BÀI TẬP TUẦN 4

Bài 1. Cho ví dụ về giải thuật trao đổi khoá Diffie – Hellman

Alice và Bob muốn trao đổi khoá bí mật để tạo thành 1 khoá dùng chung qua giao thức Diffie-Hellman.

Đầu tiên Alice chọn số ngẫu nhiên a, Bob chọn b. Cả Bob và Alice đều đã biết số p và g.

Alice sử dụng công thức: A=(g^a) mod p=> gửi giá trị A cho Bob

Bob sử dụng công thức B=(g^b) mod p => gửi giá trị B cho Alice

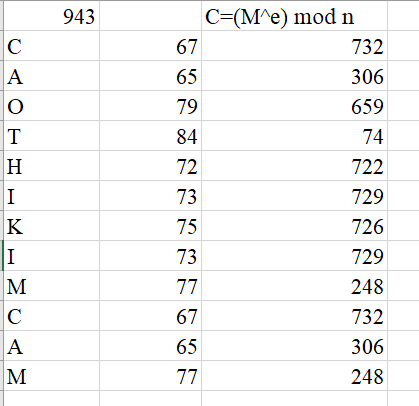
Alice và Bob sẽ nhận được khoá chung K=(B^a) mod p (Alice) = (A^b) mod p (Bob)

Có thể tìm được A,B, g, p nhưng không thể tìm được a, b nên không thể suy ra khoá chung giữa hai người.

Bài 2. Mã hoá họ tên của mình bằng giải thuật RSA biết p=23, q=41, e=13. Trong đó, các ký tự chữ cái được đánh số tương ứng dựa theo bảng mã ASCII

n=p\*q=23\*41=943

C=(M^e) mod n



C= 73230665974722729726729248732306248

Bài 3. Với p=5, q=7, e=5; các chữ cái (viết hoa) được đánh trọng số từ 0 trở đi, giả sử bạn nhận được một thông điệp: 17 19 7 9 0 12 24. Hãy giải mã thông điệp này. Từ các dữ liệu đã biết, thực hiện mã hoá thông điệp “BAO MAT THONG TIN”

* Giải mã thông điệp

N=p\*q=35

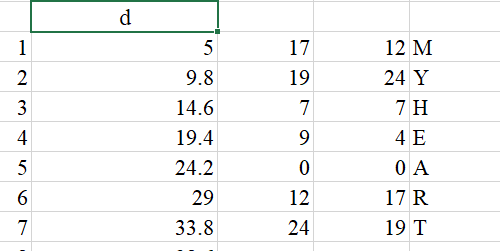
Φ(n)= (p-1)\*(q-1)=24

Chọn e = 5.

D=(e^-1) mod Φ =5

12 19 7 9 0 12 24

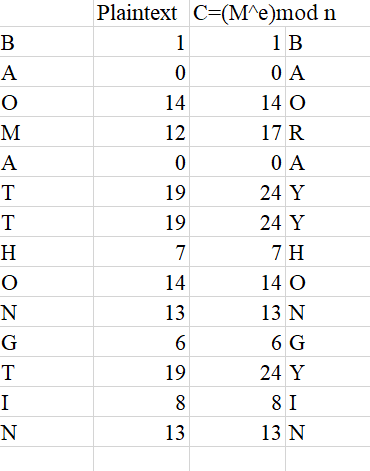
D= (C^d) mod n



C= MYHEART

* Mã hoá thông điệp: M= BAO MAT THONG TIN

C=(M^e)mod n



C=BAORAYYHONGYIN