BẢO MẬT MẠNG CỤC BỘ KHÔNG DÂY

BÀI TẬP SỐ 1

Thời hạn nộp bài: 23/04/2010

1. Giả sử các kí tự (a, b, c, ..) được ánh xạ thành các số (1, 2, 3, ..). Cho p = 3, q = 11, và e = 3. Alice sử dụng thuật toán RSA để mã hóa một từ bí mật thành một ciphertext như sau (27, 1, 18, 26), rồi gửi cho Bob. Hãy trình bày cách Bob sử dụng private key để giải mã ciphertext ở trên, từ bí mật trên là gì trong hệ thống kí tự.
2. Xét thuật toán Diffie-Hellman với p = 11 và q = 2:
    a. Nếu Alice có $Y_A = 9$, thì X_A của Alice là gì?
    b. Nếu Bob có $Y_B = 3$, giá trị của shared key Z là bao nhiêu?