Đề thi kết thúc học phần 03

Câu 1 (5.0 điểm): Áp dụng phương pháp điều khiển trong truy cập và xác thực thông tin. Yêu cầu dùng phần mềm Wireshark để thực hiện các bước lấy thông tin như: tên và mật khẩu khi đăng nhập vào địa chỉ web có đường dẫn url sau: *https://dangky.hunre.edu.vn/cmcsoft.iu.web.info/(S(5zfanbgrzbzx1h0zbzwdd0sl))/login.aspx* hoặc có thể tìm một địa chỉ khác sao cho đường dẫn url có phần đăng nhập (tên và mật khẩu).

Kết quả cách làm của từng bước được copy ra file word (có thể giải mật khẩu đã được mã hóa MD5 trên các trang web mạng).

Câu 2 (5.0 điểm): Thuật toán RSA là thuật toán mã hóa công khai, được mô tả sau:

- ✓Chọn 2 số nguyên tố ngẫu nhiên lớn khác nhau $p \neq q$
- ✓n là modul cho khóa công khai và khóa riêng, với $n=p*q$
- ✓Tính $\phi(n) = (p-1)*(q-1)$
- ✓Chọn số nguyên k sao cho $1 < k < \phi(n)$ và k đồng nguyên tố với $\phi(n)$: k và $\phi(n)$ không có thừa số nào khác 1; và ước số chung lớn nhất là: $\gcd(k, \phi(n)) = 1$.
- ✓k là khóa được giải phóng dưới dạng số mũ khóa công khai
- ✓Tính d để thỏa mãn $d \equiv k^{-1} \pmod{\phi(n)}$
- ✓Khóa công khai bao gồm n và k.
- ✓Khóa riêng bao gồm p, q và số mũ riêng d

Hãy viết chương trình mô tả thuật toán trên bằng ngôn ngữ lập trình Python.

Áp dụng thử nghiệm chương trình cho ví dụ với hai số nguyên tố p=79 và q=89, bản rõ thông điệp M=100

Kết quả chạy chương trình là: Giá trị của n = 7031, Khóa k = 5, Giá trị $\phi(n)$ = 6864, Giá trị của d= 1373, Bản được mã hóa là C= 5568, Bản được giải mã ngược lại là M= 100