**Câu hỏi ôn tập thi giữa kì**

**Lí thuyết**

**Câu 1**. Nêu khái niệm về ngành mật mã? Thời kì nào kỹ thuật mật mã chưa được coi là một ngành khoa học? Tại sao?

**Câu 2** Vẽ mô hình truyền tin bảo mật? Phân tích hoạt động cơ bản trong mô hình này

**Câu 3**. Phân tích ưu nhược điểm của nguyên lý hệ mật mã đối xứng (SKC)

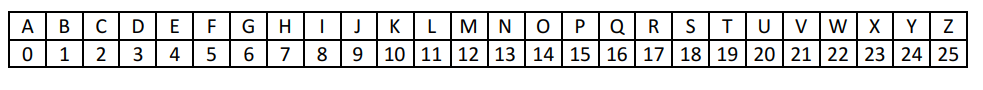
**Câu 4**. Ưu điểm chính của mật mã khóa công khai (PKC) so với mật mã đối xứng (SKC)

**Câu 5**. Các thuật toán mật mã khối thường được tổ chức như một cấu trúc nhiều vòng lặp. Hãy nêu khái niệm vòng lặp?

**Câu 6**. Mô tả tổng quan thuật toán mã hóa DES. Vẽ sơ đồ khái quát mã hóa DES (dạng tổng quát không cần vẽ sơ đồ chi tiết 16 vòng lặp)

**Bài tập**

Cho bảng chữ cái tiếng Anh với mã tương ứng

****

**Bài 1**. Giải mã bản mã sau, giả sử mã hóa Ceasar được sử dụng để mã hóa với k=3

IRXUVFRUHDQGVHYHQBHDUVDJR

**Bài 2**. Xét phương pháp Vigenere. Hãy mã hóa bản rõ ‘ATTACKTOMORROW’ với khóa ‘WIN’

**Bài 3**. Tìm nghịch đảo của 29 theo modun 37

**Bài 4**. Tính 

**Bài 3**. Cho hệ mã Knapsack có A’=(1,3,7,14), N=4, M=37, u= 29

a) Hãy tìm các khóa của hệ mã trên

b) Mã hóa và giải mã tương ứng với bản rõ 1010

**Bài 4**. Cho p=11, q=17 trong hệ RSA, chọn e=7

a) Tìm khóa riêng và khóa bí mật

b) Mã hóa X=3

c) Với bản mã Y=5, hãy giải mã Y

**Bài 5**.Trong hệ mã El-Gamal

Cho p=8, g=3, u=5, k=9

a) Hãy tìm các khóa

b) Mã hóa bản rõ X=4