LAB 1: EXPLORING THE CAESAR CIPHER

Overview

The Caesar cipher is a simple yet powerful encryption technique classified as a substitution cipher. In this method, each letter in the plaintext is replaced by another letter a fixed number of positions down the alphabet. This lab will explore the workings of the Caesar cipher, its applications, and various exercises to solidify your understanding.

Understanding the Caesar Cipher

The Caesar cipher operates by shifting the letters of the alphabet. For example, with a shift of 2

Exercises

Exercise 1: Basic Decryption

A plaintext was encrypted with a Caesar cipher using a shift of 4. The resulting ciphertext is:

Task: Determine the original plaintext.

Ciphertext: “LIPPS”

Key: Shift of 4

Plaintext: HELLO

Exercise 2: Brute Force Attack

Attempt to crack the following Caesar ciphertext using brute force:

Task: Try every possible shift (1-25) and identify the original plaintext.

Plaintext: “ZEBRAS”

Alphabets: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Ciphertext:

Shift	Decrypted Text
1	YDAQZR
2	XCZPYQ
3	WBYOXP
4	VAXNWO
5	UZWMVN
6	TYVLUM
7	SXUKTL
8	RWTJSK
9	QVSIRJ
10	PURHQI
11	OTQGPH
12	NSPFOG
13	MROENF
14	LQNDME
15	KPMCLD
16	JOBBKC
17	INAAJB
18	HMZZIA
19	GLYYHZ
20	FKXXGY
21	EJWWFX
22	DIVVEW
23	CHUUDV
24	BGTTCU
25	AFSSBT

Exercise 3: Pattern Recognition

You have the following encrypted message:

Ciphertext: “CGRRC YQ YZGE”

Task: Can you determine the plaintext?

Hint: Look for patterns, especially the repeated letters.

Step 1: Analyze Letter Patterns

- Word 1: CGRRC
    - 5 letters
    - The 3rd and 4th letters are the same (`R`, `R`)
    - The 1st and 5th letters are also the same (`C`, `C`)
    - This follows the letter structure: A B C C A

Looking for a common English word with this same structure, one good candidate is:

SHEEP

Mapping that:

- C → S
- G → H
- R → E

This matches the pattern CGRRC → SHEEP

Step 2: Decode the second word: YQ

Using a logical guess:

The sentence SHEEP makes sense in English, so we test:

YQ → IS

Then:

- Y → I
- Q → S

Step 3: Decode the third word: YZGE

We now apply our known and guessed mappings:

If we assume YZGE = LOST, then:

- Y → L
- Z → O
- G → S
- E → T

Update our substitution key:

Cipher	Plain
C	S
G	S or H (needs resolution)
R	E
Y	L or I (conflict – choose L)
Q	S
Z	O
E	T

With this mapping:

- CGRRC → SHEEP
- YQ → IS
- YZGE → LOST

Everything aligns with a reasonable and grammatically correct English sentence.

Final Decryption: SHEEP IS LOST

Conclusion:

By identifying repeating letters and matching common English word patterns, I determined that the ciphertext uses a monoalphabetic substitution cipher. The letter patterns in the first word guided the correct guess of "SHEEP", which led to a full decryption.

Exercise 4: Frequency Analysis

The following ciphertext has been created without spaces:

Task: Conduct a frequency analysis of the letters. Based on your findings, attempt to decrypt the message by hypothesizing the most common letters.

Ciphertext: "hxgfhgshvczhx"

Step 1: Frequency Count of Each Letter

Letter	Frequency
h	4
x	2
g	2
f	1
s	1
v	1
c	1
z	1

Step 2: English Letter Frequency Reference

In typical English text, the most common letters are:

E, T, A, O, I, N, S, H, R, D, L, U

So if h is the most frequent in our ciphertext, it might correspond to E or T.

Let's guess:

h = E

x = T

g = A

Step 3: Substitution Attempt

Let’s substitute based on assumptions:

h = E

x = T\

g = A

f = ?

s = ?

v = ?

c = ?

z = ?

Ciphertext: h x g f h g s h v c z h x

Apply known substitutions:

Partial Decryption

E T A ? E A ? E ? ? ? E T

E T A _ E A _ E _ _ _ E T

Grouped:

ETA

EA

E

???

ET

It resembles "EAT", "EASE", or "EATER", but it's still incomplete.

Step 4: Try Caesar Cipher (Shift of 3)

Let's try Caesar shift of -3 (each letter shifted 3 letters back in the alphabet):

Original: h x g f h g s h v c z h x

Decrypted with Caesar -3:

e u d c e d p e s z w e u

Try splitting:

- eud ce dpes zweu
- educed pess weu

Still a bit unclear possibly a jumbled or artificial phrase.

Final Thoughts

Fequency Analysis shows h is likely E.

Caesar Shift of 3 gives:

eudcedpeszweu

But without more context or known plaintext, the message is ambiguous.

Summary

Ciphertext: "hxgfhgshvczhx"

Plaintext: eudcedpeszweu

Exercise 5: Creative Sentence

Task: Create a meaningful sentence of your own, encrypt it using a Caesar cipher with a shift of 5, and present the ciphertext to your peers. Challenge them to decode it!

Key: Encrypt using a shift of five

Plaintext: My name is Cyberpen and I am a woman in tech

Ciphertext: Rd sfrj nx Hdzjwujs fsi N fr f btrfs ns yjhm

Exercise 6: Historical Context

Research the historical use of the Caesar cipher in military communication. Write a brief paragraph on its significance during Julius Caesar's time and how it relates to modern encryption

techniques.

Historical Use of the Caesar Cipher

The Caesar cipher, named after the Roman general Julius Caesar, is one of the earliest and most famous encryption techniques in history. Caesar used this simple substitution cipher during military campaigns to send confidential messages to his generals. By shifting each letter in the plaintext by a fixed number commonly three he ensured that only those who knew the shift (or key) could decode the message. This early form of encryption provided a basic level of security in an era where secrecy in military communication was crucial.

Origin:

- Developed by Julius Caesar, a Roman general and dictator.
- Used during military campaigns to protect sensitive messages.

Method:

A substitution cipher where each letter in the plaintext is shifted a fixed number of places in the alphabet.

Example: A shift of 3 turns "A" into "D", "B" into "E", and so on.

Purpose in Caesar's Time:

Ensured that intercepted messages could not be easily understood by enemies.

Offered a simple but effective way to maintain secrecy in military communication.

Significance:

- One of the first recorded uses of encryption in history.
- Introduced key concepts still used in modern cryptography like:
    - Confidentiality
    - Key-based decoding
    - Message transformation

Limitations:

- Very simple by modern standards.
- Easily broken using frequency analysis or brute-force attacks (only 25 possible shifts).

Connection to Modern Encryption

Modern Cryptography:

- Uses complex mathematical algorithms and large key sizes (e.g., AES, RSA).
- Provides strong security for digital communication, banking, data storage, and more.

Shared Principles:

Both the Caesar cipher and modern encryption rely on:

- Hiding information from unauthorized users
- Key-based access to decrypt the message
- Ensuring message confidentiality and integrity

Exercise 7: Modern Application

Choose a contemporary use case for substitution ciphers (such as in gaming or secure communications). Write a short essay discussing its relevance today and compare it to the Caesar cipher.

🔐 Substitution Ciphers in Modern Secure Communications

In today's digital world, secure communication is critical for protecting sensitive information transmitted over the internet. While simple substitution ciphers like the Caesar cipher are no longer secure enough for real-world use, their basic concept replacing characters in a message to make it unreadable without a key still underpins modern encryption techniques.

Relevance in Today's Digital World

Secure communication is vital for protecting data during transmission (e.g., emails, chats, banking). Though basic substitution ciphers like the Caesar cipher are outdated, modern encryption algorithms still rely on substitution principles. These methods are used in end-to-end encryption to keep messages private on platforms like:

- WhatsApp

- Signal
- Telegram

How Modern Substitution Works

Modern algorithms like AES (Advanced Encryption Standard) use:

- Substitution Boxes (S-boxes) for nonlinear transformations.
- Multiple rounds of substitution and permutation for added security.
- 128-bit or 256-bit keys to prevent brute-force attacks.

These encryption methods make it impractical to decode without the correct key.

Comparison with the Caesar Cipher

Feature	Caesar Cipher	Modern Substitution (e.g., AES)
Complexity	Very simple, fixed shift	Multi-layered, complex substitution
Security	Easily breakable	Extremely secure (used in governments, banks)
Use Case	Historical military communication	Digital messaging, VPNs, financial systems
Key Space	Only 25 possible keys	Trillions of combinations (128-bit+)

Conclusion

While the Caesar cipher is no longer used for secure messaging, it introduced the core idea of substitution a foundation upon which modern cryptography is built. Today's secure communication systems use highly advanced versions of substitution to protect privacy and maintain trust in the digital age.