King Saud University
College of Computer and Information Sciences
Department of Software Engineering

SWE 314 – SOFTWARE SECURITY ENGINEERING 3(3–0–1)
Trimester III, 2022–2023

Assignment #1
(Done in groups of 3-4 students)

Encryption / Decryption Software Tool

Requirements:

You are asked to design and implement an encryption/decryption software tool. This tool should contain a list of encryption algorithms and decryption algorithms as described below. The objective is to offer the user different choices of encryption/decryption techniques. This tool can be used as a kind of educational tool for those who want to understand how encryption works.

The process to follow:

1. Produce the following UML diagrams as first step:
   - Produce a use case model describing how the user will use the tool (functional requirements).
   - Complement the use cases by specifying the different encryption/decryption algorithms in pseudo-code.
   - Produce a class diagram showing the main classes, including methods and attributes needed.
2. Implement the different use cases identified in 1 by considering the class diagram.
3. Test and debug your implementation to eliminate bugs.

4. Run different test cases to show that your implementation works fine.

The tool must be designed to allow interaction with the user to enter (or upload) his plaintext or any other required parameter depending on the algorithm used. The tool shall be interactive also to show the users the different steps of the encryption/decryption process.

Encryption algorithms to include in the tool:

- Encryption based on monoalphabetic substitution.
- Encryption using the Playfair Algorithm
- Encryption using the Vigenere Algorithm
- Encryption using the Keyed Transposition
- Encryption by combining monoalphabetic substitution and one of the three algorithms (Playfair, Vigenere, or Keyed Transposition)

+

- One basic modern block cipher algorithms (bit level) of your choice – could be for example, monoalphabetic substitution but by using bits not characters.
- DES or AES

Decryption techniques to include in the tool:

- Monoalphabetic substitution
- Playfair
- Vigenere
- Decryption using frequency analysis for messages that were encrypted using basic substitution techniques.

Deliverables:

A report organized as follows:

- Cover page
- Table of Contents
- Summary
- Introduction/Overview
- Use case model
- Pseudo-code of the different algorithms

- Class Diagram
- Samples of code with appropriate explanations
- Test cases
- A series of executions showing the input and the output of the program
- Limitations (what has been done/works and what has not be done/does not work)
- Conclusion

+

CD/Flash disk containing all the code + readme file

Deadline: Thursday, May 3rd, 2023.