KIỂM TRA GIỮA KỲ NHẬP MÔN ATTT HK I NĂM HỌC 2022 - 2023

Câu 1. Với mỗi hệ mật cổ điển hãy trình 1 phiên bản cải tiến và đưa ra đánh giá độ mật theo số lượng khóa có thể.

Câu 2. Trình bày sơ đồ hệ mật và sơ đồ chữ ký RSA. Áp dụng để mã hóa và giải mã với p là số nguyên tố gần 20+ngày sinh nhất, q là số nguyên tố gần 30 + ngày sinh + tháng sinh nhất.

Số mũ mã hóa e = số nguyên tố gần 400 + ngày sinh + tháng sinh nhất.

a) Tính số mũ giải mã d.

b) Mã hóa và giải mã bản tin x = 201

Câu 3. Hãy xây dựng đường cong Elliptic ($E_p(a, b)$) $y^2 = x^3 + ax + b \pmod{127}$ trong đó, a = số cuối ngày sinh + 1, b= số cuối tháng + 2.

Hãy Xây dựng hệ mật EC- ElGamal trên $E_p(a, b)$ với khóa bí mật d = chữ số cuối ngày sinh + chữ số cuối tháng sinh + 5, k= chữ số cuối ngày sinh + chữ số cuối tháng sinh + 4. Mã hóa và giải mã với điểm M bản tin x là điểm M có hoành độ gần với 20 + chữ số cuối ngày sinh + chữ số cuối tháng sinh.

$x^3 + 2x + 11$