

TSEC/KL-7 SIMULATOR 4.1 MANUAL

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 from 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 notched rings.

This simulator is a tribute to the ASA and AFSA engineers and cryptologist who developed the KL-7, and to the men who worked with this 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. The key settings of the simulator are saved in a small file that can be accessed and read by anyone who has access to the computer, either directly or remotely.

© Dirk Rijmenants 2011

Content

1. Operating the Simulator
2. Enciphering and Deciphering
3. Customizing your KL-7
4. Technical Details
5. History of the KL-7
6. Copyright Information & Disclaimer



Image © Paul Reuvers 2009

1. Operating the Simulator

The user interface of the KL-7 simulator software is developed to mimic the mechanical, electrical and cryptographic properties of the real KL-7 as much as possible. The hands-on approach gives you the chance to operate the KL-7 as an operator would do in real life. We start with a brief description of what the machine can do and then explain how to use all its nuts and bolts. You will notice a little hand as mouse cursor when you move over switches, machine keys or places that activate some function. All functions are called with the left mouse button, but can also be performed from the PC keyboard. 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 notched rings for each rotor and set the notched 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.

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.

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** – Plain: 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. The entered text is enciphered and the ciphertext is printed onto the paper tape. Note that the rotors perform one cycle (controlled by the notched rings) when you switch from "P" to "E" mode or from "E" to "P" mode. More about this in the chapter 2.
- **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 and this function is therefore replaced by holding down the desired letter on your PC keyboard.

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.

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 to reset it to zero.

The Rotor Cage

The rotor cage contains the 8 ciphering rotors. The position of 7 rotors is visible in the little windows. The top letter in each window, marked by the white index, is 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 notched rings on the rotors. These notched 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.

Each message requires a new random start position of the rotors, the so-called message key (this procedure is explained later). To adjust the rotor positions, set the main switch in the P position and press the black lever underneath the desired rotor. Click the lever once to cycle the rotor one step or click and hold down the mouse button to cycle the rotor automatically. Note that the paper tape advances on each step of the rotors. Therefore, the paper ribbon should be torn off (DEL) after setting the rotors in the proper position. You can memorize the current rotor positions with the INSERT key. Use the HOME key to recall the memorized rotor positions.

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 operator must select the proper rotors and position of the alphabet ring, the notched rings and their position on the rotor. The KL-7 has a set of 11 normal rotors and notched rings and one special stationary rotor without ring.

Click on the rotor cage to activate the Key Settings window and select and adjust the rotors and notched rings. You can also select F9 on the PC keyboard. There is a set of 12 rotors, labelled "A" through "L". However, the "L" rotor is a special rotor that is used only as the stationary 4th rotor. 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, and also the core position of the 4th rotor. There are 11 notched rings, labelled "1" through "11". Select a notched ring for each individual rotor and set the position of that notched ring on its rotor. With the "Save" button you save the key settings in the "KL-7.dat" file. Use the "Erase Key" button to delete the key file. An error message "File not found" will be displayed on start-up when the key has been erased.

To set their machine with the required identical crypto variables, sender and receiver used a key list. Each key list contained the proper rotors, letter ring positions, notched ring settings and a daily basic start position. The basic start position is used to encipher the message keys for the individual messages. A key list was often distributed with a so-called 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 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.

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

The Auto Typing Function

To speed up the processing of large pieces of text, 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. 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! Of course, Auto Typing is not available when the switch is in OFF position.

You can type your text directly into the textbox or load the clipboard content with the "Get Clipboard" button. In the bottom left corner you can set the speed of the autotyping. "Slow" has a speed of 0.5 character per second, suitable for 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 operators). "Fast" processes the text immediately without any delay function. This enables quick processing of large pieces of text in a blink of an eye.

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 textbox, 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. 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 resp letters, for instance ABC[SPACE] [FIG]123, while the user could type ABC[FIG][SPACE]123.

Controls Overview

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

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

2. Enciphering and Deciphering

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.

Prior to enciphering or deciphering a message, the rotors must be set in the proper start position. The rotor positions for each individual message are the so-called message key and must be unique for each message. In the message key section below is explained how you can tell the receiver of the message which message key is used.

Enciphering

It is important that the main switch is always in the "P" Plain position 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 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 Message Key after finishing a message and never leave these positions unattended on the machine!

The Message Key

Each individual message must have its own unique random start position of the rotors, the so-called message key. This message key 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 different message keys will always create a unique ciphertext, even on identical messages.

A key list usually contains the rotors, the position of the alphabet ring, the notched rings, the notched ring positions, and one single basic start position of the rotors (a seven letters group) for each day. However, there are no message keys on the key list for all the individual messages. Therefore, we need a way to select our message keys and tell the receiver which message key was used on each particular message. Of course, the message key must be kept secret, so we need a secure way to communicate each message key to the receiver. There are several basic methods to communicate the message key. The first and second example make use of the basic daily start position. The third example uses an encrypted random message key without the use of a daily rotor position.

We will demonstrate three different message key systems with practical examples. Select the key settings for your KL-7: click the rotor cage or press F9 to call the key settings window. Adjust the settings according to the key list below. On the key list you see the daily basic start position, which we will use later on.

POLLUX 27 OCT 1962	1	2	3	4	5	6	7	8
ROTOR	E	H	F	L	I	A	G	B
ROTOR ALPHABET POSITION	04	28	04	16	09	32	08	11
NOTCHED RING	5	10	6		7	1	8	3
RING POSITION	04	34	25		09	03	27	14
BASIC START POSITION	X	E	G		B	V	E	Q
36-45 LETTER CHECK	NAQAD TYKXR							

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 method is performed with the help of the daily basic start position and a secret message key table, distributed beforehand. Such a table has a large number of truly random message keys which are identified by a row and column header system or by some multi-letter code. There are many ways to construct such tables, but they basically converted a message key into another letter combination. In our example, we found message key "ADXSKHO" and its code "EFGVL" in the secret message key table.

1. Switch the KL-7 to "P" mode
2. Set "XEGBVEQ", the basic daily start position from the key list, as start position on the rotors (align the rotor letters with the white index line on the rotor cage).
3. Switch to "E" position (some rotors will move one step)
4. Type in "EFGVL", the code that represents the message key from the secret table. The result should be "AMWLF". This group will be the first, spelled out, group of our message.
5. Switch the KL-7 back in "P" mode
6. Set the message key "ADXSKHO" as start position on the rotors.
7. Switch to "E" position, reset the counter and press DEL to clear the paper tape
8. Encipher the message "TOP SECRET MESSAGE 123 TEST"

The result should be "MULNO ADHJI WBACD QILQR NUEZT QWUS"

Together with our encrypted message key code (spelled out), the complete message will be:

ALPHA MIKE WHISKEY LIMA FOXTROT
MULNO ADHJI WBACD QILQR NUEZT QWUS

The receiving operator (who of course already has the appropriate machine key settings for that day) switches his machine in "P" mode, sets the daily start positions "XEGBVEQ" on his rotors and switches to "D" mode. Next, he decipheres the spelled out group "AMWLF", which results into "EFGVL". He looks up the code "EFGVL" in his secret message key table and finds out that it refers to the message key "ADXSKHO". He switches back to "P", sets "ADXSKHO" as start position on the rotors, switches to "D" and types in the ciphertext to decipher it back into the original plaintext message.

Another way to transmit the five letter code "EFGVL", representing messages key "ADXSKHO", is without encryption. This option should only be used when enough different message key are available and they are not reused. This system is suitable when only a few messages are sent each day.

A second method is also performed with the daily basic start position 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 "POFUXLS" from a roll of paper tape.

1. Switch the KL-7 to "P" mode
2. Set "XEGBVEQ", 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 "POFUXLS", the seven random letters. The result should be "HYECP EU".
5. Switch back to "P" mode
6. Set "HYECPEU" 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 "QPGDN BIJGU FRLOF ARYHA QDGSN NVYS".

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

```
POFUXLS POFUXLS
QPGDN BIJGU FRLOF ARYHA QDGSN NVYS
```

The receiver switches to "P" mode, sets the daily start position "XEGBVEQ" 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 "POFUXLS" and also gets the result "HYECPEU". He switches to "P", sets his rotors according to the result letters "HYECPEU", switches to "D" and deciphers the rest of the message.

A third method, without daily start position, is to take 14 random letters, for instance "DXGFTRK" and "ICXFGRT". The first group is set as 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 "DXGFTRK", 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 "ICXFGRT", the second part of 14 letters. The result should be "APLIR HJ"
5. Switch back to "P" mode
6. Set the resulting "DQSRCGK" 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 "OKJLU TVCGD YBTWX MVJTT OXDMT AYER"

Together with the message key, the complete message is:

```
DXGFTRK ICXFGRT
OKJLU TVCGD YBTWX MVJTT OXDMT AYER
```

The receiving operator starts with exactly the same procedure to retrieve the message. He switches his machine in "P" mode, sets "DXGFTRK", 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 "ICXFGRT", the second part of first 14 letters, which should again result in "DQSRCGK". He switches back to "P" mode, sets the resulting "DQSRCGK" as message key on his rotors, switches to "D" and deciphers the rest of the ciphertext.

This last 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 three 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.

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 and are either encoded with a secret table, encrypted with an unknown daily rotor start setting or both encoded and encrypted. Note that an error on one single letter of the message key will result in completely unreadable text. Care has to be taken to avoid errors in conveying the message key or Indicator to the receiver, for instance by spelling out the letters or by repeating the groups.

In Appendix B, you will find an exercise to decipher two messages, related to the Cuban missile crisis.

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!

3. Customizing your KL-7

During its service time, the rotors of the KL-7 were recalled and re-wired 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 notched 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 custom settings are activated on each start-up. To customize your KL-7, you simply create a text file called “custom.txt” and place it in the KL-7 program folder.

The following definitions can be used:

- “A=” through “K=” for the 11 normal rotors
- “L=” for the special stationary rotor
- “P=” for the rotor cage contact plates (left and right are identical)
- “01=” through “11=” for the 11 notched rings

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

```
T=MY CUSTOM KL-7 SETTINGS
C=JCX8OW5QTYSI3PVU60BZHER42DM9KNGF7L1A
L=T9HEMYSIOW51AUZK0BF7L2N6DJCX3PVR4QG8
P=VER24D5QT6UH8YSIOJCX7L1AW0BZ3PM9KNGF
04=00110101000101100010011001010100010011
11=010001101010110100001100000110010101
```

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

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

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

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

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

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

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

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

4. Technical Details

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

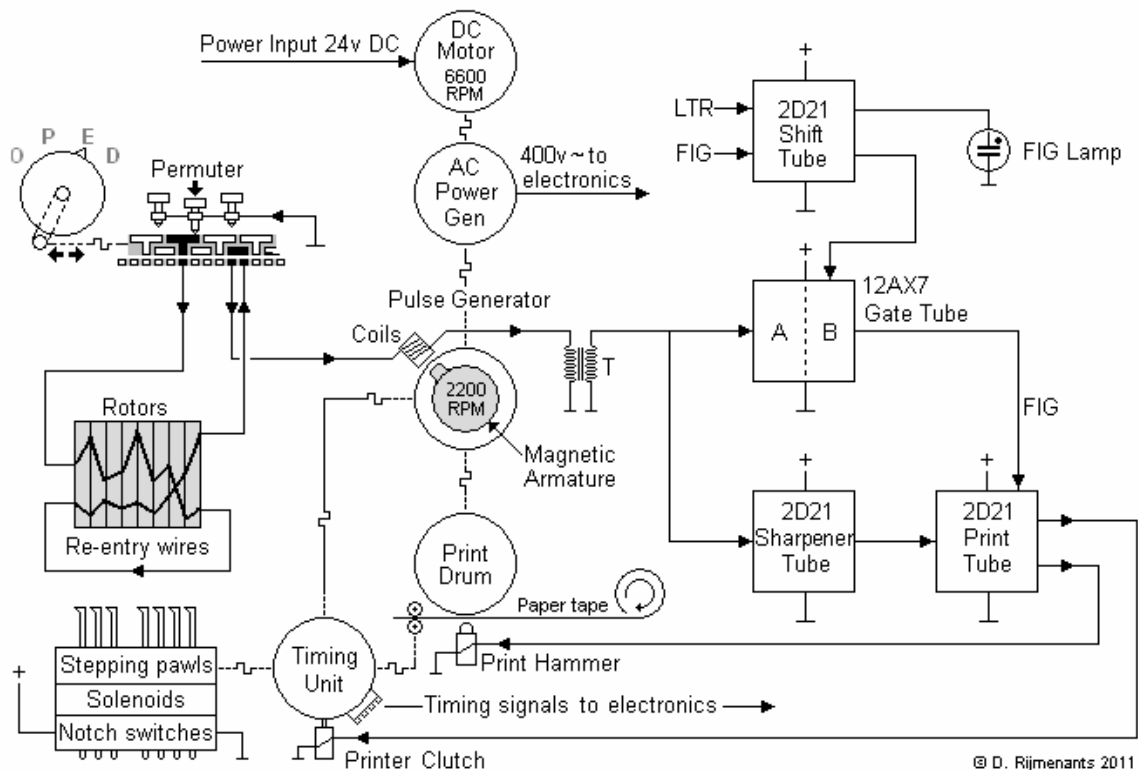
Each rotor has an adjustable outer ring with letters, a wired core with the substitution wiring, and a white notched ring. The notched rings activate switches in the KLA-7 stepping unit that control the stepping of the rotors. The secret key settings comprise the selection and order of 8 rotors from a set of 12, the position of the letter rings on the rotors, and the selection and position of 7 notched rings from a set of 11. The fourth rotor from the left is always the special non-moving "L" rotor and can only be placed in one fixed position in the rotor cage (the wiring core however is adjustable). Each individual rotor 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.

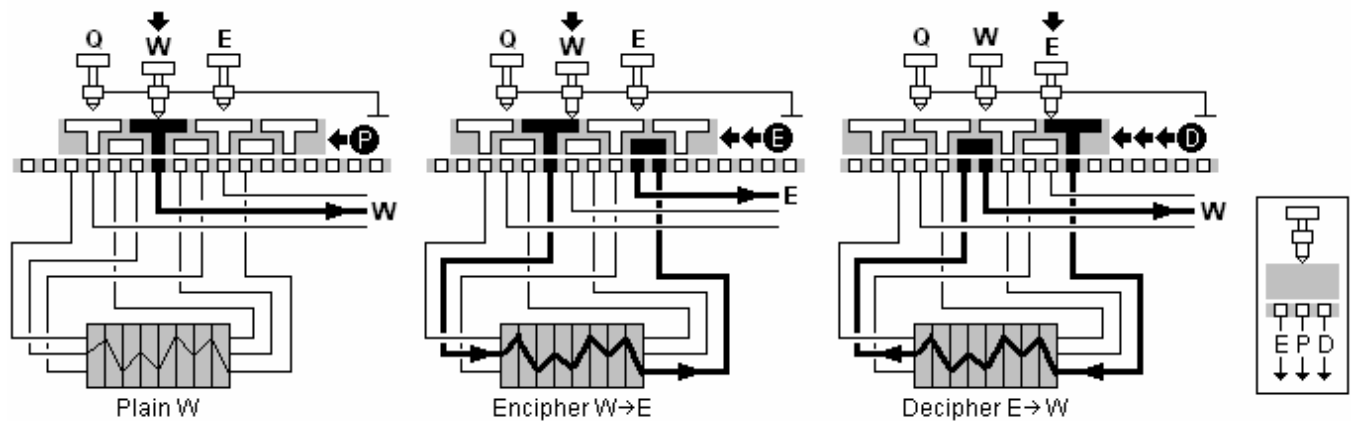
The keyboard top row letters have two pulse coils in series: a normal coil for the letter and coil with a larger core and more windings for the corresponding figure. This combination of two coils produces a double pulse of which the second pulse has a higher amplitude. In FIG mode, the shift tube will 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 neighbouring T-shapes for each key enables the O-P-E-D sequence from right to left.



© D. Rijmenants 2011

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

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

The Rotors

Each rotor 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 enciphering. The alphabet ring of the rotor is adjustable in 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 because only letters are used to represent the rotor position.

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

There is a set of 12 rotors for each KL-7, labelled "A" through "L". The stationary rotor (fourth from the left) is always the special "L" rotor. To set the machine's key, one had to fill the rotor cage with three rotors, insert the "L" 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

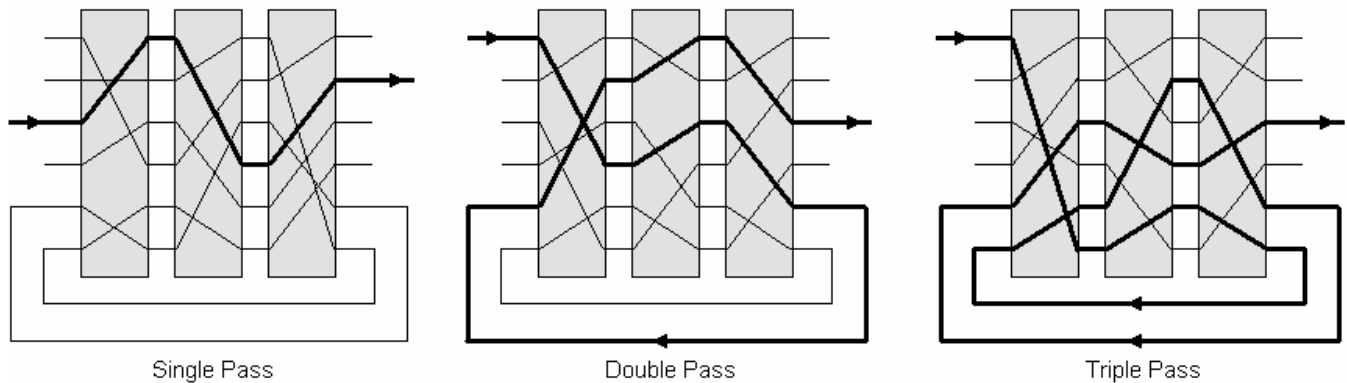
Making a simulator that is fully compatible is therefore impossible and pointless, as there is nothing to be compatible with. To write a realistic and functional simulation, there's no other solution than selecting our own wiring scheme for all rotors. Nonetheless, the cryptographic principles and strength of the machine are the same. The rotor wiring, as used in the KL-7 simulator, is found in Appendix A.

The Notched Rings

The KL-7 had a set of 11 white plastic notched rings, labelled 1 through 11. The notched rings are responsible for the highly irregular movement of the rotors. As part of the key settings, seven of them are attached to the rotors, in any of 36 positions (the 4th rotor doesn't carry a notched ring because it never moves). The notches and cams on these rings control seven stepping switches in the KLA-7 stepping unit. These notched 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 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 (through the permuter) to the pulse generator along one of the 26 wires, or it leaves the exit rotor on one of the 10 re-entry contacts. In the latter case, the signal is sent back to one of the 10 re-entry contacts at the entry rotor, to perform a new pass through the rotors. When the signal leaves the exit rotor again, the situation is repeated. Depending on the internal wiring and current position of the rotors, the signal performs one or more passes (theoretically up to 10 passes) through all rotors before leaving the exit rotor towards the pulse generator. This results in a most complex signal path that constantly changes in both number of passes and its way through the rotors.



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

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

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

The Printer Mechanism

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

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

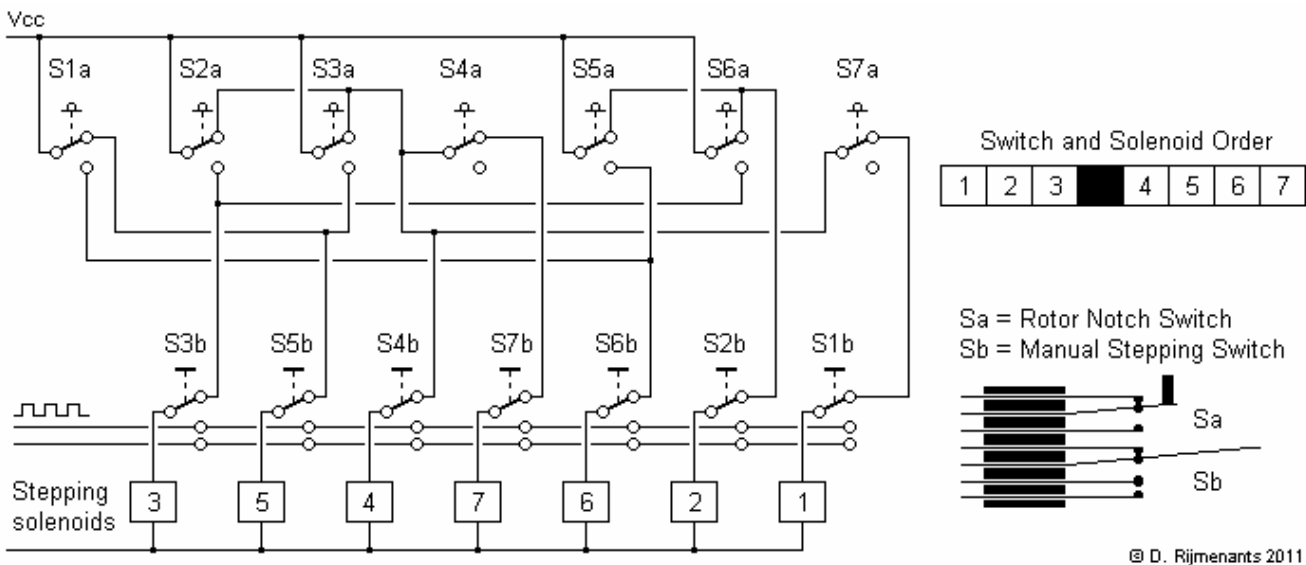
The Stepping System

The KLA-7 stepping unit holds the rotor cage and controls the stepping of the rotors. On the front of the cradle, there are seven levers to manually advance each individual rotor. Behind them are seven cams that read the notched rings of the rotors. These cams control the seven pile-up switches of the stepping logic, connected to the solenoids. In the middle of the cradle are the seven stepping pawls to advance the rotors. They are mechanically powered by the motor but controlled by the seven solenoids. At the rear of the cradle, there are eight locking pawls that prevent the non-moving rotors from moving along with neighbouring 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.

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

Stepping 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)

Knowing the operation of the machine's KLB-7 base unit and the composition of the unwired switches, we can put this in a schematic which uses only the available components, a solution as most likely incorporated in the KL-7:



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

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

On the KL-7, the stepping of a single rotor is controlled by two or three separate notched rings. Two notched rings can produce a maximum period (unique movement sequence) of 1,296 and three rings a theoretical maximum period of 46,656. This is for one single rotor. The combination of seven notched 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 these 36 characters A-Z 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 and 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 into the letter "Z". After deciphering, "Z" is translated back into a space and the letter "X" (originally the letter "Z") remains an "X".

Before enciphering, the letter "J" is changed into "Y" and the FIG key is changed into "J". After deciphering, the letter "J" is not printed, but causes the KL-7 to go into FIG mode. The letter "Y" remains "Y".

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

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

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

Cryptographic Strength

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

There are 7 rotors to be selected from a possible 11 (the 4th rotor is always the same). This gives 1,663,200 rotor combinations. The 36 positions of the 8 rotors (also the 4th rotor) give 2,821,109,907,456 combinations. There are 1,663,200 possible ways to select 11 notched rings for the visible rotors, and they can be set in 78,364,164,096 different positions. Finally, there are 78,364,164,096 ways to set the 7 visible rotors to one of their 36 positions. Note that although there are only 26 labels on the rotors to set a message key, the system of stepping rotors when switching from "P" to "E" mode makes it possible that a rotor could be in a position that carries no alphabet label at the start of a message.

The total of possible settings on the KL-7 is found by multiplying all these results. This gives a key size of 4.79×10^{46} possible different settings. This is comparable with a 156 bit key, which is enormous, even for today's standards. This key size comprises all possible settings the user can change on the KL-7, and assuming that the adversary doesn't know these variable settings, but he has all technical details of the machine, knows the internal wiring of each rotor (3.6×10^{322} possibilities for all rotors together) and the shape of each notched ring (7.2×10^{75} possibilities for all notched rings). If these fixed properties are unknown to the adversary, the over-all total of possible variables 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 156 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.

5. History of the TSEC/KL-7

Development of the machine

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

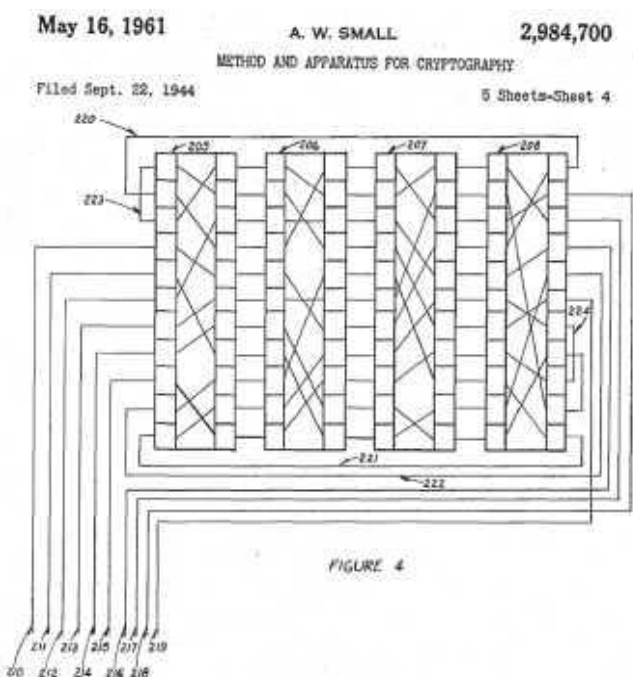
The project was designated MX-507 and ASA saw it as a long-range research project. The ASA researchers quickly decided to opt for a rotor-based machine. A design with 36-point rotors came on the forefront. They also had to design a completely new lightweight printing system, as the new machine was required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

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

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

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

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



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

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

The KL-7 in Service

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

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

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

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

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

Major Security Breaches

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

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

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

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

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

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

More about the John Walker spy case:

<http://www.fas.org/irp/eprint/heath.pdf> US Navy analysis on security weaknesses, exploited by John Walker
http://www.trutv.com/library/crime/terrorists_spies/spies/walker/1.html John Walker at Crime Library.

The KL-7 simulator website:

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

6. Copyright Information & Disclaimer

Copyright Information

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.

© Dirk Rijmenants 2008-2011

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

Appendix A

KL-7 Simulator Rotor Wiring

Below the internal wiring of all 12 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*
01-29	01-23	01-19	01-15	01-13	01-26	01-20	01-28	01-25	01-08	01-15	01-08
02-27	02-19	02-26	02-26	02-04	02-34	02-19	02-19	02-06	02-31	02-13	02-18
03-14	03-26	03-28	03-36	03-02	03-27	03-09	03-23	03-35	03-01	03-36	03-15
04-08	04-16	04-36	04-13	04-16	04-14	04-32	04-05	04-12	04-28	04-23	04-33
05-35	05-02	05-06	05-01	05-17	05-02	05-36	05-17	05-21	05-20	05-06	05-07
06-04	06-13	06-25	06-31	06-30	06-01	06-02	06-36	06-22	06-06	06-21	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
08-11	08-35	08-18	08-33	08-05	08-36	08-33	08-14	08-32	08-05	08-18	08-16
09-05	09-21	09-27	09-03	09-33	09-11	09-12	09-16	09-20	09-33	09-31	09-34
10-13	10-04	10-10	10-32	10-07	10-09	10-28	10-20	10-23	10-21	10-20	10-23
11-20	11-17	11-05	11-21	11-29	11-35	11-04	11-21	11-30	11-30	11-01	11-36
12-03	12-31	12-01	12-23	12-08	12-18	12-10	12-07	12-18	12-12	12-24	12-27
13-25	13-25	13-32	13-17	13-09	13-15	13-03	13-12	13-01	13-04	13-10	13-12
14-33	14-03	14-09	14-29	14-36	14-12	14-24	14-22	14-16	14-14	14-35	14-24
15-18	15-18	15-11	15-07	15-35	15-04	15-29	15-11	15-31	15-15	15-19	15-19
16-15	16-27	16-33	16-22	16-23	16-07	16-16	16-35	16-11	16-34	16-28	16-13
17-07	17-12	17-23	17-20	17-34	17-29	17-22	17-13	17-24	17-07	17-07	17-02
18-12	18-34	18-17	18-24	18-25	18-08	18-18	18-15	18-13	18-35	18-08	18-03
19-34	19-36	19-29	19-12	19-20	19-23	19-30	19-01	19-33	19-16	19-26	19-14
20-16	20-10	20-12	20-10	20-22	20-19	20-17	20-32	20-07	20-18	20-12	20-29
21-17	21-30	21-13	21-14	21-28	21-03	21-07	21-08	21-36	21-29	21-29	21-01
22-01	22-06	22-02	22-30	22-15	22-30	22-34	22-18	22-09	22-22	22-22	22-06
23-09	23-07	23-16	23-19	23-01	23-20	23-15	23-33	23-34	23-25	23-25	23-32
24-30	24-15	24-15	24-28	24-19	24-17	24-23	24-04	24-02	24-26	24-30	24-10
25-24	25-28	25-35	25-04	25-24	25-28	25-31	25-09	25-10	25-36	25-05	25-25
26-23	26-01	26-08	26-35	26-27	26-21	26-25	26-29	26-08	26-11	26-09	26-30
27-02	27-11	27-24	27-05	27-10	27-22	27-27	27-26	27-26	27-23	27-02	27-09
28-32	28-33	28-22	28-08	28-11	28-05	28-01	28-24	28-29	28-19	28-27	28-05
29-10	29-29	29-30	29-06	29-06	29-25	29-21	29-25	29-15	29-03	29-16	29-28
30-19	30-20	30-03	30-09	30-12	30-33	30-26	30-34	30-17	30-02	30-04	30-17
31-06	31-32	31-34	31-16	31-32	31-16	31-08	31-10	31-04	31-13	31-17	31-22
32-26	32-24	32-14	32-27	32-26	32-13	32-05	32-06	32-28	32-27	32-03	32-31
33-36	33-05	33-07	33-02	33-14	33-24	33-13	33-03	33-14	33-24	33-34	33-04
34-22	34-22	34-20	34-11	34-03	34-06	34-35	34-30	34-03	34-10	34-14	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
36-21	36-09	36-04	36-18	36-31	36-32	36-14	36-31	36-05	36-09	36-33	36-35

* The "L" rotor is the special stationary rotor, designed to be placed as 4th rotor from the left.

KL-7 Simulator Notched Rings

Below the notched 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	3	4	5	6	7	8	9	0	1	2	3	4	5	6			
1	1	0	0	0	1	0	0	0	0	1	0	0	0	1	1	0	1	0	1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	0	1			
2	0	0	1	1	0	1	0	1	0	0	0	1	0	1	1	0	0	0	1	0	0	1	1	0	0	1	0	0	1	0	1	0	0	0	1	0	0	1	
3	1	1	0	0	0	0	1	1	0	1	0	0	0	0	1	0	0	0	1	0	0	0	0	1	0	1	0	1	0	1	0	1	0	1	0	0	1	0	
4	1	0	1	0	0	0	1	0	0	1	0	0	0	1	1	0	0	1	0	1	0	0	0	0	1	1	1	0	0	1	1	1	0	1	0	0	0		
5	1	0	1	0	0	1	1	0	0	0	1	0	0	0	1	0	0	0	1	1	0	0	1	0	1	0	1	0	1	1	0	0	0	0	1	1	0		
6	0	0	0	0	0	1	1	1	0	0	1	1	0	0	0	1	0	1	0	0	0	1	1	0	1	1	0	1	1	0	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	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	1	0	0	0	0	1	1	0	1	1	
9	1	1	1	0	1	0	1	1	0	0	0	0	1	0	0	1	1	0	0	1	0	1	0	0	1	0	0	1	0	0	1	1	0	1	1	1	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	0	1	0	0	1	1	0	0	1	1	0
11	1	1	0	0	1	0	0	0	0	1	1	0	0	0	1	0	1	1	0	0	0	1	0	0	0	1	0	0	1	1	0	0	0	0	1	0	1	0	0

Appendix B

The Cold War Running Hot – The Cuban Missile Crisis

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

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

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

Sources:

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

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

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

Deciphering the Messages

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

The proper enciphering procedure is the second method, as found in the “Enciphering and Deciphering” chapter earlier in this paper. That procedure uses the random message key, enciphered with the basic start position. With the rotors in the basic start position, re-encipher the spelled-out message header to retrieve the secret message key. Use that message key as start position to decipher the rest of the message. Optionally, you could copy and past the ciphertext into the KL-7 Auto Typing window, to avoid having to type the complete ciphertext message by hand.

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

POLLUX 27 OCT 1962	1	2	3	4	5	6	7	8
ROTOR	E	H	F	L	I	A	G	B
ROTOR ALPHABET POSITION	04	28	04	16	09	32	08	11
NOTCHED RING	5	10	6		7	1	8	3
RING POSITION	04	34	25		09	03	27	14
BASIC START POSITION	X	E	G		B	V	E	Q
36-45 LETTER CHECK	NAQAD	TYKXR						

VZCZCBLE014 UU
OO RUCSSOZ
DE RUYNBCD 014 27/1810Z
O 271755Z OCT
GR 131

BT
ECHO ZOULOU INDIA YANKEE WHISKEY LIMA XRAY
USYHJ TKRFS FIDHC IEXTL LTCMV XURWW TSNBC QBMMT MCVKN YAUUU
ESWDT LBXZL MVCPL RTGPH QADQB UJFJY INRRB XERGO ETMFM LGZYZ
BYCUF LDGYN QWCDT UFJWD AMHAN BUBLM WTXRB YTEDL KPJSB MICSA
DRHCR FEDDD ELLAQ TYLBC IDHAS HSTYQ UQKRS OEBUM ZHFAZ CMDRN
DTQGP GASGQ OWMZD FRQFZ YMZSC VWECJ KZPUT RJUBT FZYDP HOJXJ
PKTWR SYTXS KTESA ECCZW UNEAC ZDUDI GPGZF XXRBU OMIJM XRRCB
OHUDU IERNE CAAWR JIDHZ QEGCQ TMCJQ CKGIZ QYJST XAZMS TVHBW
IBCPZ FYKRD ZJMGB KZTAR MOWLL FUOBP FVCAS LXIZC TLIOG LOUCZ
YBLUQ TLZDB WDRYX TXMEE ENKNN IERBE QNISY AJWBI NNDJF VGSTV
XOUNL FCRFB FIJMV QTRXP ESCWH DPDUD GEIVO TWZKG XNEDR LYATD
RIHON TSKQJ PGCEO RDOAY CHKUD DSTYR RZTTG IPVKZ VPZFO TONOC
USAJM IDTSR FNOPJ OJQVR MKECK UZPTZ MBBOQ WENZL OFZHX CWTJJ
IZDUP BYTTI EEZQM CUNOW BJYUZ AMSUQ CLIWV SXAKB ZJCRP OVWZA
DRNAB
BT

NNNN

VZCZCBLE023 UU
OO RUCSSOZ
DE RUYNBCD 023 27/2325Z
O 272310Z OCT
GR 164

BT
FOXTROT BRAVO MIKE KILO TANGO NOVEMBER OSCAR
AXFUF SIVVU OMYBX MQCBG JCEPR KUTOC HULPE BBBWT GDSZI NJPYY
MTAQO AHSFS CMQRK ALLGY EXWBU EKWNK BWHBN LPIQQ ZLTLD AKRAG
ZMHHN OWXVF BSTJW WRMLC SYABZ GXDBY AHAPJ MPVSM NEKWU QYRBX
QUCDN INKVQ ICGGX TIAOJ FROUG XTDEZ BWPCO RYZSY YQEKW RWRUB
KCFQW WYNTZ YVQAP SRFJJ FOCWH PDYVU QDMRZ UDZBX IOQTA VHxEE
SJYXY ELJKK QHVFN PZHBY XVOMH VEBMC ITFBW MNUFX GNUYB JZZGM
VNIFO YPFVW IZBUO YPUVR TIBWU CHDDI YVBVY CZICX HVRSO DNBDZ
NDWfy NIHHK IDLOJ NXIKZ XZGBS DTSBS IDHSM KHOSB ZDTGO CGMAO
PHHXG PVTWJ PMHHS QJBXA LKGLD TYAVB YHRTG FXQJT EBVDV RNLNQ
HQGKJ GPALK HGKTP XYBBO BLRNB ZTFPJ LGDHB FMNHG STDKL XJKGZ
KBZRJ RGZLP UTYLU LVTMH SRDSU DTSLI ADKAI UOGZZ ZYKIU KSOU
BZXRL YXJZP AKXOX AVSLW QOCKL RWKKQ BAGWB GOJXS RKBWO QFJZK
NWTAI SJEYB WEKTH ISWAF XAQJU XPUSD RTPWT XTAPC VRQJZ XZOSE
PSDKF DJFIS UZDAI GUFXS KDYMV XXGKK OWLLJ EGHTN YQYEL RWXEB
QSNDT HSCOE YFCAB EOWQR APFWB YUZQX SMXCG IFNPJ CWUDW HGDRQ
HROJP SEATK UHZRZ FDIWL ZCDVE CGODD FOMWB UCOAV LISXZ IILZNQ
SMYCH SOOUR CMJRS QDOZX
BT

NNNN

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