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

Bài tập Elgammal và Primitive Test

Sinh viên thực hiện: Tôn Thất Tâm Định – 1512112

2.8. Ta có: p = 1373, g = 2 là các public key

a) Khi Alice chọn private key a = 947, thi public mà Alice gửi là $A \equiv g^a \equiv 177 (\text{mod } p)$.

b) Khi Bob chọn private key b = 716 và public key $B = g^b = 469 (\text{mod p})$. Alice muốn gửi thông điệp m thì phải gửi cặp số $(c_1, c_2) = (g^k, mB^k) = (g^k, mg^{bk}) = (719, 623)$

c) Cặp giá trị (c_1, c_2) mà Bob gửi là $(g^k \text{ mod p}, mg^{ak} \text{ mod p})$ do đó để tìm lại m ta chỉ cần tính: $x \equiv \left(c_1^{\,a}\right)^{-1} \equiv \left(g^{ak}\right)^{-1} (\text{mod } p)$ và tính $xc_2 \equiv mg^{ak}\left(g^{ak}\right)^{-1} \equiv m (\text{mod } p)$.

Tính toán ta có $x \equiv 645^{-1} \equiv -579 \equiv 794 (\text{mod} 1373)$ và

$m \equiv xc_2 \equiv 794 \times 1325 \equiv 1332 (\text{mod} 1373)$.

d) Cặp giá trị (c_1, c_2) mà Alice gửi cho Bob là $(g^k \text{ mod p}, mg^{bk} \text{ mod p})$ nên nếu Eve biết b thì sẽ phá được mật thư này. Với b thỏa $2^b \equiv 893 (\text{mod} 1373)$. Dùng máy tính ta tìm được giá trị b = 219

Từ đó $x \equiv \left(c_1^{\,b}\right)^{-1} \equiv \left(g^{bk}\right)^{-1} \equiv 431^{-1} \equiv 532 (\text{mod } p)$ và $m \equiv xc_2 \equiv 532 \times 793 \equiv 365 (\text{mod} 1373)$.

2.9.

Nếu ta giải được bài toán DF tức là tính được $g^{ab} \text{ mod p}$ từ $g^a \text{ mod p}$ và $g^b \text{ mod p}$ thì khi đó với public key $A = g^a \text{ mod p}$ và $c_1 = g^k \text{ mod p}$ ta sẽ tính được $x^{-1} = g^{ak} \text{ mod p}$ và từ đó tính ra $x = (g^{ak})^{-1} \text{ mod p}$. Kết hợp giá trị x này với $c_2 = mg^{ak}$ ta sẽ tính lại được m. Vậy hệ mã El-Gammal bị phá.

2.10.

Theo định lý Fermat ta có: $a^{p-1} \equiv 1 (\text{modp})$ với (a, p) = 1. Do đó với mọi x ta có: $a^x \equiv a^{k(p-1)+y} \equiv a^y (\text{mod } p)$ nên suy ra $a^x \equiv a^{x \text{mod}(p-1)} (\text{mod } p)$. Giá trị 15619 mà Alice chọn thật ra là $x = a^{-1} (\text{mod } p-1)$ và giá trị b = 31883 mà Bob chọn là $y = b^{-1} (\text{mod } p-1)$. Để sau đó ta có $m^{ab.xy} \equiv m^{abxy\%(p-1)} \equiv m^1 (\text{mod } p)$.

b)Từ đó ta có bảng mô tả cách hoạt động của thuật toán như sau.

Public key: p	
Alice	Bob

Private key: a Message: m Compute: u = m^a (mod p) and send to Bob	
	Chose random b. Compute v = u^b = m^{ab}(mod p) and send to Alice
Compute x = a^{-1}(mod p – 1) Compute w = v^x = $m^{ab.x \text{ (mod p – 1)}}$ (mod p)	
	Compute y = b^{-1}(mod p – 1) Compute w^y = $m^{ab.xy \text{ mod (p-1)}}$=m (mod p).

c) Điểm hạn chế của thuật toán là Alice và Bob phải giao tiếp 2 lần mới có thể truyền được dữ liệu mong muốn. Điều này làm tăng khả năng gói tin bị bắt trên đường truyền dẫn đến sự truyền dễ bị phá.

d) Nếu ta giải được bài toán DLP thì thuật toán sẽ bị phá vì khi đó ta bắt được v thì ta sẽ có được ab từ đó dễ dàng có được $(ab)^{-1}$(mod p – 1) và tính lại được m dễ dàng. Nhưng nếu giải được bài DH thì ta chưa thể phá được hệ thống mã này vì bài toán DH chỉ là tính g^{ab} mod p dựa trên g^a, g^b. Do đó đây chính là điểm mạnh của thuật toán này so với ElGammal.

3.13. Carmichael number là số n thỏa $a^n \equiv a(\text{mod}\, n)$ với mọi a nhưng n không là số nguyên tố.

a) Theo định lý Fermat ta có: $a^{p-1} \equiv 1(\text{mod}p)$ với (a, p) = 1. Do đó với mọi x ta có: $a^x \equiv a^{k(p-1)+y} \equiv a^y \,(\text{mod}\, p)$ nên suy ra $a^x \equiv a^{x \text{mod}(p-1)} (\text{mod}\, p)$.

Do đó $a^{560} \equiv a^{560 \text{mod} 2} \equiv a^0 \equiv 1(\text{mod}\, 3)$ hay $a^{561} \equiv a(\text{mod}\, 3)$.

Tương tự ta cũng chứng minh được $a^{560} \equiv a^{560 \text{mod} 10} \equiv a^0 \equiv 1(\text{mod} 11)$ và $a^{560} \equiv a^{560 \text{mod} 16} \equiv a^0 \equiv 1(\text{mod} 17)$.

Theo định lý thặng dư trung hoa thì pt: $\begin{cases} a^{560} \equiv 1 (\mathrm{mod}\, 3) \\ a^{560} \equiv 1 (\mathrm{mod}\, 11) \\ a^{560} \equiv 1 (\mathrm{mod}\, 17) \end{cases}$ có nghiệm duy nhất trên modulo 3x11x17.

Xét $x \equiv (11 \times 17)^2 + (3 \times 17)^{10} + (3 \times 11)^{16} \equiv 1 (\mathrm{mod}\, 561)$. Do đó $a^{560} \equiv 1 (\mathrm{mod}\, 561)$ hay $a^{561} \equiv a (\mathrm{mod}\, 561)$.

b)

(i) Khi n = 1729, ta có: $a^{n-1} \equiv a^{(n-1)\%6} \equiv 1 (\mathrm{mod}\, 7)$, $a^{n-1} \equiv a^{(n-1)\%12} \equiv 1 (\mathrm{mod}\, 13)$ và $a^{n-1} \equiv a^{(n-1)\%18} \equiv 1 (\mathrm{mod}\, 19)$.

Theo định lý thặng dư trung hoa thì pt: $\begin{cases} a^{n-1} \equiv 1 (\mathrm{mod}\, 7) \\ a^{n-1} \equiv 1 (\mathrm{mod}\, 13) \\ a^{n-1} \equiv 1 (\mathrm{mod}\, 19) \end{cases}$ có nghiệm duy nhất trên modulo 7.13.19.

Xét $x \equiv (13 \times 19)^6 + (7 \times 19)^{12} + (7 \times 13)^{18} \equiv 1 (\mathrm{mod} 1729)$ là nghiệm của hệ đồng dư trên. Do đó $a^{n-1} \equiv 1 (\mathrm{mod} n)$ hay $a^n \equiv a (\mathrm{mod} n)$.

(ii) Tương tự câu (i) khi n = 10585, ta có: , ta có: $a^{n-1} \equiv a^{(n-1)\%4} \equiv 1 (\mathrm{mod}\, 5)$, $a^{n-1} \equiv a^{(n-1)\%28} \equiv 1 (\mathrm{mod}\, 29)$ và $a^{n-1} \equiv a^{(n-1)\%72} \equiv 1 (\mathrm{mod}\, 73)$.

Theo định lý thặng dư trung hoa thì pt: $\begin{cases} a^{n-1} \equiv 1 (\mathrm{mod}\, 5) \\ a^{n-1} \equiv 1 (\mathrm{mod}\, 29) \\ a^{n-1} \equiv 1 (\mathrm{mod}\, 73) \end{cases}$ có nghiệm duy nhất trên modulo 5.29.73.

Xét $x \equiv (29 \times 73)^4 + (5 \times 73)^{28} + (5 \times 29)^{72} \equiv 1 (\mathrm{mod} 10585)$ là nghiệm của hệ đồng dư trên. Do đó $a^{n-1} \equiv 1 (\mathrm{mod} n)$ hay $a^n \equiv a (\mathrm{mod} n)$.

(iii) khi n = 75361, ta có: $a^{n-1} \equiv a^{(n-1)\%10} \equiv 1 (\mathrm{mod}\, 11)$, $a^{n-1} \equiv a^{(n-1)\%12} \equiv 1 (\mathrm{mod}\, 13)$, $a^{n-1} \equiv a^{(n-1)\%16} \equiv 1 (\mathrm{mod}\, 17)$ và $a^{n-1} \equiv a^{(n-1)\%30} \equiv 1 (\mathrm{mod}\, 31)$

Theo định lý thặng dư trung hoa thì pt: $\begin{cases} a^{n-1} \equiv 1 (\mod 11) \\ a^{n-1} \equiv 1 (\mod 13) \\ a^{n-1} \equiv 1 (\mod 17) \\ a^{n-1} \equiv 1 (\mod 31) \end{cases}$ có nghiệm duy nhất trên

modulo 11.13.17.31.

Xét $x \equiv (13 \times 17 \times 31)^{10} + (11 \times 17 \times 31)^{12} + (11 \times 13 \times 31)^{16} + (11 \times 13 \times 17)^{30} \equiv 1 (\mod 75361)$ là nghiệm của hệ đồng dư trên. Do đó $a^{n-1} \equiv 1 (\mod n)$ hay $a^n \equiv a (\mod n)$.

(iv) khi n = 1024651, ta có: $a^{n-1} \equiv a^{(n-1)\%18} \equiv 1 (\mod 19)$,
$a^{n-1} \equiv a^{(n-1)\%198} \equiv 1 (\mod 199)$, $a^{n-1} \equiv a^{(n-1)\%270} \equiv 1 (\mod 271)$ và

Theo định lý thặng dư trung hoa thì pt: $\begin{cases} a^{n-1} \equiv 1 (\mod 19) \\ a^{n-1} \equiv 1 (\mod 199) \\ a^{n-1} \equiv 1 (\mod 271) \end{cases}$ có nghiệm duy nhất trên

modulo 19.199.271 = 1024651.

Xét $x \equiv (199 \times 271)^{18} + (19 \times 271)^{198} + (19 \times 199)^{270} \equiv 1 (\mod 1024651)$ là nghiệm của hệ đồng dư trên. Do đó $a^{n-1} \equiv 1 (\mod n)$ hay $a^n \equiv a (\mod n)$.

c) Nếu n là một số Carmichael thì $a^{n-1} \equiv 1 (\mod n)$ nên nếu số Carmichael là 1 số chẵn thì ta xét a = n – 1 ta có:

$(n-1)^{n-1} \equiv (-1)^{n-1} \equiv (-1) (\mod n)$ mâu thuẫn.

d) Gọi n là một số Carmichael. Chúng ta sẽ chứng minh số mũ của các thừa số trong p < 2. Vì n là một số Carmichael nên n lẻ và n phải lớn hơn 2.

Giả sử tồn tại một số nguyên v sao cho $n \vdots v^2$, và do n là một số Carmichael nên ta có $v^n - v \vdots n$ và $v^n \vdots v^2$. Từ đó ta suy ra $v \vdots v^2$ (Vô lý). Từ đây ta suy ra $\text{ord}_p(n) < 2$ với mọi p. Do đó n là tích của các số nguyên tố khác nhau.

3.14.

c)

294409 là hợp số theo Miller-Rabin test với Miller-rabin witness là 22983.

d)

n = 118901509 là số nguyên tố theo Miller-Rabin test với 10 giá trị không là Miller-Rabin witnesses là

test num =24916

test num =11574

test num =3321

test num =10598

test num =20270

test num =8730

test num =31802

test num =22049

test num =11466

test num =25633

e) 118901521 là hợp số với Miller-Rabin witness là test num =25165

f) 118901527 là số nguyên tố với 10 giá trị không là Miller-Rabin là

test num =25272

test num =3503

test num =17204

test num =12059

test num =30447

test num =10760

test num =10611

test num =30656

test num =8989

test num =10854

g) 118915387 là hợp số với giá trị Miller-Rabin witness là: test num =25459.