Câu hỏi ôn tập chương 2

Chú ý: Sinh viên phải làm đầy đủ các bài. Khi đi học trở lại trên lớp sẽ có bài test kiến thức.

1. Cho biến đọan mã sau dùng mã Cesar
   "GCUA VQ DTGCM"

   Suy luận tìm bản rõ.

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:
   UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIVUEPHZHMDZSH
   ZOWSFPAPPDTSVPQUZWYMXUZUHSXEPYEPOPDZSZUFPOUDTMOHMQ

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

3. Nêu thuật toán dùng bảng Saint Cyr để mã hóa và giải mã Vigenere khi biết từ khóa. Áp dụng thuật toán đó mã hóa bản rõ sau: "Network Security is very important for software development" với từ khóa là "COMPUTER SCIENCE"
4. Tại sao có thể nói "Có thể nói mã bộ đệm một lần là an toàn tuyệt đối, vì với bản rõ bất kỳ và bản mã bất kỳ, luôn tồn tại một khoá để ánh xạ bản rõ đó sang bản mã đã cho". Giải thích nhận định sau "Về mặt lý thuyết, xác suất để mọi mẩu tin (có cùng độ dài với bản rõ) trên bảng chữ mã là mã của một bản rõ cho trước là như nhau".
5. Tìm bản mã của bản rõ "We are studying cryptography this year" sử dụng mã Playfair với từ khóa "information technology".
6. Chứng tỏ rằng, phép dịch chuyển không khắc phục được tính dư thừa của ngôn ngữ tự nhiên.
7. Chứng minh rằng tích của hai phép thế đơn là một phép thế đơn và tích của hai phép dịch chuyển là một phép dịch chuyển. Có thể nói gì về tích của một phép thế đơn và một phép dịch chuyển.
8. Có bao nhiêu khóa Playfair khác nhau.
9. Mã hóa bản rõ "Chung toi se la nhung ky su cong nghe thong tin gioi trong mot vai nam nua" sử dụng từ khóa 631425.
10. Giả sử dùng mã dịch chuyển dòng với 8 cột. Hỏi có bao nhiêu khóa khác nhau. Nêu thuật toán giải mã với từ khóa cho trước.
11. Chứng minh rằng: tích của hai phép thế sẽ là một phép thế; tích của hai phép hoán vị sẽ là một phép hoán vị.