



**MÃ ĐỀ THI: 2021\_A03**

- 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 – Autokey với khóa  $K = \text{STILLWAT}$ .

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  $a = 683$ ;  $n = 4289$ .

**Câu 3 (1.0 điểm)**

Trình bày cách tính lũy thừa modulo  $b = a^m \bmod n$  với giá trị  
 $a = 281$ ;  $m = 1797$ ;  $n = 311$

**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

$m_1 = 11$ ;  $m_2 = 13$ ;  $m_3 = 17$ ;

$a_1 = 6$ ;  $a_2 = 11$ ;  $a_3 = 12$ ;

**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  $a = 3$ ;  $n = 353$ .**

**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  $q = 6199$  và  $a = 3$  (là căn nguyên thủy của  $q$ ). Biết**

**An chọn khóa riêng  $x_A = 531$**

**Ba chọn khóa riêng  $x_B = 540$**

**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  $p = 29$ ,  $q = 47$ ,  $e = 41$  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  $M = 43$ :  $C =$
- 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  $H(M) = 7$ .

An và Ba thống nhất các giá trị:  $p = 89$ ,  $q = 11$ ,  $h = 38$

và An chọn  $x_A = 5$ ,  $k = 2$

**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:.....