numbers are all located on the circumference of the print head. When a letter is to be printed (i.e. when the pulse generator issues a pulse), the paper tape is advanced by one position and the print hammer is released.

This causes a character to be printed on the paper tape. Timing is guaranteed, as the pulse generator and the print head are driven by the same axle. Hidden under the black cap, is a small ink ribbon, that travels in between the print head and the paper tape. The hammer pushes the paper against the ribbon.

The design of the printer is nearly identical to the printer of the [SIGABA](#), the war-time predecessor of the KL-7. Like the KL-7 it featured a rotating print head with two ink ribbon reels in more or less the same arrangement. The paper strip also went under the print head.

Classified

The only items that may still be classified are the rotor basket with the rotors (KLK-7/TSEC), the stepping mechanism (KLA-7/TSEC) and the circuit diagram. All other parts are unclassified. The NSA recently released a document that describes the history of the development of the KL-7 [\[3\]](#) (the reference in on the original Crypto Museum Web page). [KAO-41C/TSEC KL-7 ADONIS OPERATING MANUAL](#) has been recently declassified, as well as the operating manual for *POLLUX*.

Some of the photographs on this page were taken at the [Royal Dutch Signals Museum](#) in 2009 shortly before the museum was closed. As becomes clear from these pictures, that machine is in beautiful condition. Unfortunately, however, the machine has been 'sanitized' and the rotors are empty. The full wiring is missing from the rotors and even the spring-loaded contacts have been removed.



Technical details from Dirk Rijmenants

This section copies text and drawings from the original Dirk Rijmenants *KL-7 Help.pdf* file (available at [KL-7 Simulator](#) Web site) and his [KL-7 Web page](#) (copyrighted - all rights reserved).

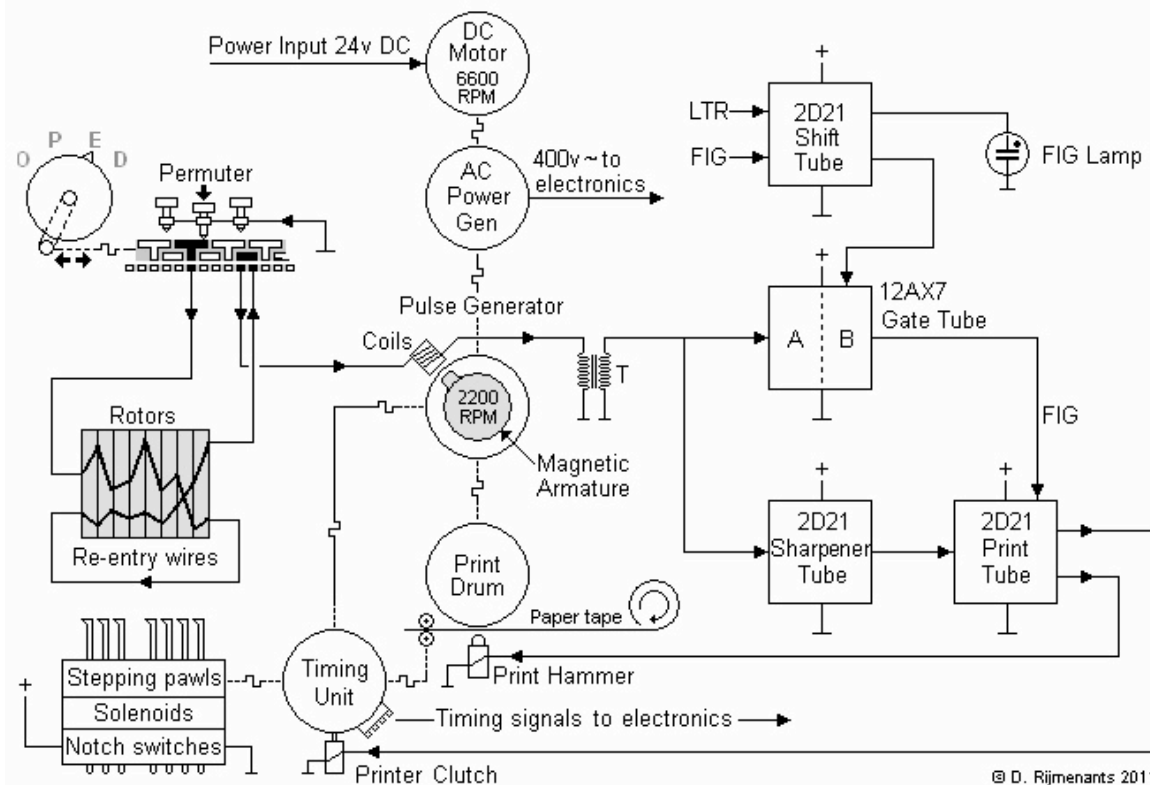
The TSEC/KL-7 is a classical off-line non-reciprocal rotor cipher machine with electro-mechanical and electronic components (vacuum tubes). The machine is powered by 24 Volts DC which drives a DC motor, which in turn drives a 400 Volts AC generator. The generator provides power to the electronics. The 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 an adjustable outer ring with letters, a wired core with the substitution wiring, 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 rotors 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 rotor from the left is always non-moving, and must be fitted with the special wide ring instead of a notch ring, and is fixed into the rotor cage. Each individual rotor (except for the one in the 4th slot) can either step once or halt after each encipher or decipher cycle.

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.

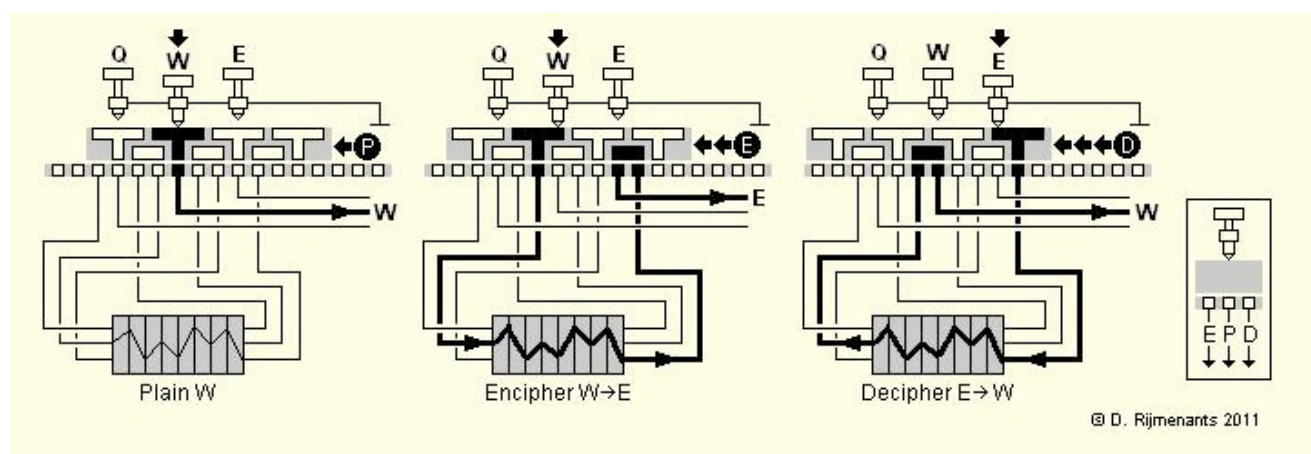
The keyboard top row letters have two pulse coils in series: a normal coil for the letter and coil with a larger core and more windings for the corresponding figure. This combination of two coils produces a double pulse of which the second pulse has a higher amplitude. In FIG mode, the shift tube will 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 switch, 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 pressing them down will ground the T-shaped contact plate at the top side of the permuter. Two rails on the permuter press down the permuter board 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 main switch has a pawl on its bottom that grasps into a vertical slot on the left of the permuter board. Turning the switch 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 neighboring 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 notch 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

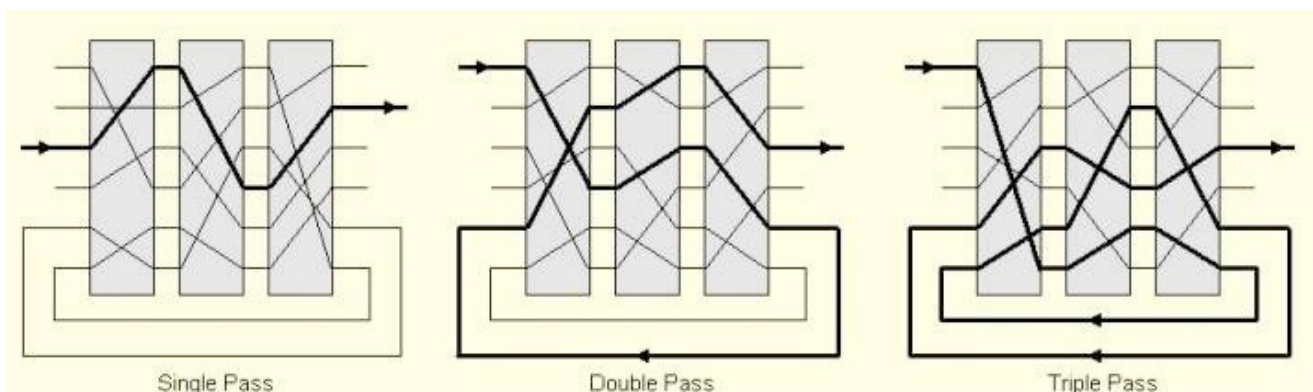
Each rotor has a wiring core with 36 contact plates on the left side and 36 spring-loaded contacts on the right side (rotors as positioned in the rotor cage). The contacts from one side are wired in a scrambled fashion with the contacts on the other side to perform a substitution encryption. The alphabet ring is permanently attached to the rotor and is adjustable to any of the 36 positions. This changes the position of the core, relative to the outer ring with letters, visible through the rotor cage window. The 36 positions on all rotors are labelled as show in the table below. Note that 10 of the positions are not labelled and left blank.

Pin	01	02	03	04	05	06	07	08	09	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 is a set of 13 rotors for each KL-7, labelled "A" through "M". The stationary rotor (fourth from the left) takes a wide ring instead of notch ring. This wide ring has two wings to fixate the non-moving 4th rotor in the rotor cage. To set the machine's key, one had to fill the rotor cage with three rotors, insert the stationary rotor, and add four other rotors. The exact rotor wiring is still classified and all surviving machines are either sanitized or their rotors are not accessible. Making a simulator that is fully compatible is therefore both impossible and pointless, as there is nothing to be compatible with. To write a realistic and functional simulation, there's no other solution than selecting our own wiring scheme for all rotors. Nonetheless, the cryptographic principles and strength of the machine are the same. The rotor wiring used in this KL-7 simulator is found in Appendix A.

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 either is passed immediately to the pulse generator through 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.



The above is a simplified example with three 6-pin rotors and 2 re-entry connections. In reality, we have eight 36-pin rotors with 36 wires each, of which 10 are re-entry wires.

Each side of the detachable rotor cage has at the bottom a 26 plates connector (coming from permuter) and a 10 plates connector (re-entry), to connect the cage with its corresponding spring-loaded contacts on the KLA-7 stepping unit. The "E and "D" connections of the 26 letters from the keyboard permuter are connected (through the KLA-7) 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
Pins	01	02	03	04	05	06	07	08	09	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 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 (i.e., after M follows M+). The fourth (non-moving) rotor must carry the wide ring. The notches and cams on these 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 A.

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. These pawls are mechanically powered by the timing unit, under controlled by the seven solenoids. At the rear of the cradle, there are eight locking pawls that prevent the non-moving rotors

Moving Rotor	Notched 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)

from moving along with neighboring moving rotors. The fourth locking pawl normally isn't used, but keeps the "L" rotor in place when testing the rotors without the rotor cage shell.

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 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 enciphers and deciphers only the 26 alphabet letters and the ciphertext is letters-only. However, the machine must process 37 different characters: the complete alphabet, the figures 0 through 9 and a SPACE. Note that the 36 characters A-Z and 0-9 have no relation whatsoever with the 36 pins on a rotor. The rotors only encrypt 26 signals and the 10 remaining wires are hard-wired for the re-entry function.

To enable the processing of 37 different characters, the KL-7 uses a special trick, also used on the five-bit teletype code. Two signals, LET and FIG, switch the machine between letters and figures. Both character sets use the same signal and they are only distinguished by the FIG (figures) or LET (letters) mode on that particular moment. The characters "QWERTYUIOP" are processed as "1234567890" in FIG mode.

This still gives 26 alpha (-numeric) keys, the additional space, LET and FIG. The KL-7 must encipher 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 enciphering, the letter "Z" is changed into "X", and the space key to the letter "Z".
- After deciphering, "Z" is translated back to a space, and the letter "X" (originally the letter "Z") remains "X".
- Before enciphering, the letter "J" is changed into "Y", and the FIG key into "J".
- After deciphering, the letter "J" is not printed, but causes the KL-7 go into FIG (numbers) mode. The letter "Y" remains "Y".
- Before enciphering, both the letter "V" and the LET key are changed into the letter "V".
- After deciphering, if the KL-7 is in the LET (Letters) mode, the letter "V" remains "V" (is printed as "V"). If the KL-7 is in the FIG mode, the letter "V" causes 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 enciphering and the second sentence is the same text after it is deciphered back into plain text. To show the changes in spaces after switching to LET-mode more clearly, the spaces in the example below are replaced by a dash:

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

Notice that only the seldom used letters "J" and "Z" are affected by the piggy-back system.

Cryptographic Strength

We can calculate the theoretical security of the KL-7 by considering the selection of the rotors, the position of the letters, relative to the wiring core, the notch ring combinations and their position, and finally the start position of the rotors.

There are 8 rotors to be selected from a possible set of 13. This gives 51,891,840 rotor combinations, ballpark of 2^{17} . The 36 positions of the 8 rotor give 2,821,109,907,456 combinations, ballpark of 2^{28} . There are 1,663,200 (ballpark 2^{14}) possible ways to select 7 notch rings from the set of 11 for the visible rotors, and they can be set in 78,364,164,096 (ballpark 2^{25}) different positions. Finally, there are 78,364,164,096 (ballpark 2^{25}) ways to set the 7 visible rotors to one of their 36 positions.

The total of possible settings on the KL-7 is found by multiplying all these results. This gives a total key size of 2^{109} possible different settings. This is good enough even for today's standards. Don't forget that, to calculate these figures, we assume that the adversary knows the machine, the wiring of each rotor (3.6×10^{322} possibilities for all rotors) and the shape of each notch ring (7.2×10^{75} possibilities for all notch rings). If these variables are unknown to the adversary, the over-all total of possible different settings is 1.2×10^{455} , which is comparable with a 1511 bit key.

Trying out all possible keys, a so-called brute force attack, on a 109-bit key is considered infeasible with present and future computer power, let alone on a 1511 bit key. 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, it still requires considerable resources and skilled cryptanalysts to mount a successful attack on the KL-7.

The biggest threat to cipher systems like KL-7 comes from "known plaintext" and "chosen plaintext" attacks, when the attacker gets a few (the more the better) plaintext copies of your encrypted traffic, or worse - can entice or coerce you into encrypting texts of his choice.

From the cryptanalyst's point of view, the main thing that matters for attacking a single message is the set of starting positions of the wiring cores, and the offset of the corresponding notch rings against them. This significantly reduces the number of the unknowns. To attack one message, even the notch rings may be ignored during the first phase of the attack, concentrating only on the relative positions of the rotors at each encryption step, and utilizing Markov's chains to cut off the impossible combinations. Given just one pair of the the plaintext and the ciphertext, recovery of the rotor positions and their steps could be of the magnitude of 2^{60} , which is within the power of the modern computers. It could be computed how long the plaintext must be to facilitate the complete recovery.

If the complete set of the original settings need to be recovered, one cannot ignore alphabet ring offsets, etc. Also, the attacker must know the wirings of the rotors, of the cage, and the configuration of the notch rings - all of which used to change periodically. This simulator fully supports complete rewiring.

Cryptanalyst's job of breaking KL-7 is formidable even in this day and age.

Appendix A

Simulator Rotor Wiring

Below the internal wiring of all 13 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 that during enciphering, 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

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	0	1	2	3	4	5	6	7	8	9	0	1	2	2	2	2	2	2	2	2	3	3	3	3	3	3		
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	0	1	0	1	1	0	0	0	1	0	0	0	1	0	0	1	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	0	1	0	0	0	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	1	0	0	0	0	1	1	1	0	0	1	1	0	1	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	0	1	1	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	0	0	1	1	0	1	1	0	0	1	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	0	0	1	0	1	0	0	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	0	1	0	1	0	0	1	0	0	1	1	1	0	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	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	0	1	1	0	0	0	0	1	0	1	0	0	0

Base Plate Wiring

Base	Q	P	O	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