Multi-Layer Encryption and Decryption System for Information Security

PRESENTATED BY :

AYESHA NOOR [FA23-BSE-087]

AMENA SAJID [FA23-BSE-078]

AREEBA ASIM [FA23-BSE-090]

FALAK SHABIR [FA23-BSE-066]

Introduction

Overview of Classical Cryptography

Multi-layered encryption increases security

This project includes:

1. **Caesar Cipher**
2. **Block Reversal**
3. **ADFGVX Cipher (Substitution + Transposition)**

Caesar Cipher (1st Layer)

Purpose: Simple letter shifting

Input: Plaintext + shift value

Output: Shifted text (preserving case)

C++ Logic:

```
char base = isupper(c) ? 'A' : 'a'; c = char((c - base + shift + 26) % 26 + base);
```

Block Reversal (2nd Layer)

Purpose: Scrambles text in fixed-size blocks

Preserves: Original spacing

Input: Caesar output + block size

Output: Reversed text by block

Visual Example:

Input: HELLO WORLD

Block Size: 3 → Output:LEHWO LLROD

ADFGVX Cipher /PRODUCT CIPHER

Two Steps:

Substitution using a Polybius Square

Columnar Transposition using keyword

User Inputs:

- 6-letter Substitution Key
- Transposition Keyword

Substitution Step

Polybius Square: 6x6 grid of A-Z and 0-9

Labeled with User's 6-character Key

Each character → pair of labels (row + col)

Example Table (Key: ABCDEF):

A	B	C	D	E	F
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	0	1	2	3	4
5	6	7	8	9	.

Transposition Step

Create Grid: Row-wise fill of substituted text

Columns Labeled by Keyword Characters

Sort Columns by Alphabetical Order of Keyword

Read Column-wise to get Final Ciphertext

Create Grid

Sort Columns

Read Column-wise

Transposition Table Example

Keyword: author

Key: a u t h o r

After sorting (alphabetical): a h o r t u

Read column-wise to get ciphertext

Original Keyword Order

a	u	t	h	o	r
b	a	a	a	a	c
a	c	a	c	b	d
d	c	c	e	c	e
c	d	d	b	X	X

Sorted Keyword Order

a	h	o	r	t	u
b	a	a	c	a	a
a	c	b	d	a	c
d	e	c	e	c	c
c	b	X	X	d	d

Input Validation & Flow

Ensures:

Substitution key is exactly 6 characters

Keyword length is at least 2

Re-prompts user on invalid input

Prints:

- Caesar output
- Block reversal output
- Substitution table & result
- Transposition table & final ciphertext

Example

Enter plaintext: ayesha noor
Caesar Shift: 2 → Caesar Text: cayguc pqqt
Block Size: 3 → Block Text: yacugc tqpp
Substitution Key: abcdef → Substitution Table shown → Substituted Text: baaaacacbddccecedddb
Transposition Key: author → Table Shown → Final Ciphertext: bacdccdXadeXadcXabcXaceb

Enter plaintext: ayesha noor
Caesar Shift: 2 → Caesar Text: cagujc pqqt
Block Size: 3 → Block Text: gaccju qqpt
Substitution Key: abcdef → Substitution Table shown → Substituted Text: baaaacacbddccecedddb
Transposition Key: author → Table Shown → Final Ciphertext: bacdadeXadcXccdXabcXaceb

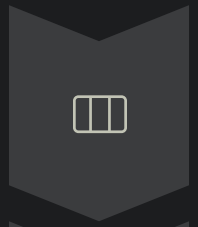
Output

```
Enter plaintext (A-Z, 0-9): ayesha noor

Enter Caesar shift: 2

Caesar Cipher Text: cagujc pqqt

Enter block size for reversal: 3

Block Reversal Text: gaccju qqpt

Enter 6-letter substitution key (e.g. ADFGVX): abcdef

Substitution Table:
    a b c d e f
  +--------------------
a | a b c d e f
b | g h i j k l
c | m n o p q r
d | s t u v w x
e | y z 0 1 2 3
f | 4 5 6 7 8 9

Substituted Text: baaaacacbddccececddb

Enter transposition key: author

 Transposition Table
  a  u  t  h  o  r
------------------
  b  a  a  a  a  c
  a  c  b  d  d  c
  c  e  c  e  c  d
  d  b  X  X  X  X

Final Encrypted Ciphertext: bacdadeXadcXccdXabcXaceb
```

Code Highlights

- **Modular Design:** Each encryption layer uses separate, dedicated functions. This improves readability and simplifies maintenance.
- **Robust I/O:** The system incorporates clean input and output. Strict validation prevents common errors and enhances reliability.
- **Standard Libraries:** Utilizes C++ libraries such as **<string>**, **<vector>**, and **<map>**. These provide efficient data structures and algorithms.

Decryption Process



Reverse Transposition

Reconstruct the original table using the keyword.

Reverse Substitution

Use the substitution key to map characters back.

Reverse Block Reversal

Reorder text blocks to their original sequence.

Reverse Caesar Shift

Shift characters backward to reveal plaintext.

Decryption example:

Output

```
Do you want to (encrypt/decrypt)? decrypt
Enter ciphertext: bacdadeXadcXccdXabcXaceb
Enter Caesar shift: 2
Enter block size for reversal: 3
Enter 6-letter substitution key (e.g. ADFGVX): abcdef

Substitution Table:
    a b c d e f
  +------------------
a | a b c d e f
b | g h i j k l
c | m n o p q r
d | s t u v w x
e | y z 0 1 2 3
f | 4 5 6 7 8 9
Enter transposition key: author

Transposition Table (Decryption):
  a  u  t  h  o  r
-----------------
  b  a  a  a  a  c
  a  c  b  d  d  c
  c  e  c  e  c  d
  d  b  X  X  X  X

Decrypted Transposition: baaaacacbddcceceddbXXXX
Decrypted Substitution: gaccjuqqpt
Decrypted Block Reverse: cagujcpqqt
Final Decrypted Text: ayeshanoor
```

Q&A Session

We welcome your questions on the multi-layer encryption system.

Thank you for your valuable time and engagement today.