

MTH 312 - Semester Project Proposal

Team Members: Wesley Guthrie, Tom Novakoski, Gloire Rubambiza, Colin Smith

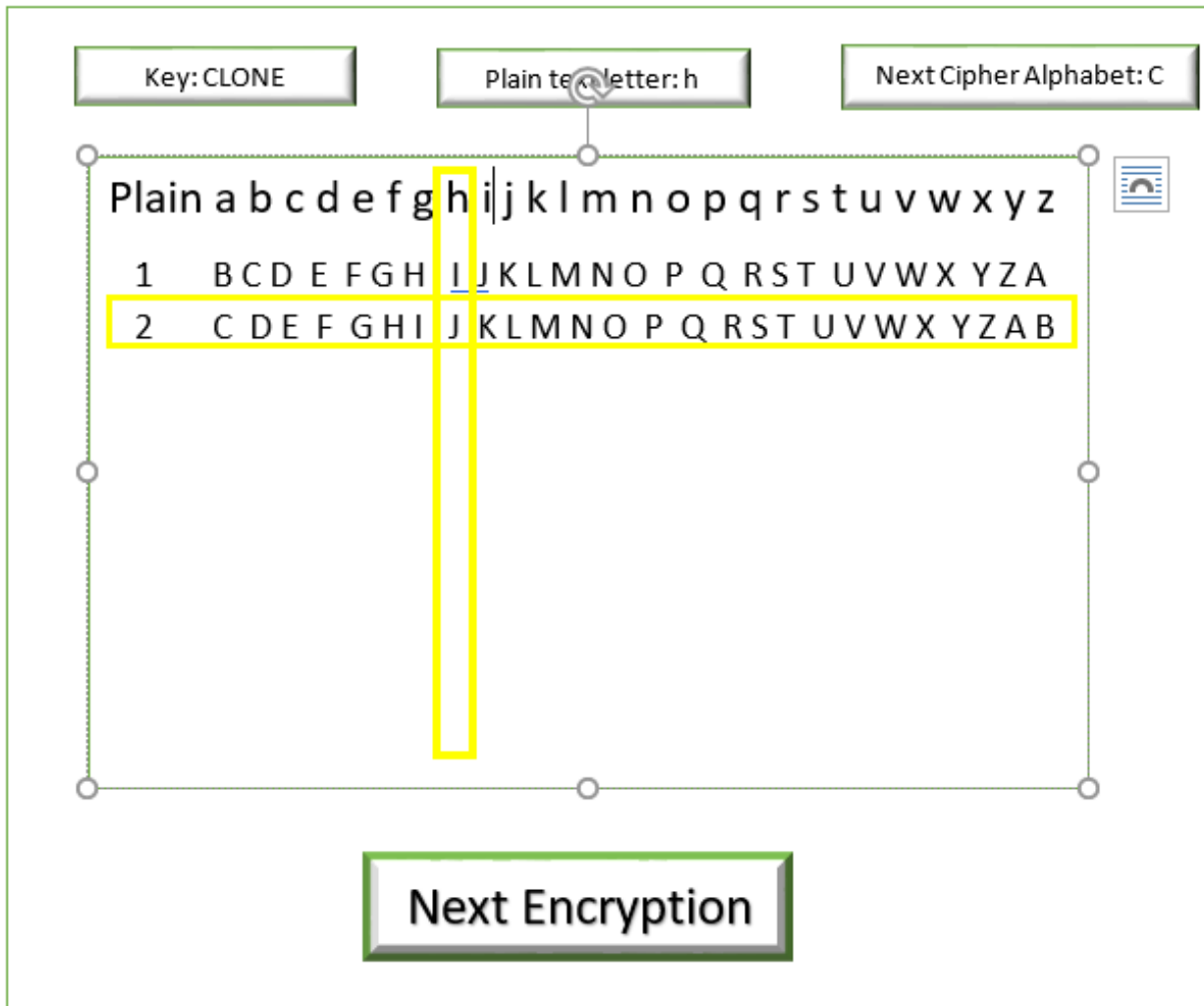
1. Introduction

The Vigenère cipher, developed by Blaise de Vigenère in the 1523, is a polyalphabetic cryptographic system that relies on a secret key shared by a sender and receiver. The secret key determines the cipher alphabets to be used when encrypting and decrypting messages. Despite its promise of security against people not schooled in cryptanalysis, the system was not widely adopted in its infancy in the 16th century mostly due to its complexity. In our project, we will reach out to the public and provide them with a basic understanding of the Vigenère cipher.

2. Public Service Project

Because the general public uses applications on their smartphones and desktops on a daily basis, we will explore that space to achieve our goal of introducing them to the Vigenère cipher. Specifically, we will build a Java program that a user can launch and easily step through to learn about the encryption and decryption process of the Vigenère cipher.

The program will feature a simple graphical user interface, as shown in fig. 1, that illustrates the steps involved in selecting a cipher alphabet using the key and enciphering a single letter.



3. Division of Labor

The preliminary division of labor is as follows:

- Model/Controller class(es): Wesley, Colin
- GUI: Gloire, Wesley
- Documentation: Gloire, Tom

4. Deliverables

- Java program runnable on any system featuring Linux and Java Runtime Environment
- Project design documentation
- Demo with a few classmates/prof
- Final report/reflection