Họ tên sinh viên: . . . . . Lớp: . . . . . MSSV: . . . . . STT:	Bộ môn CNPM

ĐỀ THI GIỮA KỲ
MÔN: IT4015 – Nhập môn an toàn thông tin (2021-1)

(Thời gian: phút. Không sử dụng tài liệu, điện thoại – Nộp đề kèm bài làm)

Câu 1. (6 điểm)

Gọi $abcd$ là 4 số cuối cùng trong mã số sinh viên.

p là số nguyên tố lớn nhất mà nhỏ hơn $abcd$

q là số nguyên tố lớn nhất mà nhỏ hơn $dcba$ và khác p.

a) Xây dựng 1 mã RSA với 2 số nguyên tố p, q **(2 điểm)**

b) Gọi T là chuỗi số biểu diễn tên (không có dấu) của sinh viên. Trình bày các bước sử dụng mã RSA trong câu a để mã hoá T **(2 điểm)**

(gợi ý: cần chuyển T về chuỗi nhị phân rồi mới tiến hành mã hoá)

c) Gọi C là đoạn mã sinh ra trong câu b. Hãy trình bày các bước giải mã C. **(2 điểm)**

Câu 2. (3 điểm)

Giả sử rằng A và B đều biết khóa công khai của đối phương.

a) Áp dụng các kiến thức về mật mã công khai và chữ ký số, hãy xây dựng một giao thức trao đổi giữa hai người A và B sao cho giao thức này đảm bảo tính mật, tính toàn vẹn và tính xác thực xác thực của gói tin. **(1.5 điểm)**

b) Lập luận giải thích tính mật, tính toàn vẹn và tính xác thực xác thực của giao thức vừa đề xuất **(1.5 điểm)**

Câu 3. (1 điểm)

Nêu ý kiến của em về môn học này:

a) Những điều em thấy thú vị/tâm đắc **(0.5 điểm)**

b) Những vấn đề mà theo em cần phải cải thiện để giờ học tốt hơn **(0.5 điểm)**

---------- HẾT ----------