Unit 179
SIGABA

SIGABA, also known as *Electric Cipher Machine Mark 2* (*ECM II*), *M-134-C, ASAM 1*, or *CSP-889*, is a rotor machine used by the United States during and after World War II. In this machine, the signal for a plaintext letter passes through five rotors, similar to those of the Enigma. But there is no reflector, and the stepping of the rotors is controlled by a complicated process. There are ten rotors from which to choose the *cipher wheels*; the other five serve as *control wheels*. In addition, there are five smaller, ten-contact rotors, called *index rotors*, which help in determining the irregular stepping of the cipher wheels. See Figure 179.2 for an overall functional view of the machine.

The ten large rotors are numbered 1 to 10 (or 11 to 20, or 21 to 30, etc.). In the codebooks, rotor 10 is referred to by "0". Each of these has twenty-six contacts on each side and is labeled on the rim with the letters of the English alphabet, like those of the Enigma machine. In code books, they are referred to by the second digit only. The alphabetic permutations of these rotors are listed in Table 179.1. These rotors can be inserted into a slot in either forward or reverse ("R") orientation, i.e., a rotor can be turned over so that the signal travels in the reverse direction through it. This does not invert its alphabetic permutation, but does an inversion and a reflection (B↔Z, C↔Y, etc.). We leave it as an exercise to work out the alphabetic permutations of the reversed rotors.

Figure 179.1: SIGABA. Photo by United States Air Force.

The small rotors are labeled on their rims by two-digit numbers. The first digit identifies the rotor, and the second is its current setting. These serve as index rotors to help scramble the signals that control the stepping of the cipher wheels. They are removable and replaceable in any order, but during WW II they were kept in numerical order (1, 2, 3, 4, 5). These rotors are not reversible and do not rotate while encryption or decryption is occurring. Their wirings are given in Table 179.2.

The overall function of the machine during encryption is as follows. The operator presses a letter or space key on the keyboard. The machine translates Z to X and space to Z. A signal on the wire designating the plaintext letter runs through the five cipher wheels from first to fifth. The signal emerges from the fifth wheel on the wire designating the ciphertext letter. Then four signals are sent into the first control wheel, on lines F, G, H, and I. They pass through the control wheels in reverse direction, some logic circuits whose actions are listed in Table 179.4, through the index rotors, then more logic (Table 179.5), and out to control the stepping of the cipher wheels. Any cipher wheel that receives a signal steps; if the rotor is inserted in the forward direction, then it steps to the alphabetically preceding letter; if it is inserted in the reverse direction, it steps to the following letter. After the cipher wheels have advanced, the center control wheel advances one step. If it passes from O to N in the forward orientation, or from O to P in the reverse orientation, then the control wheel in the fourth slot advances one step. If it, too, passes from O to an adjacent letter, then the control wheel in the second slot advances one step. The wheels in the first and last slots do not rotate.

The cipher is not self-reciprocal like the Enigma, so in order to decrypt, signals must pass through the cipher wheels in the reverse direction. Stepping, and the control of it, of course, is the same as in the encryption process.

The internal configuration of the SIGABA serves as its daily key. It includes

- the choices and ordering of five rotors as cipher wheels (five numbers, 0-9)
- the orientation (forward or reverse) of each of the five cipher wheels
- the choices and ordering of five rotors as cipher wheels (five numbers, 0-9)
- the orientation (forward or reverse) of each of the five control wheels
- the ordering of the five index wheels (five digits, 1-5)
- the settings of the five index wheels (five digits)

The lists of five cipher wheels and five control wheels must include all ten of the large rotors; none can appear more than once in the key. Here is an example of a daily key as it might appear in a codebook:

day	control	cipher	index
today	4 1R 9 0 3R	2 6R 5R 7 8	13 26 34 42 59

For each new message, the operator chooses five letters at random for the control-wheel settings and derives the settings of the cipher wheels from them (see below). These ten letters serve as the message key, although the operator only needs to send the control-wheel settings to the receiver.

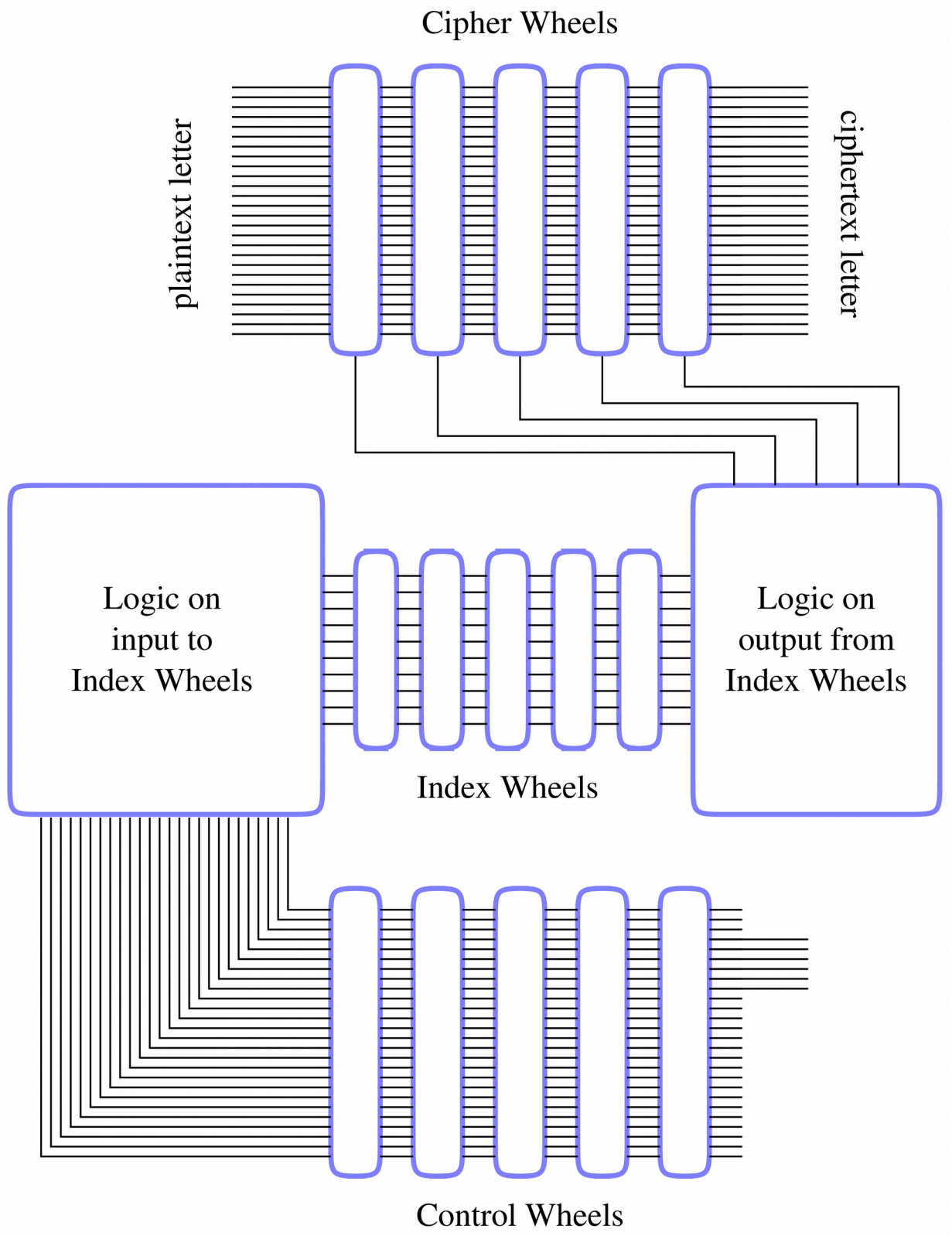

Figure 179.2: Functional overview of SIGABA.

rotor	input ABCDEFGHIJKLMNOPQRSTUVWXYZ
1	INPXBWETGUYSAOCHVLDMQKZJFR
2	WNDRIOZPTAXHFJYQBMSVEKUCGL
3	TZGHOBKRVUXLQDMPNFWCJYEIAS
4	YWTAHRQJVLCEXUNGBIPZMSDFOK
5	QSLRBTEKOGAICFWYVMHJNXZUDP
6	CHJDQIGNBSAKVTUOXFWLEPRMZY
7	CDFAJXTIMNBEQHSUGRYLWZKVPO
8	XHFESZDNRBCGKQIJLTVMUOYAPW
9	EZJQXMOGYTCSFRIUPVNADLHWBK
[1]0	YCHLQSUGBDIXNZKERPVJTAWFOM

Table 179.1: Alphabetic permutations of the SIGABA cipher and control rotors, in forward orientation and at position A*.*

rotor	input 1	2	3	4	5	6	7	8	9	10
1	8	6	10	2	5	9	3	7	4	1
2	4	9	2	1	6	10	3	8	7	5
3	5	1	9	7	2	6	4	3	10	8
4	4	10	9	1	6	3	7	2	8	5
5	7	5	10	8	2	4	6	3	9	1

Table 179.2: Wirings of the SIGABA index rotors. Permutations listed are for rotors in position 0*.*

inputs		output
0	0	0
0	1	1
1	0	1
1	1	1

Table 179.3: The logical OR *operation. The output of* OR *is on (*1*) if either input is on, and off (*0*) if both inputs are off.*

input line to index wheels	logical expression
1	OFF
2	B
3	C
4	D OR E
5	F OR G OR H
6	I OR J OR K
7	L OR M OR N OR O
8	P OR Q OR R OR S OR T
9	U OR V OR W OR X OR Y OR Z
10	A

Table 179.4: Logic applied to input to the index wheels in CSP-889. The first column contains the number of the control line entering the index wheels. The second column is the logical expression applied to the output of the control wheels.

control line for stepping cipher wheels	logical expression
1	(1) OR (10)
2	(8) OR (9)
3	(6) OR (7)
4	(4) OR (5)
5	(2) OR (3)

Table 179.5: Logic applied to output from the index wheels. The first column contains the number of the control line determining the stepping of a cipher wheel. The second column is the logical expression applied to the outputs of the index wheels, where "(n)" indicates the signal on line n.

Some attention should be spent explaining how the cipher-wheel settings are derived from a five-letter message key. First, the operator sets all of the large rotors to the letter O. Start with the control wheel in slot 1 and advance it one letter (if in forward orientation, then one earlier letter alphabetically; if in reverse orientation, then one letter later alphabetically). Then send the signal on the four lines (F, G, H, I) through the control wheels (in reverse direction), logic circuits, and index rotors and allow them to advance the cipher wheels as if the machine were in normal operation enciphering a text. Continue with this procedure until the control wheel in slot 1 is set to the first letter of the message key. Note that if that letter is O, then it must take 26 steps and go all the way around. Now advance the control wheel in slot 2 until it shows the second letter of the message key, and advance the cipher

wheels after each step. Do the same for the remaining three wheels. Any time the target is O, the wheel must go all the way around. When the procedure is finished, the letters showing on the cipher wheels are the second half of the message key. Suppose we start with the example daily key:

day	control	cipher	index
today	4 1R 9 0 3R	2 6R 5R 7 8	13 26 34 42 59

Choose five random letters as the first half of the message key: WICSO. Remember that when one of them is O, that wheel must go all the way around. With the given internal settings, the procedure gives us PUJRC as the cipher-wheel settings.

Now we can attempt an example of encryption using the daily key above and message key WISCO. We already know that the initial cipher-wheel settings are PUJRC. Start with a plaintext:

THIS MESSAGE IS ENCRYPTED WITH SIGABA

The first step is to replace all Zs with X (there are none), then all spaces with Z:

THISZMESSAGEZISZENCRYPTEDZWITHZSIGABA

To encipher the first letter, let us find the alphabetic permutation for the cipher-wheel bank. We know what rotations are, from Table 20.1. The reflection that we need has this permutation:

$$X = (\text{AZYXWVUTSRQPONMLKJIHGFEDCB})$$

This is b_{25} in Table 54.1, and is the same as $R_1 \circ z$ or $z \circ R_{25}$, where, as you recall, z is the reversal of the alphabet. A signal first enters the cipher-wheel bank into rotor 2 which is in forward orientation and set to P (=15). The effect of this rotor is $R_{15}^{-1} \circ W_2 \circ R_{15}$ (we have kept the notation of "W" for "wheel"). The signal then passes through rotor 6, which is in reverse orientation and set to U; its action is $R_{20} \circ X \circ W_6^{-1} \circ X \circ R_{20}^{-1}$ (notice where the inverses of rotations appear, and that X is its own inverse). Considering all five rotors in the cipher bank, the action of the entire bank is (where we have decided to drop the symbol for composition) (remember that things work from right to left in operator notation)

$$\begin{aligned} P_{\text{cipher}} &= (R_2^{-1}\, W_8\, R_2)\,(R_{17}^{-1}\, W_7\, R_{17})\,(R_9\, X\, W_5^{-1}\, X\, R_9^{-1})\,(R_{20}\, X\, W_6^{-1}\, X\, R_{20}^{-1})\,(R_{15}^{-1}\, W_2\, R_{15}) \\ &= R_{24}\, W_8\, R_{11}\, W_7\, R_1\, z\, W_5^{-1}\, z\, R_{11}\, z\, W_6^{-1}\, z\, R_{16}\, W_2\, R_{15} \\ &= (\text{CETVLDQWOUZFYIHPMRJABNGKSX}) \end{aligned}$$

The first plaintext letter is therefore enciphered to A. We now have to find the stepping of the cipher wheels. To do so, we find the permutation for the control-wheel bank. We apply the same technique as above to find it when the wheels are set to WICSO.

$$\begin{aligned} P_{\text{control}} &= (R_{14}\, X\, W_3^{-1}\, X\, R_{14}^{-1})\,(R_{18}^{-1}\, W_0\, R_{18})\,(R_2^{-1}\, W_9\, R_2)\,(R_8\, X\, W_1^{-1}\, X\, R_8^{-1})\,(R_{22}^{-1}\, W_4\, R_{22}) \\ &= (\text{CPKVFDZLIBOEQAJHSTXYGNWMRU}) \end{aligned}$$

Remember that the signals pass through the control bank in reverse direction, so we need the inverse of the permutation:

$$P_{\text{control}}{}^{-1} = (\texttt{NJAFLEUPIOCHXVKBMYQRZDWSTG})$$

The inputs on lines F, G, H, and I are mapped to E, U, P, and I. From Table 179.4, we see that the active inputs to the index-rotor bank are on lines 4, 6, 8, and 9. We now have to play the same game with the index-rotor bank. With our key, the overall permutation of the index rotors is

$$\begin{aligned} P_{\text{index}} &= (R_9{}^{-1}\, I_5\, R_9)\,(R_2{}^{-1}\, I_4\, R_2)\,(R_4{}^{-1}\, I_3\, R_4)\,(R_6{}^{-1}\, I_2\, R_6)\,(R_3{}^{-1}\, I_1\, R_3) \\ &= R_1\, I_5\, R_7\, I_4\, R_8\, I_3\, R_8\, I_2\, R_3\, I_1\, R_3 \\ &= (1\ \ 4\ \ 7\ \ 8\ \ 9\ \ 5\ \ 10\ \ 3\ \ 6\ \ 2) \end{aligned}$$

where now the rotations are of ten items and I_n represents the n^{th} index rotor's permutation, from Table 179.2. We see that the inputs (4, 6, 8, 9) are mapped to outputs on lines 8, 5, 3, and 6. From the logic in table 179.5, we find that the cipher wheels that step are in slots 2, 3, 4, and 5. Because the wheels in slots 2 and 3 are in reverse orientation, they advance to the next letter alphabetically; so U goes to V and J to K. The wheels in slots 4 and 5 are in forward orientation, so they advance to the previous letter alphabetically; R to Q and C to B. The cipher wheels are now set to PVKQB for the encipherment of the second letter. The center control wheel advances, so the control bank is now set to WIBSO. We can find the new permutation of the cipher-wheel bank:

$$\begin{aligned} P_{\text{cipher}} &= (R_1{}^{-1}\, W_8\, R_1)\,(R_{16}{}^{-1}\, W_7\, R_{16})\,(R_{10}\, X\, W_5{}^{-1}\, X\, R_{10}{}^{-1})\,(R_{21}\, X\, W_6{}^{-1}\, X\, R_{21}{}^{-1})\,(R_{15}{}^{-1}\, W_2\, R_{15}) \\ &= (\texttt{KCAIXJTBFLRMUPDHZYNWSGVEQO}) \end{aligned}$$

The second letter of the plaintext, H, is enciphered to B. If we continue in this manner, we find that the full ciphertext is

ABOTTYSYZJAQWNETZPSCCUQMUFSPJRUJTDUEI

A later version of the SIGABA machine, known as *CSP-2900*, is similar to the CSP-889, with these differences:

- The set of active lines into the control wheels is expanded to six: D, E, F, G, H, I.
- The logic applied to the output of the control wheels to form the input to the index wheels is modified to be what is listed in Table 179.6.
- The cipher wheels in slots 2 and 4 rotate in the opposite direction to those in slots 1, 3, and 5, which rotate as in CSP-889.

input line to index wheels	logical expression
1	U OR V
2	B
3	C
4	D OR E
5	F OR G OR H
6	I OR J OR K
7	L OR M OR N OR O
8	S OR T
9	W OR X OR Y OR Z
10	A

Table 179.6: Logic applied to input to the index wheels in CSP-2900. The first column contains the number of the control line entering the index wheels. The second column is the logical expression applied to the output of the control wheels.

Reading and references

Mark Stamp and Richard M. Low, *Applied Cryptanalysis: Breaking Ciphers in the Real World*, Hoboken: Wiley, 2007, section 2.4.

George Lasry, “Functional Description of SIGABA.” This document can be found in the supplementary materials for some challenges on MysteryTwister, in this zip file: https://mysterytwister.org/media/challenges/add/mtc3-kopal-25-SIGABA-CSP889-01-add.zip

George Lasry, “A practical meet-in-the-middle attack on SIGABA,” Proceedings of the 2nd International Conference on Historical Cryptology, HistoCrypt 2019, Linköping University Electronic Press, 2019, 41-49, https://ep.liu.se/ecp/158/005/ecp19158005.pdf

> Note that the above paper has an error in the table of index input logic. The following paper has the correct table.

George Lasry, “Cracking SIGABA in less than 24 hours on a consumer PC,” *Cryptologia* 47:1 (2023) 1-37, DOI: 10.1080/01611194.2021.1989522

Timothy J. Mucklow, The SIGABA/ECM II Cipher Machine: “A Beautiful Idea,” Center for Cryptologic History, [U.S.] National Security Agency, 2015, https://www.nsa.gov/portals/75/documents/about/cryptologic-heritage/historical-figures-publications/publications/technology/The_SIGABA_ECM_Cipher_Machine_A_Beautiful_Idea3.pdf

Operating Instructions for ECM Mark 2 and CCM Mark 1, transcribed at https://maritime.org/doc/crypto/ecm/index.php

Crypto-operating Instructions for ASAM 1, transcribed at https://maritime.org/tech/ecminst.php

Programming tasks

1. Create a function that finds the alphabetic permutation of a reversed rotor. Tabulate the reversals of the ten rotors in Table 179.1.

2. Implement enough of the machine in Python so that you can find the initial cipher-wheel settings when given a five-letter message key.

3. Add the remaining pieces to simulate the entire SIGABA CSP-889. Inputs should be the daily and message keys and, of course, the plaintext. Allow for the message key to have five or ten letters.

4. Now simulate the CSP-2900.

Exercises

1. Find the cipher-wheel settings for these five-letter message keys for the CSP-889 version of SIGABA, given today's daily key (see above in the text of this unit for the key).

   a. `SMFCJ`

   b. `OTCDP`

   c. `XGDRF`

2. Encipher this text with version CSP-889 and today's daily key and message key `MSRZN IVLDO`. Do not include punctuation, and remember to replace spaces with `Z` in the plaintext, if your program does not already do so.

   > Science shall extend the bounds of knowledge and power, adding unimaginable strength to the hands of men, opening innumerable resources in the earth and revealing new secrets and harmonies in the skies.
   >
   > (from "The Glory of Peace" by Charles Sumner, in *Standard Selections*, edited by Robert I. Fulton, Edwin P. Trueblood, and Thomas C. Trueblood)

3. Decipher this text with version CSP-889 and today's daily key and message key `NRJCK`. Remember that `Z` in the plaintext is space.

```
QMNTJQSULAPPIQHXDDKDBVFALCMOAYVXGJKRYGHOGVJHKMLUCLEAHBBKNTFWBQNI
QVHILLUHFSEBSALAGJIJEZLSHWXSOKAMWSAVEMXQRGHXMRKATEUDUTHAYILMYJBG
JNYCFKOWVKRGZTKJHTOEYEDPNAVLPYCKBSZROQZNXNZZCMNPSRKDLAYORMERYYKE
YDFCYUHQJJSXIPJDYLXOJXYXTTSCADSRATQNVXUSUGBQIVIVCMNFQJAETNGXMVHT
TJVCUKAUXEMGWYESDFKGXSKKLCXLYHLQXQLGTBUAFKTJZTLQDKXHEHOZVRUMUSJD
MMMIXOABZXXQDPZNWONRILGWLDOMWZOKEPRJUFEROUCIGNQBGHGKBCZKEIKINDCU
CQZZYXICWOBKENPNXAONRJKHKXECLQCUGLOZMCIQOSJLXCLBGAIWPEBJFTZALQUZ
XUJPNYTKQPBKDUUGLITRBIJYMZWZERSNQXMIBEDYJFFVMRZJDWSJTYGJJMZBQAIZ
ZWMAJZCZTQCZHTVASCFEXXOMQLCJDQOCEPIGTLGAIXSSVOKWTWPDDDZHTMVYSXIP
KXMGGEQDBOLZHBEYNFDEHGLPLQLNHREYREOFJTZQTYZOCHMNPBQFF
```

4. Decipher with version CSP-2900, the following daily key, and message key `ZIHMF`.

day	control	cipher	index
tomorrow	9R 8R 2 5 3R	0R 7 4R 1 6	29 30 18 58 44

```
RCWWMQXIVNASRUDGPRFKXLOYMUFUKDHHWEZBDMDVKARBUNPBBMEIMPEZPVUTILMO
NIBVQSAJPQPJHUKUYSDXXUVBFRULWVDCADCRDXFJOYHTZLKRQSNSJGBCVBRUEWKV
RXWEQHBDLFCEJQJSIEAUQCWRUZNRFOVMIUVFETDSSRLHCDAHUIFDMYVHUPPEUGHH
ERDCITZSSVRQOSHAMPENKJKDAHZRLXHTCYGCHONEFTQMDNQGEYGHKQJEHKXWSCWQ
ELMBVPPPWLEFCWRSEHOEZGXFBYRQWIDEDONXLMECOTYFHEMNWLAWSDDGSKEJKSUR
IYDPJKLXKUKBCFIDSRVJJYVFDMEQDYDMZGZJVAEJVRSOTLODMQYKPSYHKOPPVNQI
KUSRTKOPSLOMWKCREVIIJMGOQPZOBTJFKSBFZMUKSOUGFMODAWRREWANHPPSMRWY
YAHRAUVSGOBABIHTYVSWFVIMCEYEDWVQRURYQZBIQVZKPIOINSMKABDDHFNZBVTA
NVSDZYOILCBMDRIELW
```