**BUỔI 2: MẬT MÃ CÔNG KHAI – ĐỀ CƯƠNG**

1. Trong thuật toán RSA, tại sao phải chọn *p,q* đều lớn, nếu chỉ chọn 1 số lớn, 1 số nhỏ có được không ?

2. Trong thuật toán RSA, tại sao phải chọn *e < m*

3. bài 2 sách giáo trình trang 82

4. bài 5 sách giáo trình trang 82

**BUỔI 2 – GỢI Ý TRẢ LỜI**

*Chú ý: các gợi ý dưới đây chỉ là các ý chính, không phải là câu trả lời đầy đủ. Sinh viên cần tự mình suy nghĩ để tìm ra câu trả lời hoàn chỉnh, đầy đủ.*

1. Nếu trong hai số *p,q*  có một số nhỏ thì khi biết *n* và 1 trong hai số *p,q* sẽ dễ dàng tìm được số còn lại. Dẫn đến việc khóa bí mật sẽ dễ dàng bị lộ (Cần chứng minh rõ ràng).
2. Tương tự câu 1
3. Tự làm
4. Tự làm