



MÃ ĐỀ THI: 2021_A06

- 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 $M = \text{STILLWATERSRUNDEEP}$ được mã hóa bằng phương pháp Vigenere – Lặp Khóa với khóa $K = \text{WALLSHAV}$.

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 $a = 673$; $n = 3719$.

Câu 3 (1.0 điểm)

Trình bày cách tính lũy thừa modulo $b = a^m \bmod n$ với giá trị
 $a = 401$; $m = 1618$; $n = 269$

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

$m_1 = 19$; $m_2 = 11$; $m_3 = 13$;

$a_1 = 8$; $a_2 = 2$; $a_3 = 8$;

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 $a = 5$; $n = 263$.

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 $q = 6947$ và $a = 5$ (là căn nguyên thủy của q). Biết

An chọn khóa riêng $x_A = 395$

Ba chọn khóa riêng $x_B = 338$

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

Câu 7 (1.5 điểm)

Thuật toán RSA

Giả sử An chọn các giá trị $p = 37$, $q = 59$, $e = 53$ 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 $M = 47$: $C =$
- 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 $H(M) = 20$.

An và Ba thống nhất các giá trị: $p = 59$, $q = 29$, $h = 3$

và An chọn $x_A = 19$, $k = 25$

Hãy cho biết

- a) Khóa công khai của An: $y_A =$
- 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:.....