**BÀI TẬP VÀ THỰC HÀNH HỌC PHẦN BẢO MẬT: (*BUỔI 3*)**

**Bài tập 1:** Cho biến đọan mã sau dùng mã Ceasar

"CSYEVIXIVQMREXIH"

Suy luận tìm bản rõ (sử dụng bảng chữ cái tiếng Anh).

**Bài tập 2:** Sử dụng kỹ thuật thám mã bảng chữ đơn, lập bảng tần suất các chữ, bộ chữ đôi, bộ chữ ba của đọan mã sau:

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIVUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSXEPYEPOPDZSZUFPOUDTMOHMQ

Lập luận và cho biết ánh xạ của bảng chữ đơn và đưa ra bản rõ phù hợp

**Bài tập 3:** Tìm bản mã của bản rõ “CHUNG TOI LA SINH VIEN CNTT HUBT” sử dụng mã Playfair với từ khóa “KINH DOANH CONG NGHE”.

**Bài tập 4:** Mã hóa bản rõ “CONG NGHE THONG TIN THE KY 21” sử dụng từ khóa 631425 bằng phương pháp Vigenere.

**Bài tập 5:** Cho hệ mã Vigenere có M = 6, K = “LEG”.

a) Hãy thực hiện mã hóa xâu P = “THIS IS ROBOT SOPHIA“.

b) Hãy thực hiện giải mã xâu M = “PBVWEOYEZTST”.

**Bài tập 6:** Cho hệ mã Vigenere . Biết bản mã “PVRLHFMJCRNFKKW” có bản rõ tương ứng “ Networksecurity” Hãy tìm khóa K ??

a) Hãy tìm khóa mã hóa đã dùng của hệ mã trên.

b) Dùng khóa tìm được ở phần trên hãy giải mã bản mã C = “KLGZWT OMBRVW”.

**Bài tập 7:** Cho hệ mã Vigenere có M = 6. Mã hóa xâu P = “SPIRIT“ người ta thu được bản mã là “OXHRZW”.

a) Hãy tìm khóa mã hóa đã dùng của hệ mã trên.

b) Dùng khóa tìm được ở phần trên hãy giải mã bản mã C = “BQETYH HMBEEW”.

**Bài tập 8:** Cho hệ mã Vigenere có M = 6. Giải mã xâu C = “RANJLV” người ta thu được bản rõ là “CIPHER”.

a) Tìm khóa đã sử dụng của hệ mã trên.

b) Dùng khóa tìm được ở phần trên hãy hãy giải mã xâu M = “PLDKCI DUJQJO“.

Sử dụng một trong các ngôn ngữ lập trình C, C++, Java hoặc C# để làm các bài tập sau:

**Bài tập 9**: Viết chương trình đếm tần số xuất hiện của các chữ cái tiếng Anh trong một văn bản tiếng Anh ở dạng file text.

**Bài tập 10**: Viết chương trình cài đặt thuật toán mã hóa và giải mã của hệ mã Ceasar.