Rail Fence Cipher

Overview: Cryptography is the writing and decoding of secret messages, called ciphers. Now for governments, these secret ciphers are a matter of national security. They hire special cryptanalysts who work on these ciphers using cryptanalysis. The secret is that solving substitution ciphers can be pretty entertaining! Ciphers are published daily in newspapers everywhere. If you practice encoding and decoding ciphers, you too can become a really great cryptanalyst.

Materials

- Pencil
- Paper

Activity: In this lesson, let's take a look at how to code and decode the Rail Fence Cipher. Here's your original message: MEET ON THURSDAY

Now write one letter on the top row and one on the bottom row, alternating as you go so it looks like this:

M   E   O   T   U   S   A

   E   T   N   H   R   D   Y

Now group the letters in groups of 5 so that it's harder for a snooper to break it:

MEOTU SAETN HRDY

Notice that the last group of 5 only has four letters. Fill the last spot with an optional letter like a Q or Z:

MEOTU SAETN HRDYQ

That's the message you send to your friend! Don't forget to tell them how you encoded it so they can break it easily.

Once they've received your message, they need to decode it. Here's how to do it:

Count up the letters and separate them into two equal groups:

MEOTU SA   ETNHRDYQ

Place the first group on top of the second, and space the letters apart a little:

M   E   O   T   U   S   A

   E   T   N   H   R   D   Y   Q

Now use a zigzag pattern to pull the letters off one at a time, starting with the M at the top left. Follow it by the first letter on the bottom row, then the second letter on the top, then the second on the bottom, and so forth until you have the entire message.

MEET ON THURSDAY Q   (You can ignore the last letter Q.)

Now it's your turn! Work out the exercises below. (You'll find answers at the back of this book.)

Exercises

Write the cipher of the following message:

1. COME TOMORROW AT 2PM
2. HE HAS ARRIVED AT THE AIRPORT
3. HE IS CARRYING A BAG
4. THEY ARE HERE NOW
5. COME AT MY PLACE

Write the cipher of the following message (use a three row zigzag)

6. COME TOMORROW IN MY OFFICE
7. LEAVE THEM BEHIND
8. WE WILL BE THERE SOON
9. The cipher below was encoded using a two rows zigzag method with six letters in every row. Decode it.
   IMOIG OACMN NW
10. The cipher below was encoded using a three rows zigzag method with four letters in every row. Decode it.
    ICINA ONOMM GW

Answers to Exercises: Rail Fence Cipher

1. CMTMR OA2MO EOORW TP
2. HHSRI DTTAR OTEAA REATI PR
3. HICRY BGESA RAAXZ
4. TEAEE EOHYR HRNWZ
5. CMAMP AEOET YLCXZ
6. CEMRI YFEOT OONOI MORWM FC
7. LVHBI EEEEN ATMHD
8. WIBHE OELEE SNWLT ROXQZ
9. I AM COMING NOW
10. I AM COMING NOW