Green University of Bangladesh

Department of Computer Science and Engineering (CSE)

Faculty of Sciences and Engineering

Semester: (Summe, Year:2023), B.Sc. in CSE (Day)

Project Report

Course Title: Computer and Cyber Security

Course Code: CSE 323

Section: 202 D2

Experiment Name: Project proposal preparation and planning

Student Details

Name	Student ID
Jihad	202002082
S M Ibrahim Kayum	2011002235

Submission Date: 15-5-2023

Course Teacher's Name: Mr. Palash Roy

[For Teachers use only: Don't Write Anything inside this box]

Lab Report Status	
Marks:	**Signature:**
Comments:	**Date:**

Contents

0.1 Introduction

In this lab report, we will discuss four different security algorithms:

1. Playfair cipher
2. Vigenere cipher
3. Multiplicative cipher
4. Rail fence cipher

0.1.1 Playfair Cipher

Playfair cipher is a polygraphic substitution cipher that was invented by Charles Wheatstone in 1854. It uses a 5x5 grid of letters to encrypt plaintext into ciphertext.

0.1.2 Vigenere Cipher

Vigenere cipher is a polyalphabetic substitution cipher that was invented by Giovan Battista Bellaso in the 16th century. It uses a keyword to encrypt plaintext into ciphertext.

0.1.3 Multiplicative Cipher

Multiplicative cipher is a monoalphabetic substitution cipher that uses modular arithmetic to encrypt plaintext into ciphertext.

0.1.4 Rail Fence Cipher

Rail fence cipher is a transposition cipher that was used by the ancient Greeks and Spartans. It rearranges the plaintext by writing it diagonally over a number of "rails" or lines, then reading off the ciphertext from left to right.

0.2 Objectives

The objectives of this report are:

1. To understand the working of different cryptographic algorithms.
2. To implement these algorithms using programming.
3. To demonstrate the functionality of these algorithms with proper examples.

0.3 Solution methodology

Here's the solution methodology for each of the algorithms: Playfair, Vigenere, Multiplicative Cipher, and Rail Fence.

1. **Playfair Algorithm:**
   - Generate a Playfair grid using a given keyword.
   - Break the plaintext into pairs of letters.
   - For each letter pair:
     - If the letters are in the same row in the grid, replace each letter with the letter to its right .
     - If the letters are in the same column, replace each letter with the letter below it .
     - If the letters are in different rows and columns, form a rectangle with the letters and replace them with the letters on the opposite corners of the rectangle.
   - Repeat the above step for the entire plaintext.
   - The resulting letters form the ciphertext.
2. **Vigenere Algorithm:**
   - Repeat the keyword until it matches the length of the plaintext.
   - Convert both the keyword and the plaintext to numerical values (using a suitable mapping).
   - For each letter in the plaintext:
     - Add the numerical value of the corresponding keyword letter to the numerical value of the plaintext letter (modulo the alphabet size).
     - Convert the resulting numerical value back to a letter.
   - Repeat the above step for the entire plaintext.
   - The resulting letters form the ciphertext.
3. **Multiplicative Cipher Algorithm:**
   - Assign numerical values to each letter in the plaintext and the key (using a suitable mapping).
   - Multiply the numerical value of each plaintext letter by the numerical value of the corresponding key letter.
   - Convert the resulting numerical values back to letters.
   - Repeat the above step for the entire plaintext.
   - The resulting letters form the ciphertext.
4. **Rail Fence Algorithm:**
   - Write the plaintext diagonally in a zigzag pattern on a specified number of rails (rows).
   - Read off the characters row by row to obtain the ciphertext.
   - Repeat the above step for the entire plaintext.

0.4 Results

Provide Screenshot:

Live Web Site **Click here** to visit the website.

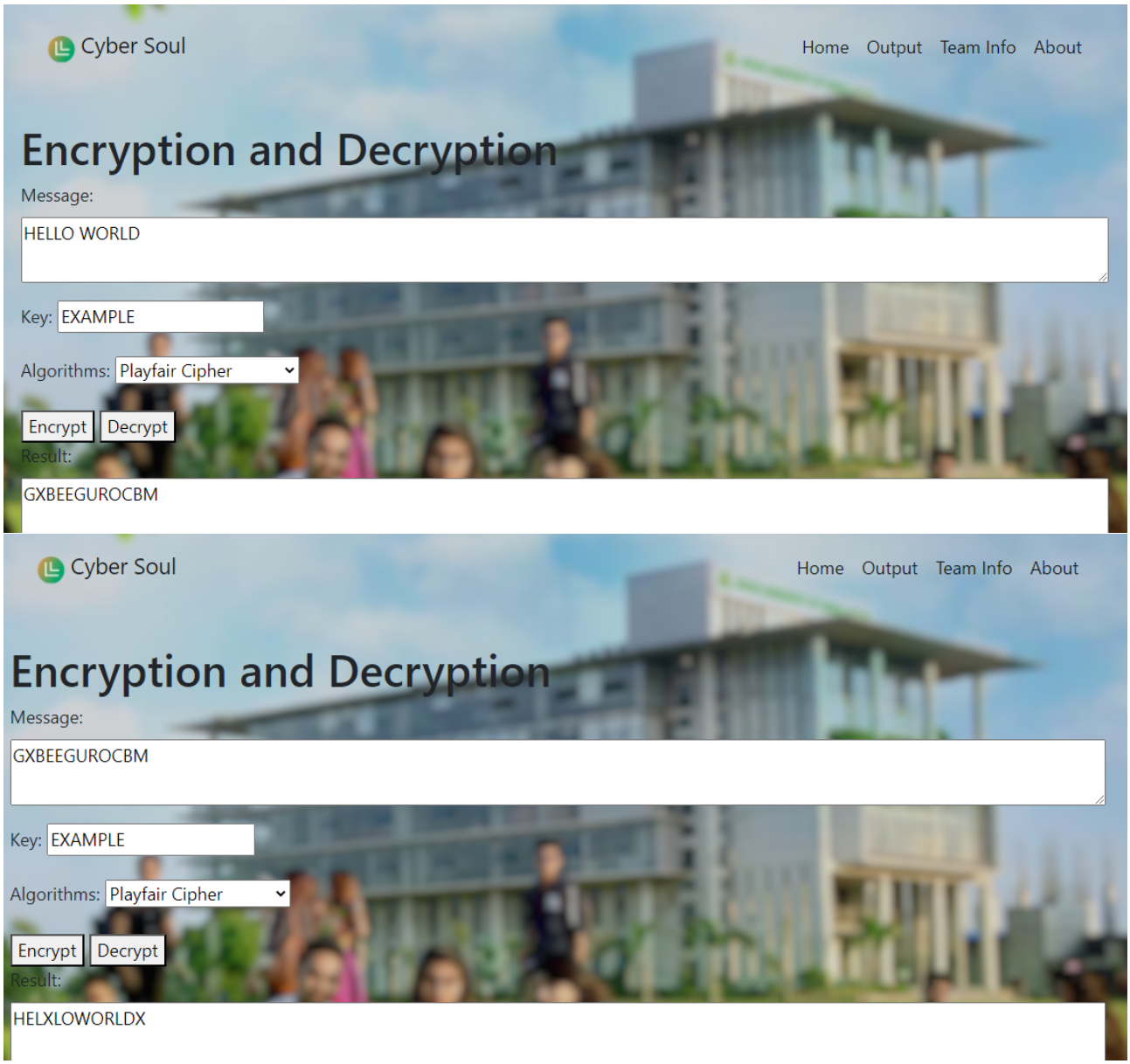

Figure 1: Playfair Cipher

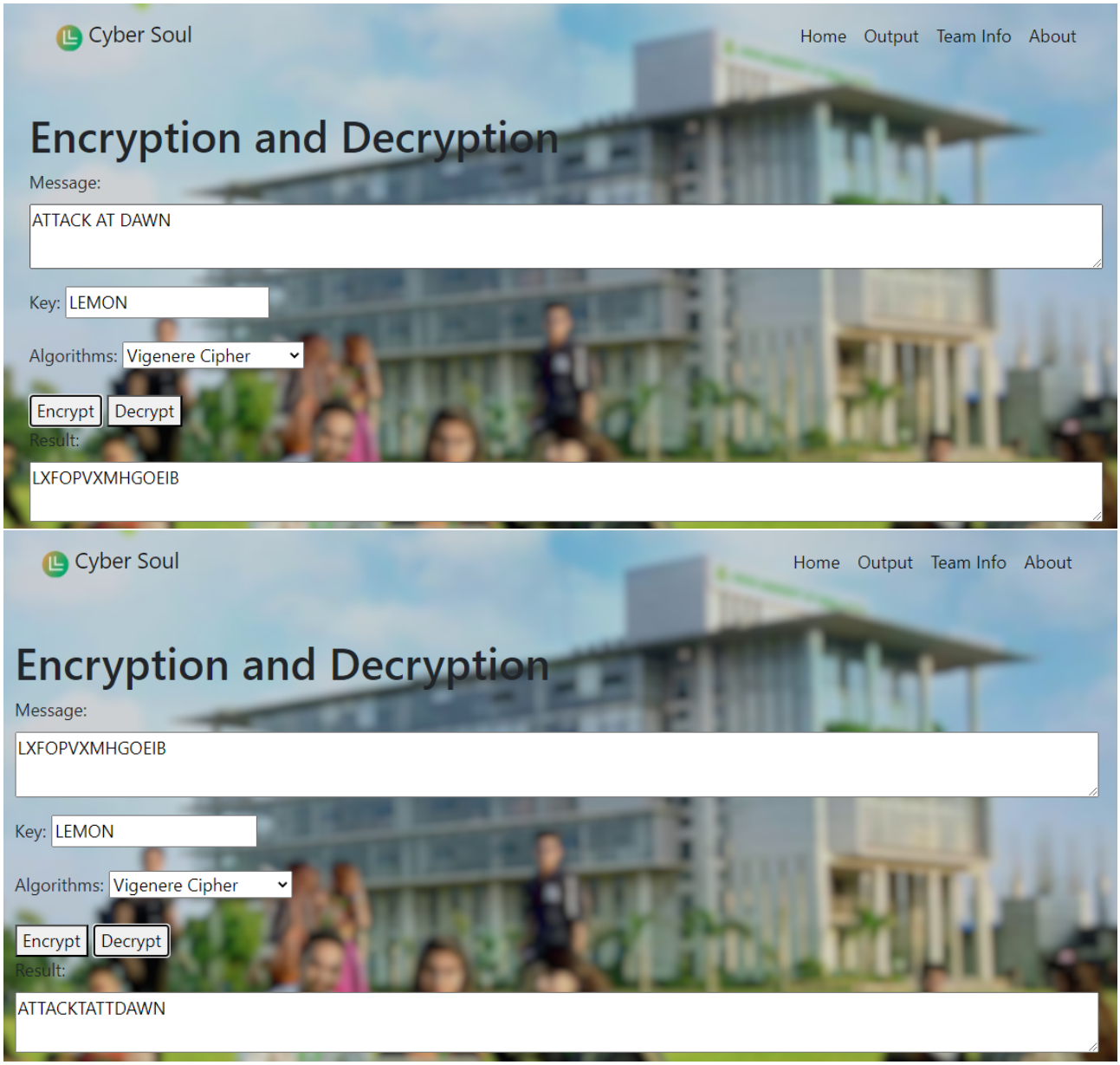

Figure 2: Vigenere Cipher

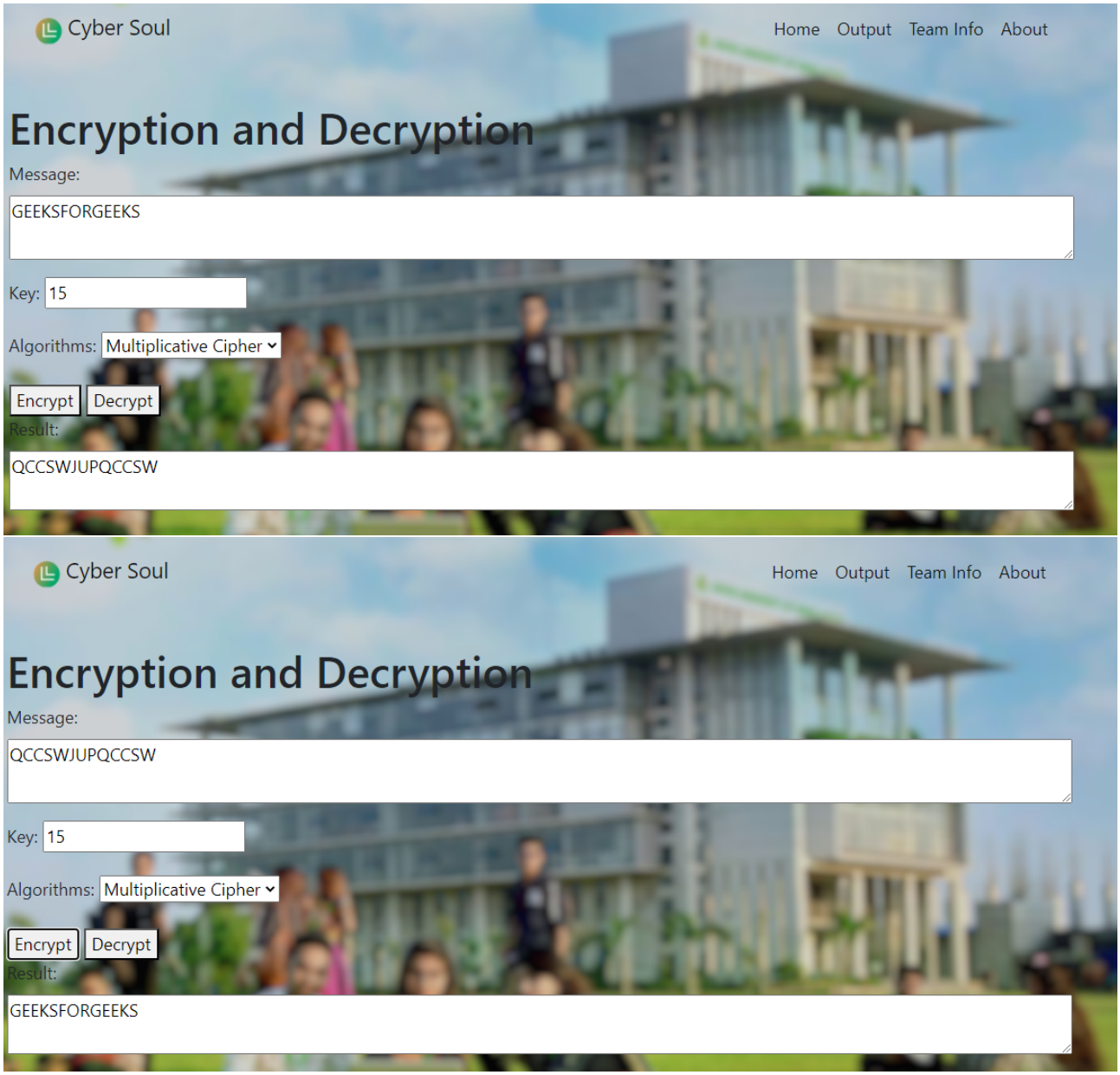

Figure 3: Multiplicative Cipher

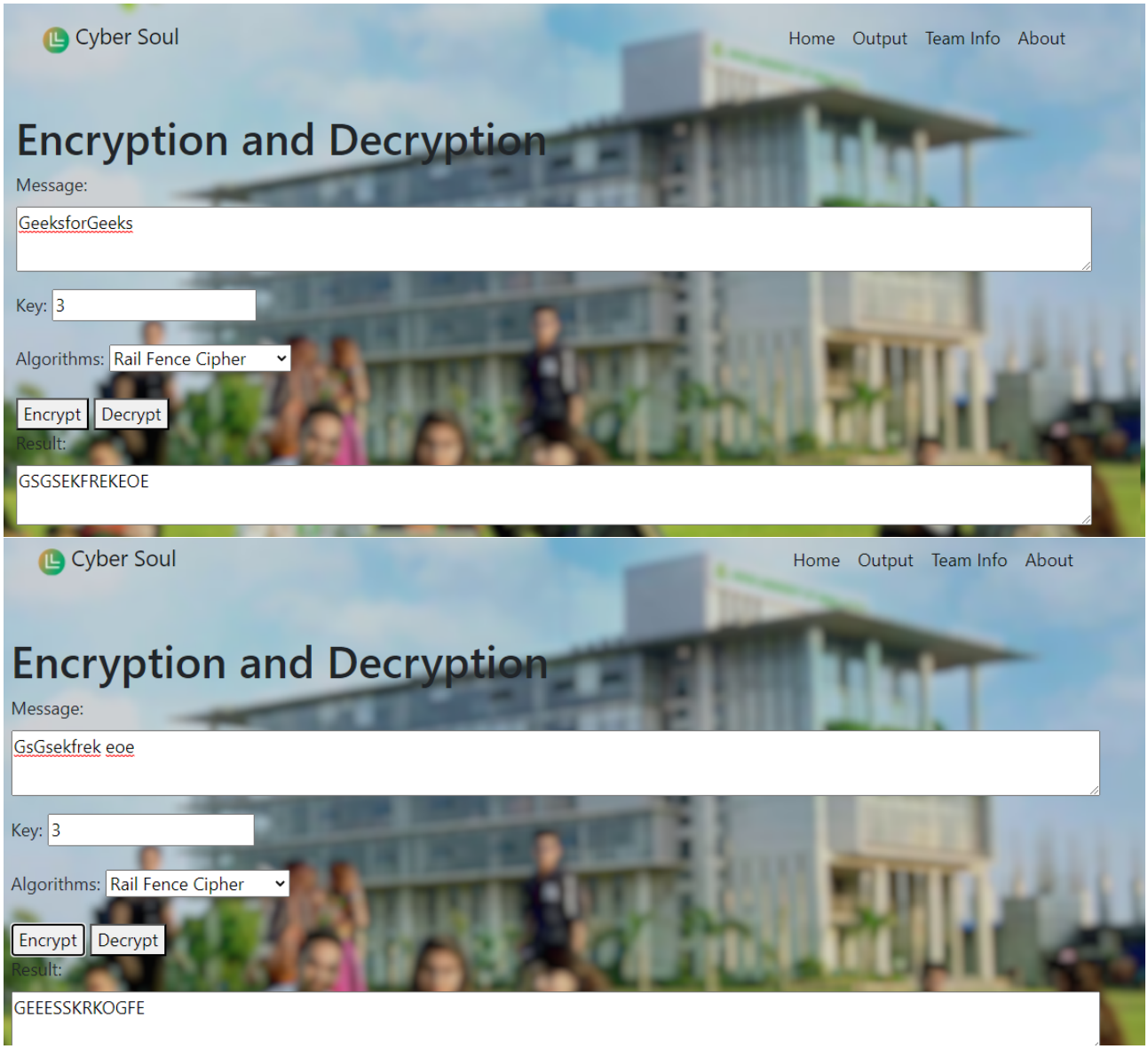

Figure 4: Rail Fence Cipher

0.5 Learning and Difficulties:

- I learned about various encryption and decryption algorithms and their solution methodology.
- Implementing the algorithm correctly can lead to problems, especially when dealing with various edge cases, input validation and special characters.

0.6 Conclusion:

Playfair, Vigenere, Multiplicative Cipher, and Rail Fence algorithms are cryptographic algorithms that can be used to secure communications and protect sensitive information. Each algorithm has its own methodology and strengths. Implementing these algorithms requires attention to detail and an understanding of their principles.