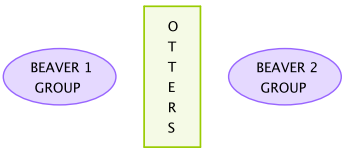
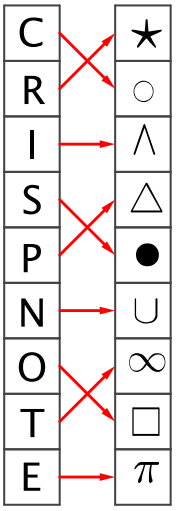


Problem of the Week
Problem D and Solution
Say What?



Problem

The Beavers are playing a game with the Otters. The Beaver 1 group needs to communicate secretly with the Beaver 2 group, but their message will pass through a zone controlled by the Otters. The Beavers decide to use a mechanism called the B-Enigma machine to encrypt (disguise) their messages while sending them from one side to the other. The device has two rotors. As described below, the left rotor moves after a letter is typed. The right rotor never moves.

The following is a description of how the B-Enigma machine works.

The machine begins in the START position illustrated in the diagram up to the right. A letter on the left rotor is encrypted to the corresponding symbol on the right rotor. If, for example, P is the letter typed first from the START position, it will be encrypted as $\triangle$. After typing the first letter, the left rotor will move up one position. The top letter moves down to the bottom. A second letter is typed and encrypted to the symbol on the right rotor. If, for example, O is typed second, it will be encrypted as $\cup$. After typing the second letter, the left rotor will move up two positions. The top two letters will move to the bottom and stay in the same order. A third letter is typed and encrypted to the symbol on the right rotor. If, for example, R is typed third, it will be encrypted as ∞. After typing the third letter, the left rotor will move up three positions. The top three letters will move to the bottom and stay in the same order. A fourth letter is typed and encrypted to the symbol on the right rotor. If, for example, T is typed fourth, it will be encrypted as $\star$. After typing the fourth letter, the left rotor will move up four positions. The top four letters will move to the bottom and stay in the same order.

The procedure and pattern repeat until the SEND button (not shown) is pressed. After a message is sent, the left rotor automatically returns to the START position. Our four-letter message was PORT and it was encrypted $\triangle \cup \infty \star$.

The Beaver 1 Group sends the message "TOP SECRET SCRIPT" and then presses SEND. Assuming the left rotor is in the START position and spaces in the message are ignored, what is the encrypted message received by the Beaver 2 Group.

Solution

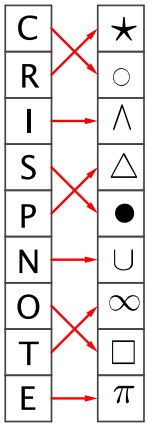
Let the START position of the left rotor be Position 0. If the left rotor is in Position 1, the letters have moved 1 position up from their initial position. If the left rotor is in Position 2, the letters have moved 2 positions up from their initial position. In fact there are actually only 9 positions that the rotor can be in. If the rotor moves 9 positions it will be back in the START position again. If the left rotor has moved 9 positions or more, we can determine its position relative to the START position by subtracting multiples of 9 from the total number of moves until we obtain a position number from 0 to 8.

The table allows us to determine where the left rotor is when a letter is encrypted. For example, when the O is encrypted, the left rotor is in Position 1 and the O is encrypted $\cup$. When the I is encrypted, the left rotor has moved a total of 78 positions. The closest multiple of 9 to 78 is 72 so, relative to the START Position, each letter has moved $78 - 72 = 6$ positions. Using the Position 6 illustration below, the letter I is encrypted $\cup$.

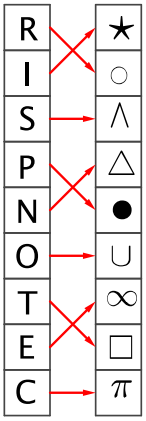
Letter to Encrypt	Number of Positions Moved before encryption	Position Relative to START Position	Letter is encrypted to
T	0	0	∞
O	0+1=1	1	$\cup$
P	1+2=3	3	$\star$
S	3+3=6	6	$\square$
E	6+4=10	10-9=1	∞
C	10+5=15	15-9=6	$\bullet$
R	15+6=21	21-18=3	∞
E	21+7=28	28-27=1	∞
T	28+8=36	36-36=0	∞
S	36+9=45	45-45=0	$\bullet$
C	45+10=55	55-54=1	π
R	55+11=66	66-63=3	∞
I	66+12=78	78-72=6	$\cup$
P	78+13=91	91-90=1	$\bullet$
T	91+14=105	105-99=6	$\star$

It turns out that we only need four positions of the left rotor relative to the START position. We need position 0 (START Position), position 1, position 3, and position 6.

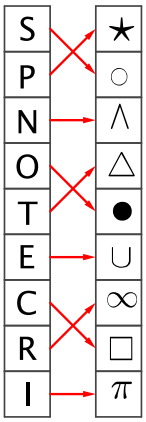
Position 0



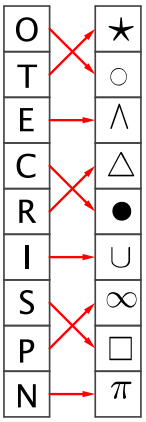
Position 1



Position 3



Position 6



The message TOP SECRET SCRIPT is encrypted $\infty \cup \star \square \infty \bullet \infty \infty \infty \bullet \pi \infty \cup \bullet \star$.

The message SCRIPT TOP SECRET is encrypted $\bullet \pi \infty \cup \bullet \star \triangle \cup \triangle \bullet \infty \square \triangle \infty \star$.

See the next page for further discussion and comments about this problem.

For Further Thought

- How would the Beaver 2 group decrypt (decipher) the message?
- When the rotor moves $n + 9m$ positions from the start position, $0 \leq n \leq 8, n \in I$, $m \geq 1, m \in I$, its final position will be n positions from the start position. A study of modular arithmetic could help if you wish to explore this further.
- In our example, there were 9 letters on the left rotor and 9 symbols on the right rotor. The cycle of positions used on the left rotor only caused positions 0, 1, 3, and 6 of the left rotor to be used. Is there a size of rotor so that every position of the rotor would be used in the encryption process? Experiment with a few different sizes.