Đề thi Nhập môn an toàn thông tin Cuối kì I năm học 2022 - 2023
GV: Lê Phê Đô

# ĐỀ THI

**Sinh viên chọn làm 3 bài trong số 5 bài**

**Bài 1.** Các tham số công khai của hệ mật RSA là (n, e), ở đây n = pq.
a) Tìm giá trị hợp lệ của cặp (n, e) sao cho mỗi số nguyên tố p, q đều lớn hơn 100.
b) Xác định các tham số bí mật tương ứng (p, q, d, φ(n)).
c) Giải mã bản mã C = 2 trong hệ mật của bạn.

**Bài 2.** Xét số nguyên tố p=9973 và phần tử nguyên thủy g=11.
(a) Chỉ ra các bước của Diffie-Hellman giữa Alice và Bob sao cho họ chọn các giá trị bí mật là a = 4096 và b = 8192. Các giá trị của g^a và g^b là gì? Giá trị của khóa bí mật đã thỏa thuận là gì?
(b) Giả sử đối thủ bắt được y = 1985 của một x chưa biết sao cho y = 11^x (mod p). Có bao nhiêu x như vậy tồn tại và tại sao? Có bao nhiêu giá trị của x bạn phải tìm kiếm (theo cách vét cạn) để tìm x?
(c) Giả sử đối thủ bắt được y = 1985 cho một x chưa biết sao cho y = 2^x (mod p). Có bao nhiêu x như vậy tồn tại và tại sao lại như vậy? Có bao nhiêu giá trị của x bạn phải tìm kiếm (theo cách vét cạn) để tìm x?

**Bài 3.** Trong lớp chúng ta đã trình bày cách khởi tạo hệ khóa công khai ElGamal bằng một trong hai nhóm: (1) nhóm Z*p1 cho một số p1 nguyên tố và (2) nhóm các điểm của đường cong elip E(Fp2 ) cho một số nguyên tố p2 . Tại sao p1 phải có ít nhất 2048 bit, nhưng p2 chỉ cần 256 bit để có được mức độ bảo mật tương đương?

**Bài 4.** Anh/Chị hãy trình bày Sơ đồ xưng danh Guillou-Quisquater và cho ví dụ.

**Bài 5.** Anh/Chị hãy trình bày giao thức thỏa thuận khóa Diffie – Hellman trên hệ mật đường cong Elliptic với số nguyên tố p. Cho ví dụ p là số nguyên tố gần 10 + 2*c. Ở đây c là tháng sinh của sinh viên làm bài, còn a, b trong phương trình y^2 = x^3 + a*x + b (modp) được chọn sao cho 4*a^3 + 27*b^2 ≠ 0 (modp) và số điểm của đường cong là số nguyên tố.

$x^3$ ... 2 10 + 2*c ---