

Name: _____ Student No.: _____ Date: ____/____/____

Classical
Cryptography

CAESAR CIPHER (10 pts)

The Caesar cipher works by **substituting each letter of a message with a new letter after shifting the alphabet over.**

To encrypt:
(p + k) mod 26

To decrypt:
(c - k) mod 26

Step 1: Find Your Key (1 pt)

1. Write down the **last two** digits of your student number.
- _____
2. Use this number as your key for encryption.

Step 2: Encrypt the Messages

Encrypt the plaintext messages **INFORMATION** and **TECHNOLOGY**.

1. Convert the plaintext to numbers. Use the table below. (2 pts)

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

Plaintext	I	N	F	O	R	M	A	T	I	O	N
Number (p)											

Plaintext	T	E	C	H	N	O	L	O	G	Y
Number (p)										

2. Add your key to each number. (2 pts)

Plaintext	I	N	F	O	R	M	A	T	I	O	N
p + k											

Plaintext	T	E	C	H	N	O	L	O	G	Y
p + k										

3. Apply Modulo 26 (3 pts)

Plaintext	I	N	F	O	R	M	A	T	I	O	N
(p + k) mod 26											

Plaintext	T	E	C	H	N	O	L	O	G	Y
(p + k) mod 26										

Step 3: Convert the Ciphertext to Symbols (2 pts)

- **INFORMATION** → _____
- **TECHNOLOGY** → _____

VIGENÈRE CIPHER (13 pts)

The Vigenère cipher **uses multiple keys**, applying a different Caesar cipher to each letter of the plaintext, unlike the Caesar cipher, which uses one key for the whole text.

Imagine you are in a war, stationed in different locations. Your commander-in-chief sends an encrypted message to everyone, but each message is encrypted with a unique key. Your mission is to decrypt your message and uncover its meaning.

Step 1: Find Your Key (1 pt)

1. Check your Google Classroom for the key: _____

Step 2: Decrypt the Message

1. Convert the ciphertext to numbers. (2 pts)

Ciphertext									
Number (c)									

Ciphertext						
Number (c)						

2. Write your key under the ciphertext and also convert it to numbers. (2 pts)

Number (c)									
Key									
Number (k)									

Number (c)						
Key						
Number (k)						

3. Subtract the key from the ciphertext. (2 pts)

c - k									
-------	--	--	--	--	--	--	--	--	--

c - k						
-------	--	--	--	--	--	--

4. Apply modulo 26. (4 pts)

(c - k) mod 26									
----------------	--	--	--	--	--	--	--	--	--

(c - k) mod 26						
----------------	--	--	--	--	--	--

Step 3: Convert ciphertext to symbols. (2 pts)

PLAYFAIR CIPHER (10 pts)

The Playfair cipher uses a 5x5 letter matrix created from a keyword. It treats digraphs in the plaintext as single units and converts them into ciphertext digraphs.

Your military has upgraded to the Playfair Cipher. Follow the steps below to decrypt the message.

Step 1: Find Your Key

1. Use the same key as the Vigenère cipher.

Step 2: Create Your Playfair Square (3 pts)

1. Fill in the square, following the Playfair rules.

Step 3: Break Down the Ciphertext (2 pts)

1. Write the digraphs in each box below.

_____	_____	_____	_____	_____	_____
-------	-------	-------	-------	-------	-------

Step 4: Decrypt the Digraphs (3 pts)

- 1. Decrypt each digraph using your square and determine its position:
 - A: Same column
 - B: Same row
 - C: Neither in the same row nor column

Plaintext	_____	_____	_____	_____	_____	_____
Position						

Step 5: Remove Unnecessary Letters and Format the Message Properly (2 pts)

RAIL FENCE CIPHER (7 pts)

In Rail Fence cipher, the plaintext is **written down as a sequence of diagonals** and then **read off as a sequence of rows**.

Step 1: Find Your Key (1 pt)

- Check the **last** digit of your student number.
 - If 0, 1, 2 → **Use key 3**
 - If 3, 4, 5 → **Use key 4**
 - If 6, 7, 8, 9 → **Use key 5**
- What is your key? _____

Step 2: Decrypt the Message (4 pts)

- Check your Google Classroom for the ciphertext.
- Draw a rail fence based on your key and write the ciphertext in zigzag lines.

Step 3: Read the Rows (2 pts)

- Read off each row to get the message.
- What is the message?

References:
 Crypto Corner
 Cracking Codes with Python, Sweigart
 Cryptography and Network Security, Stallings