TRƯỜNG ĐẠI HỌC GTVT KHOA CÔNG NGHỆ THÔNG TIN BỘ MÔN KHOA HỌC MÁY TÍNH	**ĐỀ THI KẾT THÚC HỌC PHẦN** **HỌC PHẦN: AN TOÀN BẢO MẬT THÔNG TIN** THỜI GIAN: 90 PHÚT	**Trưởng Bộ Môn** ***(ký ghi rõ họ tên)***

MÃ ĐỀ THI: 2021_A08

Ghi chú: ***- Thí sinh được sử dụng tài liệu trong khi làm bài.***
- Thí sinh không được trao đổi trong khi làm bài.
- Cán bộ coi thi không giải thích gì thêm.

ĐỀ BÀI

Câu 1 (1.0 điểm)

Cho bản tin M = STILLWATERSRUNDEEP được mã hóa bằng phương pháp Caesar với khóa K = 21.

Hãy trình bày cách mã hóa và cho biết kết quả mã hóa

Câu 2 (1.0 điểm)

Trình bày cách tìm nghịch đảo $x = a^{-1} \bmod n$ theo thuật toán euclid – mở rộng với giá trị a = 617; n = 3907.

Câu 3 (1.0 điểm)

Trình bày cách tính lũy thừa modulo $b = a^m \bmod n$ với giá trị

a = 463; m = 1781; n = 239

Câu 4 (2.0 điểm)

Trình bày các bước sử dụng định lý số dư trung hoa để giải hệ phương trình modulo

$$\begin{cases} x \bmod m_1 = a_1 \\ x \bmod m_2 = a_2 \\ x \bmod m_3 = a_3 \end{cases}$$

với giá trị các tham số như sau

m1 = 17; m2 = 19; m3 = 11;

a1 = 16; a2 = 18; a3 = 7;

Lưu ý: *Khi cần hỗ trợ kỹ thuật, Sinh viên liên hệ với Bộ môn theo số đt:..... ;*

Email:.....

Câu 5 (1.0 điểm)

Trình bày các bước kiểm tra số nguyên a có là một căn nguyên thủy của số nguyên n hay không? Biết a = 5; n = 257.

Câu 6 (1.0 điểm)

Giả sử An và Ba muốn trao đổi khoá phiên bằng cách sử dụng lược đồ Trao đổi khóa Diffie-Hellman, họ đồng ý chọn số nguyên tố q = 7687 và a = 6 (là căn nguyên thủy của q). Biết

An chọn khóa riêng xA = 437

Ba chọn khóa riêng xB = 354

Trình bày các bước mà An tính ra khóa công khai yA và khóa phiên K?

Câu 7 (1.5 điểm)

Thuật toán RSA

Giả sử An chọn các giá trị p = 43, q = 47, e = 67 để tạo cặp khóa.

Hãy trình bày các bước và cho biết:

a) Khóa công khai của An: PU = {e, n} =
b) cách An tạo ra khóa riêng: PR = {d, n} =
c) Cách An tạo bản mã hóa thông điệp M = 59: C =
d) Việc mã hóa ở câu c) thực hiện nhiệm vụ chữ ký số hay bảo mật.

Câu 8 (1.5 điểm)

CHỮ KÝ ĐIỆN TỬ DSA

Giả sử An cần gửi cho Ba một bản tin M kèm chữ ký số, bản tin M có mã băm là H(M) = 2.

An và Ba thống nhất các giá trị: p = 83, q = 41, h = 32

và An chọn xA = 2, k = 2

Hãy cho biết

a) Khóa công khai của An: yA =
b) Chữ ký số của An cho bản tin M: (r, s) =
c) Cách Ba xác minh chữ ký số được đính kèm với bản tin M?

Lưu ý: *Khi cần hỗ trợ kỹ thuật, Sinh viên liên hệ với Bộ môn theo số đt:..... ;*

Email:.....