BÀI TẬP MẬT MÃ CHƯƠNG BA

Bài 1: Cho hệ mật RSA với p = 47, q = 61 và số mũ mã hoá e = 211.

a) Hãy tính số mũ giải mã d.

b) Hãy mã hoá bản tin m = 55 và giải mã bản mã vừa thu được.

Bài 2:

a) Giả sử ta có bản rõ '*Friday*' được mã hóa bằng hệ mã Hill với m = 2, bản mã nhận được là PQCFKU. Hãy tìm ma trận khóa mã.

b) Ta có phương thức mã hoán vị như sau : Giả sử m, n là các số nguyên dương. Ta viết bản rõ theo từng hàng thành một ma trận nxm. Sau đó tạo ra bản mã bằng cách lấy các cột của ma trận này. Cho n = 3, m = 4 hãy mô tả cách giải mã bản mã ''CETORINSOVAN '' thu được bằng phương pháp đã nêu ở trên

Bài 3:

a) Giả sử sử dụng hệ mật Playfair với từ khóa cho trước là "SECURITY"

- Hãy thiết lập ma trận khóa
- Hãy giải mã bản mã "AFSFCEYDOPKEAQDLTUOQ" thu được khi dùng ma trận khóa ở trên.

b) Hãy giải mã bản mã "OQQJOQEJGMRGQJ" thu được từ mã Affine. Biết rằng "J" là mã hóa của "t", "E" là mã hóa của "a".

Bài 4: Trong hệ mật Rabin, giả sử p = 199, q = 211

a) Tính bản mã của 1254

b) Xác định 4 bản giải mã có thể của bản mã thu được ở trên

Bài 5: Trong hệ mật Rabin, giả sử p = 199, q = 211

a) Tính bản mã của 1731

b) Xác định 4 bản giải mã có thể của bản mã thu được ở trên

Bài 6: Áp dụng thuật toán tính căn bậc hai của một số a modulo p (p là số nguyên tố). Hãy tính căn bậc hai của 75 mod 97, cho trước giá trị ngẫu nhiên b = 5 thoả mãn điều kiện $\left(\frac{b}{p}\right)=\left(\frac{5}{97}\right)=-1$.

Bài 7:

a) Hãy tìm căn bậc hai của 117 mod 2357.

b) Giải hệ phương trình đồng dư sau:

$23x \equiv 2 \bmod 37$

$14x \equiv 3 \bmod 51$

$3x \equiv 11 \bmod 19$

Bài 8:

a) Áp dụng thuật toán Euclide mở rộng tìm cặp (x, y) thoả mãn 137x + 371y = 1

b) Cho $\alpha = 18$ là một phần tử sinh của Z^*_{61}, hãy tìm tất cả các phần tử sinh còn lại của Z^*_{61}

Bài 9:

a) Hãy giải hệ phương trình đồng dư sau:

$17x \equiv 11 \bmod 99$

$5x \equiv 37 \bmod 101$

b) Tìm tập các phần tử sinh của Z^*_{41}.

Bài 10:

a) Cho $\alpha = 15$ là một phần tử sinh của Z^*_{73}, hãy tìm tất cả các phần tử sinh còn lại của Z^*_{73}.

b) Hãy áp dụng thuật toán bước lớn bước nhỏ để tính logarit rời rạc $\log_{17}15$ trên Z^*_{97}?

Bài 11: Áp dụng thuật toán tính căn bậc hai của một số a modulo p (p là số nguyên tố). Hãy tính căn bậc hai của 37 mod 41**,** cho trước giá trị ngẫu nhiên b = 3 thoả mãn điều kiện $\left(\frac{b}{p}\right)=\left(\frac{3}{41}\right)=-1$.