Joel Sivanish

Professor Kaur

Lab 1 – Traditional Ciphers

1/15/2026

Introduction:

The purpose of this lab was to implement and analyze several classical cryptographic ciphers to understand their underlying mechanisms and limitations. Classical ciphers are historically significant but are no longer considered secure by modern standards. Implementing these ciphers provides insight into why modern cryptography relies on more complex mathematical constructions.

In this lab, six traditional ciphers were implemented in the C programming language: Caesar, Atbash, Vigenère, Affine, Playfair, and Hill. Each cipher supports encryption and decryption and includes automated test cases to verify correctness.

Cipher Descriptions:

Caesar Cipher:

- The Caesar cipher is a simple substitution cipher that shifts each letter of the plaintext by a fixed number of positions in the alphabet. Decryption reverses the shift. While easy to implement, it is vulnerable to brute-force attacks due to its small key space.

Atbash Cipher:

- The Atbash cipher replaces each letter with its mirror in the alphabet (A ↔ Z, B ↔ Y). Encryption and decryption use the same transformation. Because it has no key, it provides no real security.

Vigenère Cipher:

- The Vigenère cipher is a polyalphabetic substitution cipher that uses a keyword to vary the shift applied to each letter. While more secure than Caesar, it is still vulnerable to frequency analysis and known-plaintext attacks.

Affine Cipher:

- The Affine cipher applies a mathematical transformation to each letter using the formula
  $E(x) = (ax + b) mod 26$.
  Decryption requires computing the modular inverse of a. The cipher is stronger than simple substitution but still easily broken with modern techniques.

Playfair Cipher:

- The Playfair cipher encrypts pairs of letters using a 5×5 key matrix. It combines the letters I and J and uses digraph substitution rules based on rows, columns, and rectangles in the matrix. This implementation follows the classic 5×5 definition and omits non-letter characters.

Hill Cipher:

- The Hill cipher uses linear algebra to encrypt blocks of letters using matrix multiplication modulo 26. A 2×2 key matrix was implemented for this lab. Decryption requires computing the modular inverse of the matrix. Like Playfair, this implementation operates on letters only.

Implementation Details:

Each cipher includes a dedicated test file containing multiple test cases. These tests cover simple examples, mixed case and punctuation, and inputs containing digits and spaces when applicable.

Known reference examples from the lab materials were used to validate correctness. For example, the Hill cipher correctly encrypts the plaintext “HELP” using the key matrix $\begin{bmatrix} 1 & 8 \\ 8 & 5 \end{bmatrix}$ to produce the ciphertext “NYBH”, which decrypts back to the original plaintext.

Playfair and Hill cipher tests demonstrate that non-letter characters are omitted, consistent with their classical definitions.

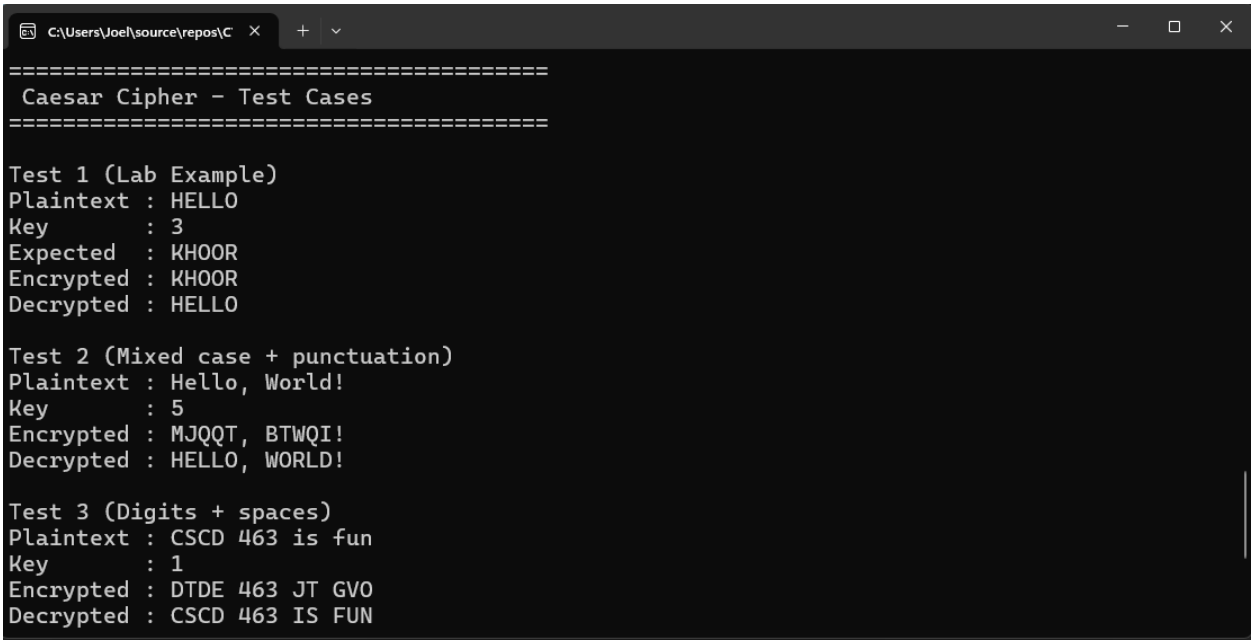
Discussion:

This lab highlights the weaknesses of classical ciphers. Most are vulnerable to brute-force attacks, frequency analysis, or known-plaintext attacks. Even ciphers such as Vigenère and Hill, which introduce additional complexity, are insecure by modern standards.

However, implementing these ciphers provides valuable insight into foundational cryptographic concepts such as substitution, modular arithmetic, key management, and matrix inversion.

Testing and Results:

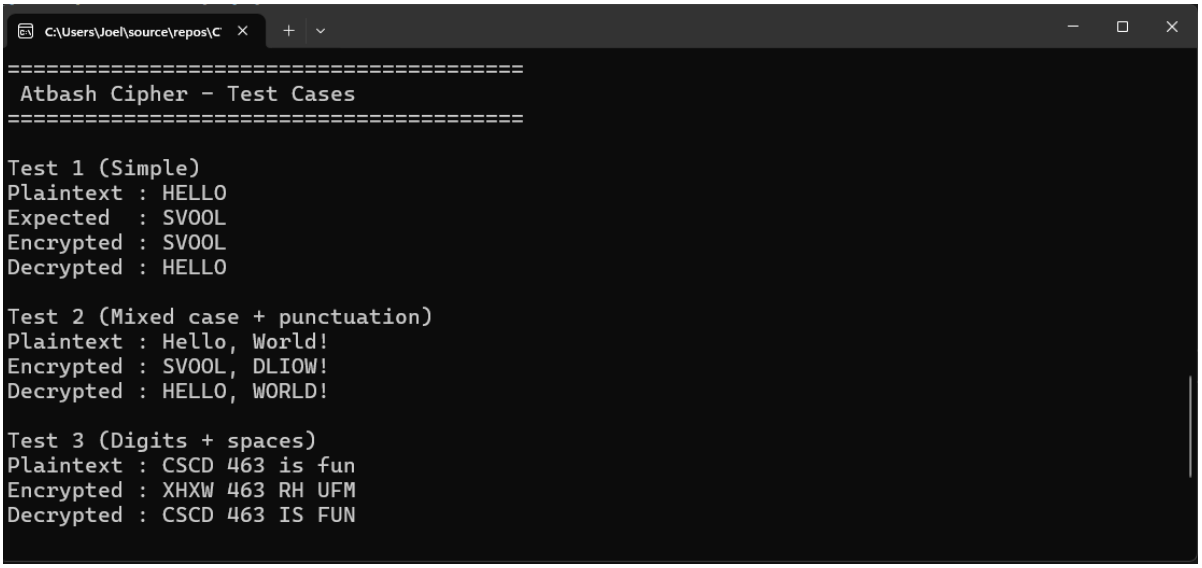
1. Caesar Cipher:



Edge Cases Handled:

- Large shift values: Keys greater than 25 correctly wrap modulo 26.
- Negative shifts: Decryption and negative shifts produce correct results.
- Non-letter characters: Digits, spaces, and punctuation are preserved.

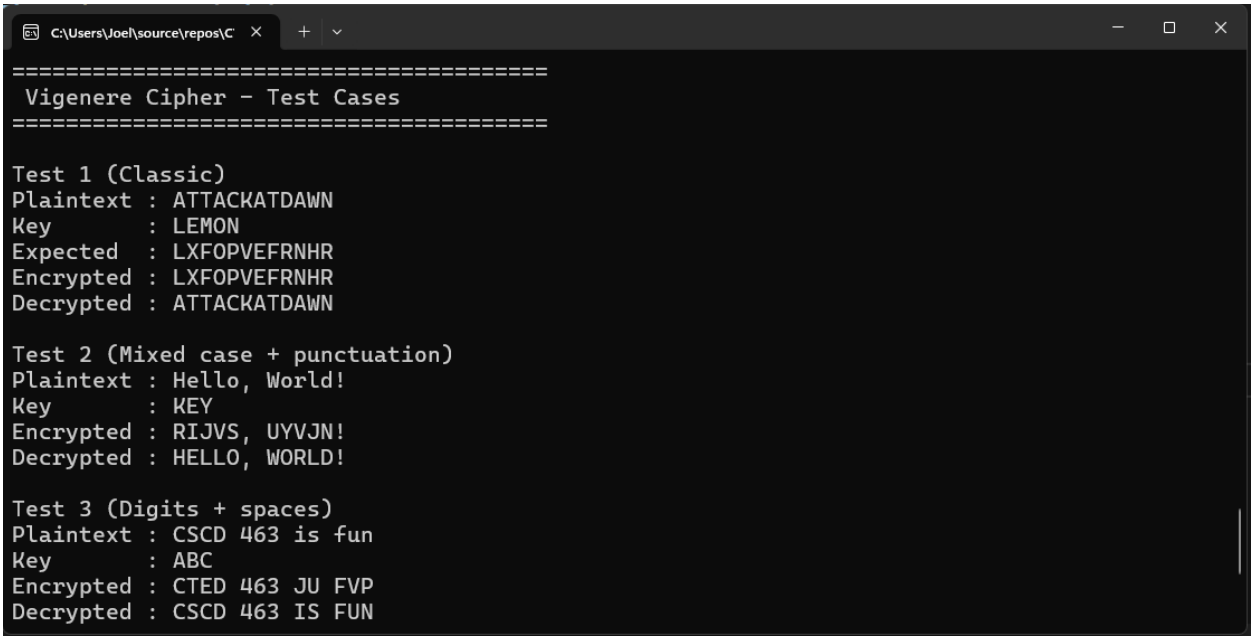
2. Atbash Cipher:



Edge Cases:

- Non-letter characters: Digits and punctuation are left unchanged.
- Mixed case input: Lowercase input is handled consistently.

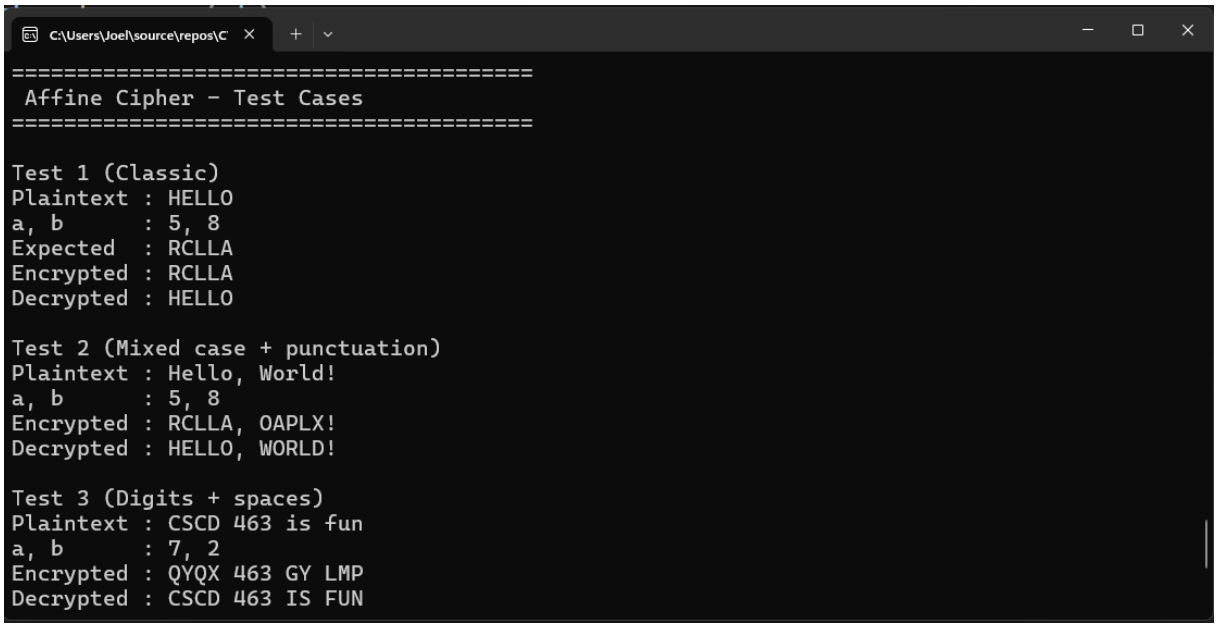
3. Vigenère Cipher:



Edge Cases:

- Short keys: Keyword repeats correctly across long plaintext.
- Mixed case input: Plaintext and key are normalized consistently.
- Non-letter characters: Preserved and do not consume key characters.

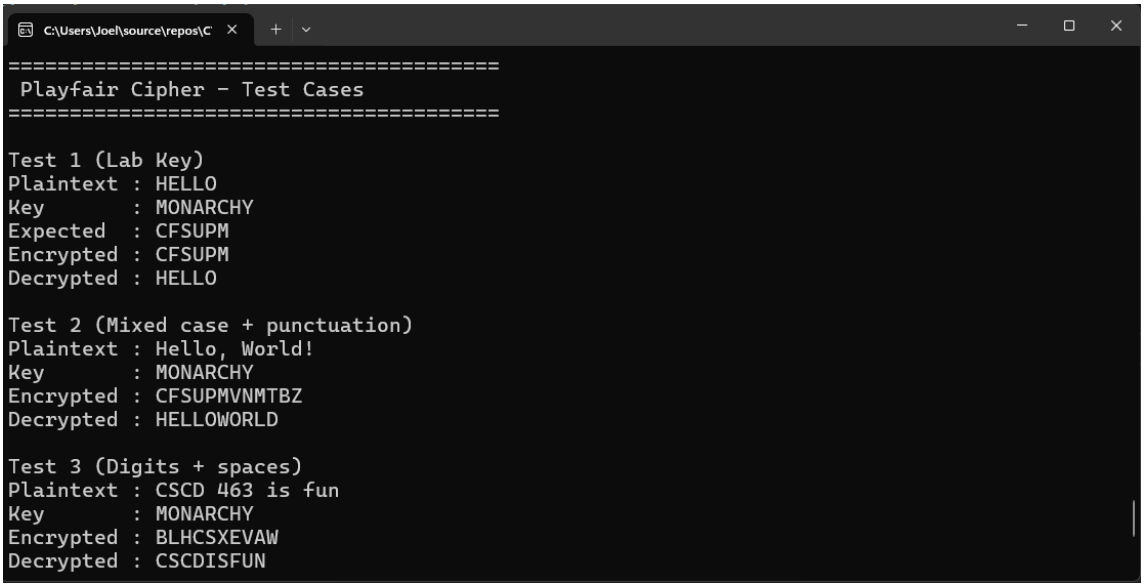
4) Affine Cipher:



Edge Cases:

- Invalid key values: Non-invertible values of a are safely handled.
- Large key values: Keys are reduced modulo 26.
- Non-letter characters: Preserved during encryption and decryption.

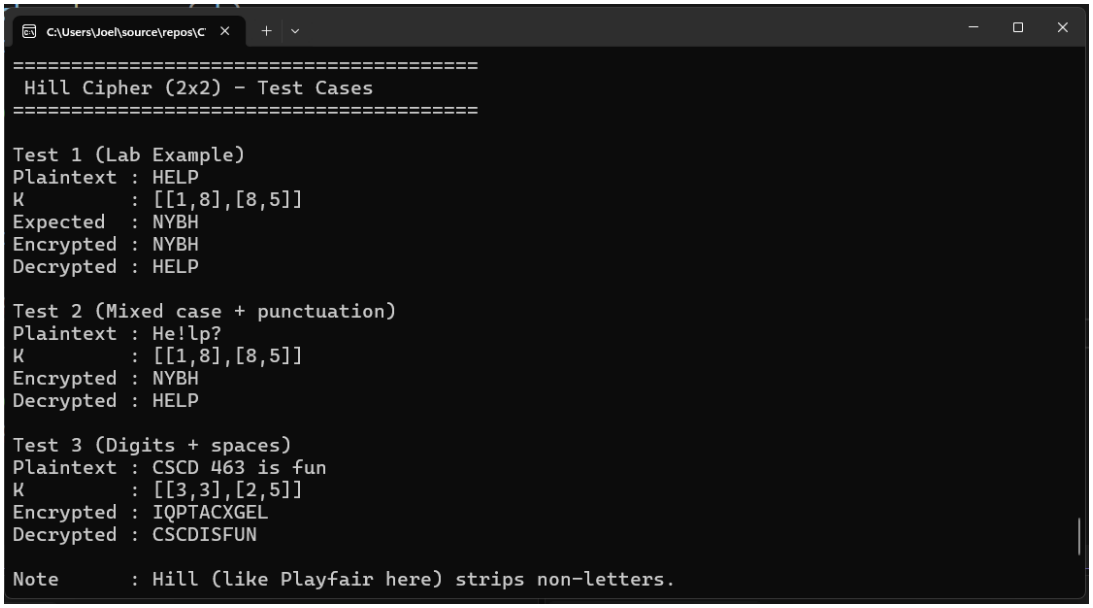
5) Playfair Cipher:



Edge Cases:

- Duplicate letters: Repeated letters in digraphs insert filler X.
- Odd-length input: Plaintext is padded with X when necessary.
- I/J handling: Letters I and J are combined per the standard 5×5 definition.
- Non-letter characters: Omitted during processing.

6) Hill Cipher



Edge Cases:

- Non-invertible matrices: Keys with non-invertible determinants are safely rejected.
- Odd-length input: Plaintext is padded to match block size.
- Non-letter characters: Omitted during encryption and decryption.

Conclusion:

In this lab, multiple classical ciphers were successfully implemented and tested. The exercise reinforced core cryptographic principles and demonstrated why modern cryptography requires more advanced algorithms. While these ciphers are no longer secure, they serve as an important educational foundation for understanding cryptography.