

ĐẠI HỌC QUỐC GIA TP.HCM
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
KHOA CÔNG NGHỆ THÔNG TIN



Bài tập môn:
Nhập môn mã hóa & mật mã.

Sinh viên thực hiện: Tôn Thất Tâm Định - 1512112

2.3

a. Vì g là primitive root của F_p nên $(g, p) = 1$. Do đó theo định lý Fermat ta có $g^{p-1} \equiv 1 \pmod{p}$.

Do đó nên ta có $g^a \equiv g^b \equiv h \pmod{p}$, điều này tương đương với $g^a \equiv g^b \cdot (g^{p-1})^k$, hay $a = k(p-1) + b$.

Vậy $a \equiv b \pmod{p-1}$.

Người ta đặt \log_g là một hàm từ $F_p \rightarrow \mathbb{Z}/(p-1)\mathbb{Z}$ để loại trừ bớt các trường hợp $a \equiv b \pmod{p-1}$.

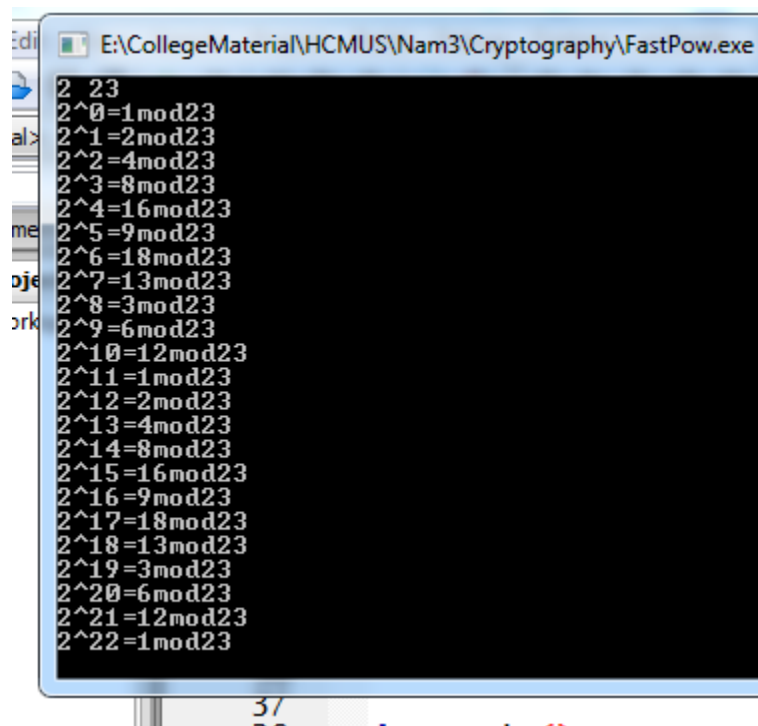
b. Đặt $x = \log_g(h_1 h_2)$, $y = \log_g(h_1)$, $z = \log_g(h_2)$.

Theo cách đặt thì ta có: $g^x \equiv h_1 h_2 \pmod{p}$, $g^y \equiv h_1 \pmod{p}$ và $g^z \equiv h_2 \pmod{p}$. Do đó $g^x \equiv g^{y+z} \pmod{p}$. Điều này tương đương với $x = y + z$.

c. Áp dụng bài b vào ta có: $\log_g(h^n) = \log_g(h) + \dots + \log_g(h) = n \log_g(h)$.

2.4

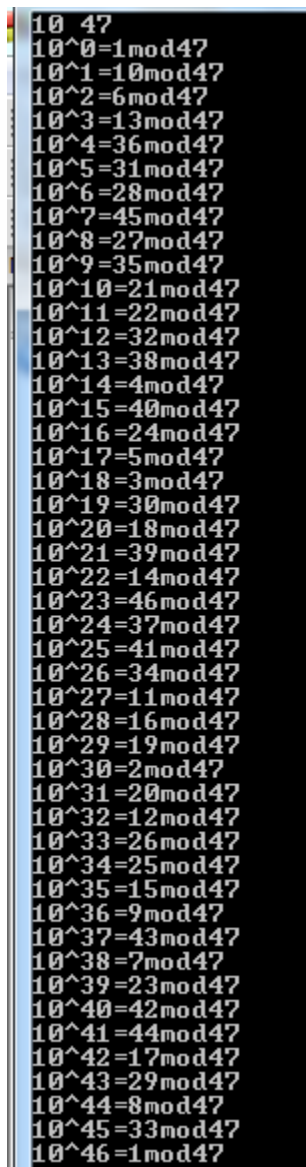
a. Ta sẽ thử tính tất cả các giá trị của $g^x \pmod{p}$ với $0 \leq x \leq p-2$.



```
E:\CollegeMaterial\HCMUS\Nam3\Cryptography\FastPow.exe
2 23
2^0=1mod23
2^1=2mod23
2^2=4mod23
2^3=8mod23
2^4=16mod23
2^5=9mod23
2^6=18mod23
2^7=13mod23
2^8=3mod23
2^9=6mod23
2^10=12mod23
2^11=1mod23
2^12=2mod23
2^13=4mod23
2^14=8mod23
2^15=16mod23
2^16=9mod23
2^17=18mod23
2^18=13mod23
2^19=3mod23
2^20=6mod23
2^21=12mod23
2^22=1mod23
```

Dựa vào kết quả tính toán ta có: $x = 7$ và $x = 18$ là giá trị cần tìm.

b. Làm tương tự câu a ta có: $x = 11$.



```
10 47
10^0=1mod47
10^1=10mod47
10^2=6mod47
10^3=13mod47
10^4=36mod47
10^5=31mod47
10^6=28mod47
10^7=45mod47
10^8=27mod47
10^9=35mod47
10^10=21mod47
10^11=22mod47
10^12=32mod47
10^13=38mod47
10^14=4mod47
10^15=40mod47
10^16=24mod47
10^17=5mod47
10^18=3mod47
10^19=30mod47
10^20=18mod47
10^21=39mod47
10^22=14mod47
10^23=46mod47
10^24=37mod47
10^25=41mod47
10^26=34mod47
10^27=11mod47
10^28=16mod47
10^29=19mod47
10^30=2mod47
10^31=20mod47
10^32=12mod47
10^33=26mod47
10^34=25mod47
10^35=15mod47
10^36=9mod47
10^37=43mod47
10^38=7mod47
10^39=23mod47
10^40=42mod47
10^41=44mod47
10^42=17mod47
10^43=29mod47
10^44=8mod47
10^45=33mod47
10^46=1mod47
```

c. Làm tương tự câu a và b ta có: $x = 18$ là giá trị cần tìm.

2.6. Ta có: $p = 1373$, $g = 2$, $A = 974$, $b = 871$.

Theo thuật toán tạo khóa Diffie-Hellman ta có: $B \equiv g^b(\text{mod } p) \equiv 805(\text{mod } p)$ đồng thời ta tính được khóa trao đổi giữa 2 người là: $g^{ab} \equiv (g^a)^b \equiv A^b \equiv 397(\text{mod } p)$.

Giá trị của a sao cho $g^a \equiv A(\text{mod } p)$ là:

2.7

- a. Nếu ta giải được bài toán Diffie-Hellman thì ta có thể tính được g^{ab} từ g^a và g^b , rồi sau đó lấy giá trị này so sánh với C . Khi đó bài toán Diffie-Hellman Decision Problem được giải quyết.
- b. Bài toán Diffie-Hellman Decision là một bài toán dễ. Vì người ta đã có thể tìm được một vài elliptic curve trên F_p sao cho có thể dễ dàng kiểm tra được C có bằng g^{ab} hay không. Cho nên bài toán DHD là bài toán dễ hơn so với bài toán DH và DLP.