

1) Decoding a Message

- The message was coded using a basic shift cipher (caesar cipher)
- Create some algorithm to attempt to decode the message
 - Try all 25 shift values with a sample test and print out the results.
 - Use letter frequency analysis to make educated guesses about the shift amount.

Here's my Decoded Code in Python in repl.it

<https://replit.com/@arobinson1/Decode-message-caesar-cipher#main.py>

2) Encoding a Message: (Sending the message)

- Select a symmetric cipher other than shift/caesar cipher.
- Create a program or design an algorithm to take a string and encode it using a simple written method.

Transposition Cipher

I will use a **transposition cipher**. A transposition cipher is one in which the order of the characters is changed to obscure the message). One modern transposition cipher is done by writing the message in rows, then forming the encrypted message from the text in the columns.

Encrypt the message "Meet at three pm today at the usual location " using rows of 6 characters.

M	E	E	T	A	T
T	H	R	E	E	P
M	T	O	D	A	Y
A	T	T	H	E	U
S	U	A	L	L	O
C	A	T	I	O	N

The encoded message would be:
MTMASC EHTTUA EROTAT TEDHLI AEAELO TPYUON

The spaces would be removed or repositioned to hide the size of table used, since that is the encryption key in this message.

0:55 / 10:22

Encrypt the message "Meet at three pm today at the usual location" using rows of 6 characters.

1	2	3	4	5	6
M	E	E	T	A	T
T	H	R	E	E	P
M	T	O	D	A	Y
A	T	T	H	E	U
S	U	A	L	L	O
C	A	T	I	O	N

The encoded message would be:
MTMASC EHTTUA EROTAT TEDHLI AEAELO TPYUON

The spaces would be removed or repositioned to hide the size of table used, since that is the encryption key in this message.

Final encryption:
MTMASCEHTTUAEROTATTEDHLIAEAELOTPYUON

Using the Rail Fence Technique: A great visual technique. I think this is easier for elementary students to understand and students with disabilities/English as New Language/ELL's students that I teach. You write the letters in a zig-zag pattern in rows across the page or rails.

Rail Fence Technique

Eg: Plaintext: MEET ME AFTER THE PARTY IS OVER

→ M E E T M E A F T E R T H E P A R T Y I S O V E R

→ E T E F T H E P A R T Y I S O V E R

Ciphertext:
MEMATRHI

Play (k)

1:50 / 17:30

Cryptography | Transposition Cipher | Rail Fence Technique

Algorithmic Steps to Encode in Scratch

1. Choose your letters for your message
2. Choose how many rails/rows you will use for your message.
3. Use 3 rows for your message
4. Your letters are "HELLO WORLD"
5. Write the message "HELLO WORLD" in a zig-zag pattern across the rails/page/row, starting at the top left rail and moving down diagonally to the bottom right rail, then back up diagonally to the top right rail, and so on.
6. After the message is written out in a zig-zag pattern, read it off row by row starting from the top row/rail.
7. Then combine the rows to read out the encoded message

TRANSPOSITION CIPHER USING RAIL FENCE TECHNIQUE VISUAL:

Number of rails/rows: 3 rows in a zig-zag pattern

```
H . . . O . . . L . . . .  
. E . L . W . . R . D . .  
.. L . . . O . . . . . . .
```

Zig-zag pattern:

```
H . . . O . . . R . .  
.. L . . . O . . . .  
E . . W . L . D . . .
```

Encoded message: HORLOEWLD