1. **Ví dụ về giải thuật trao đổi khoá Diffie\_Hellman**

Giả sử Alice và Bob muốn tạo một khóa chung để mã hóa giao tiếp giữa họ.

1. **Chọn Số Nguyên Chung:**
   * Chọn một số nguyên tố lớn p. Ví dụ, p = 23.
   * Chọn một cơ sở g sao cho g< p. Ví dụ, g = 5.
2. **Tạo Khóa Riêng:**
   * Alice chọn một số bí mật a. Giả sử a = 6.
   * Bob chọn một số bí mật b. Giả sử b =15.
3. **Tính Khóa Công Khai:**
   * Alice tính A = g^a mod p
     + A = 5^6 mod 23 =15625 mod 23 = 8
   * Bob tính B = g^b mod p
     + B = 5 ^ 15 mod 23 = 30517578125 mod 23 = 19
4. **Trao Đổi Khóa Công Khai:**
   * Alice gửi A = 8 cho Bob.
   * Bob gửi B =19 cho Alice.
5. **Tính Khóa Bí Mật Chung:**
   * Alice nhận B = 19 và tính khóa bí mật s:
     + S = **B ^ a mod p** = 19^ 6 mod 23 = 2
   * Bob nhận A =8 và tính khóa bí mật s:
     + S = **A ^ b mod p** = 8^15 mod 23 = 1152 mod 23 = 2

**Kết Quả:** Cả Alice và Bob đều tính được khóa bí mật chung s = 2.

1. **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.**

* Lập bảng giá trị trong excel và thự hiện chuyển đổi từng kí tự trong chuỗi plain text sang mã ASCII
* Sau đó tính ra M theo công thức **C = M ^ e mod n**

**A screenshot of a computer

Description automatically generated**

1. **Với p = 5, q = 7, e = 5 các chữ cái (viết hoa) được đánh số từ 0 trở đi, giả sử bạn nhận được một thông điệp: 17 19 79 0 12 24. Hãy giải mà thông điệp này.**

**Từ các dữ liệu đã biết, thực hiện mã hoá thông điệp “BAO MAT THONG TIN"**

– Với các p, q, e đã cho ta có được bản giá trị sau:

A white grid with black letters and numbers

Description automatically generated

* Theo đó ta cũng có bảng các giá trị của d, chọn d là 5:

A screenshot of a spreadsheet

Description automatically generated

* Tiến hành mã hoá các kí tự trong cipher text theo công thức:

17 ^ 5 mod 35 = 12

19 ^ 5 mod 35 = 24

79 ^ 5 mod 35 = 4

0 ^ 5 mod 35 = 0

12 ^ 5 mod 35 = 17

24 ^ 5 mod 35 = 19

* Đổi từng kết quả đã ra theo thứ tự chữ cái trong bảng Alphabet:
* Kết quả là **M Y H E A R T**
  + - 1. Lập bảng và thực hiện phép tính trong excel ta ra được dãy cipher text kết quả

A screenshot of a computer

Description automatically generated

Cipher text: **1 0 14 17 0 24 24 7 14 13 6 24 8 33**