BÀI 5: ỨNG DỤNG CÁC THUẬT TOÁN

Nội dung

- Các thuật toán trên modulo
  - Quan hệ đồng dư.
  - Thuật toán Euclid.
  - Thuật toán bình phương nhân liên tiếp.
  - Thuật toán Euclid mở rộng.
  - Căn nguyên thủy và logarit rời rạc.
- Thuật toán RSA.
- Thủ tục trao đổi khóa Diffie-Hellman.
- Thuật toán chữ ký điện tử DSA.

Mục tiêu

- Biết cách thực hành các phép toán số học đồng dư.
- Áp dụng được các định lý Ferma nhỏ, Euler.
- Thao tác trên các thuật toán Euclid, Euclid mở rộng, bình phương và nhân liên tiếp.
- Giải được RSA với các số nhỏ.
- Biết tạo và kiểm tra chữ ký DSA.

Thời lượng học

- 6 tiết.

TÌNH HUỐNG DẪN NHẬP

Tình huống

- Để hiểu được các thuật toán mã công khai, cần phải tính toán trên modulo.
- Tính toán trên các số lớn cần các thuật toán hiệu quả: Euclid, Euclid mở rộng, bình phương và nhân liên tiếp.
- Cơ sở là các định lý số học Ferma, Euler.
- Hiểu và thực hành được trên các thuật toán RSA và chữ ký điện tử DSA.

Câu hỏi

1. Làm sao có thể cộng, trừ, nhân, chia cho số khác 0 trên các số nguyên có độ lớn không vượt quá phạm vi cho trước. Các phép toán đó được tính toán như thế nào?
2. Việc sử dụng các định lý cơ bản về số học modulo trong việc tính toán các biểu thức, đặc biệt là tính lũy thừa theo modulo được thực hiện như thế nào?
3. Nêu việc ứng dụng các cặp các bài toán thuận-dễ, nghịch-khó vào mã công khai. Trình bày các bước tính toán của thuật toán RSA, thủ tục trao đổi khóa Diffie – Hellman và chữ ký điện tử DSA.

5.1. Các thuật toán MODULO

5.1.1. Số học đồng dư

- Giả sử n là số nguyên dương, a là số nguyên, ta biểu diễn dưới dạng:

$$a = \lfloor a/n \rfloor .n + a \bmod n \qquad (*)$$

- Viết công thức (*) cho các cặp số (n, a) sau:
  - (15, 51): 51 = ?
  - (15, –51): –51 = ?
- Tìm đại diện của các số 215 và –157 theo mod 29
  - 215 mod 29 =
  - (–157) mod 29 =
- Theo modulo 13: chia tập các số từ –26 đến 25 thành các lớp tương đương, nêu các đại diện của chúng?
- Biểu thức nào đúng:
  - 101 ≡ 36 mod 13?
  - (–101) ≡ (–36) mod 13?
  - 165 ≡ 34 mod 65?
  - (–165) ≡ 30 mod 65?
- Viết công thức (*) cho các cặp số (n, a) sau:
  - (15, 51): 51 = 3.15 + 6; Do đó theo định nghĩa: 51 mod 15 = 6
  - (15, –51): –51 = –4.15 + 9; Vậy: (–51) mod 15 = 9
- Tìm đại diện của các số 215 và -157 theo mod 29
  - 215 mod 29 = 12; Do đó theo định nghĩa: 12 là đại diện của 215 theo modulo 29
  - –158 mod 29 = 29 – 158 mod 29 = 29 – 13 = 16
- Các lớp tương đương và đại diện modulo 13:

-26 -25 -24 -23 -22 -21 -20 -19 -18 -17 -16 -15 -14
-13 -12 -11 -10 -9 -8 -7 -6 -5 -4 -3 -2 -1
0 1 2 3 4 5 6 7 8 9 10 11 12
13 14 15 16 17 18 19 20 21 22 23 24 25

Hàng viết đậm từ 0 đến 12 gồm các đại diện của modulo 13.

- Quan hệ tương đương đồng dư: hai số có quan hệ đồng dư theo modulo n, nếu chúng có cùng số dư khi chia cho n:
  - 101 ≡ 36 mod 13? – Đúng
  - -101 ≡ -36 mod 13? – Sai
  - 165 ≡ 34 mod 65? - Sai
  - -165 ≡ 30 mod 65? - Đúng

Các công thức cộng, trừ, nhân theo modulo:

$$(a \pm b) \bmod n = [a \bmod n \pm b \bmod n] \bmod n \qquad (**)$$

$$(a.b) \bmod n = [a \bmod n \,.\, b \bmod n] \bmod n \qquad (***)$$

- Lập bảng nhân theo modulo 11, nêu các cặp nghịch đảo nhau trong bảng.
- Bạn có thể thay các số bằng các số tương đương theo mod n bất cứ lúc nào?
  - (74 - 215) mod 9 = ?
  - (244.315) mod 250 = ?
  - (144.315 – 265.657) mod 51 = ?

Bảng nhân modulo 11

×	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	8	2	6	10	3	4
5	0	5	10	4	8	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	11	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

Các cặp sau nghịch đảo nhau theo modulo 11, vì chúng có tích theo modulo bằng 1:
(1, 1), (2, 6), (3, 4), (4, 3), (5, 9), (6, 2), (7, 8), (8, 7), (9, 5), (10, 10).
Cộng, nhân modulo

- Áp dụng tính chất (**):
  (74 – 215) mod 9 = – 141 mod 9 = 9 – 141 mod 9 = 9 – 6=3
  hay (74 mod 9 – 215 mod 9) mod 9 =
  (2 – 8) mod 9 = – 6 mod 9 = 3.
- Áp dụng tính chất (***):
  (244 . 315) mod 250 = (244 mod 250 . 315 mod 250) mod 250
  = ((–6) mod 250 . 65 mod 250) mod 250 = (– 6 .65) mod 250 = (– 390) mod 250
  = 250 – 390 mod 250 = 250 – 140 =110.
- (144.315 – 265.657) mod 51
  = (144.315 mod 51 – 265.657 mod 51) mod 51
  = (–9.9 mod 51– (10.(– 6)) mod 51) mod 51
  = (–81 + 60) mod 51 = –21 mod 51 = 51 – 21 mod 51 = 30.

5.1.2. Thuật toán Euclid

Áp dụng thuật toán Euclid:

2110 = 1 × 1945 + 165 gcd(1945, 165)
1945 = 11 × 165 + 130 gcd(165, 130)
165 = 1 × 130 + 35 gcd(130, 35)
130 = 3 × 35 + 25 gcd(35, 25)
35 = 1 × 25 + 10 gcd(25, 10)

$25 = 2 \times 10 + 5$ gcd(10, 5)
$10 = 2 \times 5 + 0$ gcd(5, 0)

Vậy ta có ước chung cần tìm là 5:

GCD(2110, 1945) = GCD(5, 0) = 5.

Thuật toán Euclid mở rộng

- Số a được gọi là nghịch đảo của b theo mod m, ký hiệu $a = b^{-1} \bmod m$, nếu

  $(a.b) \bmod m = 1$.

  Nếu gcd(b, m) = 1, tức là hai số nguyên tố cùng nhau, thì tồn tại $b^{-1} \bmod m$.
- Tìm trực tiếp bằng định nghĩa:
  - $6^{-1} \bmod 11 = ?$
  - $5^{-1} \bmod 11 = ?$
  - $6^{-1} \bmod 13 = ?$
  - $12^{-1} \bmod 13 = ?$; $(n–1)^{-1} \bmod n = ?$
  - $13^{-1} \bmod 15 = ?$
  - $21^{-1} \bmod 25 = ?$

Giải:

- $6^{-1} \bmod 11 = 2$, vì $6.2 \bmod 11 = 1$
- $5^{-1} \bmod 11 = 9$, vì $9.5 \bmod 11 = 1$
- $6^{-1} \bmod 13 = 11$, vì $(-2).6 \bmod 13 = 1$
- $12^{-1} \bmod 13 = (-1)^{-1} \bmod 13 = –1 \bmod 13 = 12$
- $(n–1)^{-1} \bmod n = n–1$
- $13^{-1} \bmod 15 = (–2)^{-1} \bmod 15 = –8 \bmod 15 = 7$
- $21^{-1} \bmod 25 = (–4)^{-1} \bmod 15 = 6$
- Với các số lớn thì ta dùng thuật toán nào để tìm nghịch đảo của số b theo modulo n?
  - $845^{-1} \bmod 2011 = ?$ Ta sử dụng thuật toán Euclid mở rộng để tìm nghịch đảo.

Q	A1	A2	A3	B1	B2	B3
—	1	0	2011	0	1	845
2	0	1	845	1	–2	321
2	1	–2	321	–2	5	203
1	–2	5	203	3	–7	118
1	3	-7	118	-5	12	85
1	-5	12	85	8	-19	33
2	8	-19	33	-21	50	19
1	-21	50	19	29	-69	14
1	29	-69	14	-50	119	5
2	-50	119	5	129	-307	4
1	129	-307	4		426	1

- Vậy $845^{-1} \bmod 2011 = 426 \bmod 2011 = 426$.

5.1.3. Các định lý số học cơ bản

- **Định lý Fermat nhỏ:** Cho p là số nguyên tố và a là số nguyên dương không là bội của p, tức là GCD(a, p) = 1. Khi đó

$$a^{p-1} \pmod p = 1$$

hay $$a^p \pmod p = a \pmod p.$$

- Tính các giá trị sau:
  - $5^{12} \pmod{13} = 1$
  - $8^{13} \pmod{13} = 8$
  - $10^{100} \pmod{17} = (10^{16})^6 . 10^4 \pmod{17} = 9^2 \bmod 17 = 13$
  - $15^{125} \pmod{19} = (15^{18})^7 . 15^{-1} \pmod{19} = 14$
- **Hàm Euler**. Hàm Euler của một số n là số các số nguyên tố cùng nhau với n và nhỏ hơn n.

N	Φ(n)	Điều kiện
P	P - 1	p nguyên tố
p^n	$p^n - p^{n-1}$	p nguyên tố
s.t	Φ(s).Φ(t)	s, t nguyên tố cùng nhau
p.q	(p-1)(q-1)	p, q hai nguyên tố khác nhau

- Tính giá trị hàm Euler:
  - $\Phi(23) = 22$
  - $\Phi(55) = \Phi(5.11) = \Phi(5).\Phi(11) = 4.10 = 40$
  - $\Phi(180) = \Phi(4.5.9) = \Phi(4).\Phi(5).\Phi(9) = \Phi(2^2).\Phi(5).\Phi(3^2) = (2^2-2).4.(3^2-3) = 48$
  - $\Phi(200) = \Phi(8.25) = \Phi(2^3).\Phi(5^2) = (2^3-2^2).(5^2-5) = 80$
  - $\Phi(900) = \Phi(4.9.25) = \Phi(4).\Phi(9).\Phi(25) = \Phi(2^2).\Phi(3^2).\Phi(5^2)$ $= (2^2-2).(3^2-3).(5^2-5) = 2.6.20 = 240$
  - $\Phi(6300) = \Phi(7.900) = \Phi(7).\Phi(900) = 6.240 = 1440$

Định lý Euler

- Cho a, n là hai số tự nhiên nguyên tố cùng nhau, tức là gcd(a,n) = 1. Khi đó

$$a^{\Phi(n)} \pmod n = 1$$

- Tính:
  - $4^8 \bmod 15 = 1$, vì $\Phi(15) = 8$, gcd(4, 15) = 1.
  - $11^9 \bmod 20 = 10$, vì $\Phi(20) = 8$, gcd(11, 20) = 1
  - $12^{402} \bmod 25 = 19$, vì $\Phi(25) = 20$, gcd(12, 25) = 1, $402 = 20.20 + 2$,
  - $12^{402} \bmod 25 = 12^{400}.12^2 \bmod 25 = 144 \bmod 25 = 19$

- $135^{162} \bmod 64 = (135 \bmod 64)^{32.5+2} \bmod 64 = 7^2 \bmod 64 = 49$, vì $\Phi(64) = \Phi(2^6) = 64 - 32 = 32$
- $335^{453} \bmod 23 = (335 \bmod 23)^{22.20+13} \bmod 23 = 5^{13} \bmod 23 = 5^8.5^4.5 \bmod 23 = 16.4.5 \bmod 23 = 21$, vì $\Phi(23) = 22$
- $(3/7)^8 \bmod 10 = (3.7^{-1})^8 \bmod 10 = (3.3)^8 \bmod 10 = (-1)^8 \bmod 10 = 1$

5.1.4. Lũy thừa theo modulo

- Dựa vào định lý Euler đơn giản bài toán.
- Theo thuật toán lũy thừa dựa trên biểu diễn nhị phân của số mũ n
  - $11^{23} \bmod 187$
    $23 = 16 + 4 + 2 + 1$; $23_2 = 10111$
    $11^{23} \bmod 187 = (((((11)^2)^2.11)^2.11)^2.11) \bmod 187$
- Trên thực tế tính toán bằng tay được dựa trên phép lặp bình phương và nhân với cơ số
  - $11^{23} \bmod 187 = 11^{16}.11^4.11^2.11 \bmod 187$
  - $11^2 \bmod 187 = 121$
  - $11^4 \bmod 187 = 121^2 \bmod 187 = 55$
  - $11^8 \bmod 187 = 55^2 \bmod 187 = 3025 \bmod 187 = 33$
  - $11^{16} \bmod 187 = 33^2 \bmod 187 = 1089 \bmod 187 = 154$
  - $11^{23} \bmod 187 = 11^{16}.11^4.11^2.11 \bmod 187 = (154.55.121.11) \bmod 187$
    $= (-33.(-66).5.11.11) \bmod 187 = 3.6.5.11^4 \bmod 187 = 3.6.5.55 \bmod 187$
    $= 265 \bmod 187 = 88$

Căn nguyên thủy

- Xét m để $a^m \bmod n = 1$.
  Nếu giá trị $m = \Phi(n)$ là số dương nhỏ nhất thoả mãn công thức trên thì, a được gọi là căn nguyên thủy của n.
- a = 2 có phải là căn nguyên thủy của 7 không? $\Phi(7) = 6$
  $2 \bmod 7 = 2$; $2^2 \bmod 7 = 4$; $2^3 \bmod 7 = 1$;
  $3 < 6 = \Phi(7)$, vậy 2 không là căn nguyên thủy của 7.
- a = 2 có phải là căn nguyên thủy của 11 không? $\Phi(11) = 10$
  $2 \bmod 11 = 2$; $2^2 \bmod 11 = 4$; $2^3 \bmod 11 = 8$;
  $2^4 \bmod 11 = 5$; $2^5 \bmod 11 = 10$; $2^6 \bmod 11 = 9$,
  $2^7 \bmod 11 = 7$; $2^8 \bmod 11 = 3$; $2^9 \bmod 11 = 6$, $2^{10} \bmod 11 = 1$
  Vậy 2 là căn nguyên thủy của 11.
- a = 3 có phải là căn nguyên thủy của 11 không? $\Phi(11) = 10$
  $3 \bmod 11 = 3$; $3^2 \bmod 11 = 9$; $3^3 \bmod 11 = 5$;
  $3^4 \bmod 11 = 4$; $3^5 \bmod 11 = 1$;
  $5 < 10 = \Phi(11)$, vậy 3 không là căn nguyên thủy của 11.

- Ta lấy ví dụ một số cặp (số nguyên tố, căn nguyên thủy) sau:
  (3, 2); (5, 2); (7, 3), (11, 2); (13, 6); (17, 10); (19, 10); (23, 10)

Logarit rời rạc

- Cho a, b, p là các số tự nhiên, với gcd(a,p)=1 = gcd(b,p)
- Tìm x sao cho $a^x = b \bmod p$ hay $x = \log_a b \bmod p$
- Dễ dàng thấy, nếu a là căn nguyên thủy của p thì luôn luôn tồn tại:
  - $x = \log_2 5 \bmod 11 = 4$
    $2^0 \bmod 11 = 1$; $2^1 \bmod 11 = 2$; $2^2 \bmod 11 = 4$;
    $2^3 \bmod 11 = 8$; $2^4 \bmod 11 = 5$;
  - $x = \log_2 5 \bmod 13 = 9$
    $2^0 \bmod 13 = 1$; $2^1 \bmod 13 = 2$; $2^2 \bmod 13 = 4$;
    $2^3 \bmod 13 = 8$; $24 \bmod 13 = 3$; $2^5 \bmod 13 = 6$;
    $2^6 \bmod 13 = 12$; $2^7 \bmod 13 = 11$; $2^8 \bmod 13 = 9$;
    $2^9 \bmod 13 = 5$;
  - $x = \log_3 7 \bmod 13 = ?$
    $3^0 \bmod 13 = 1$; $3^1 \bmod 13 = 3$; $3^2 \bmod 13 = 9$;
    $3^3 \bmod 13 = 1$,

Vô nghiệm (3 không phải là căn nguyên thủy của 13).

- Trong khi lũy thừa là bài toán dễ dàng, thì bài toán logarit rời rạc là bài toán khó.

5.2. Mã công khai RSA

- Chọn ngẫu nhiên 2 số nguyên tố p và q
- Tính: $N = p.q$; $\Phi(N) = (p - 1).(q - 1)$
- Người dùng A chọn ngẫu nhiên khoá công khai (hoặc riêng) e: $1 < e < \Phi(N)$, $\gcd(e, \Phi(N)) = 1$.
- Tìm khóa riêng (hoặc công khai) d của A: $(e.d) \bmod \Phi(N) = 1$, $0 < d < \Phi(N)$.
- Để mã hoá mẩu tin gửi cho A, người gửi B:
  - Tính $C = M^e \bmod n$, trong đó $0 \le M < n$.
  - Để giải mã, người sở hữu khóa riêng:
  - Tính $M = C^d \bmod n$
- Để ký mẩu tin M gửi cho B, người gửi A mã bằng khóa riêng của mình:
  - Tính $C = M^d \bmod n$, trong đó $0 \le M < n$.
- Để kiểm tra chữ ký, người nhận giải mã bằng khóa công khai của người gửi:
  - Tính $M = C^e \bmod n$
- Cho p = 3; q = 11; khóa công khai e = 7; thông điệp M = 5.
  - $N = 3.11 = 33$; $\Phi(N) = 2.10 = 20$;
  - $d = e^{-1} \bmod \Phi(N) = 7^{-1} \bmod 20 = 3$, khóa riêng d = 3;
  - Mã: $C = M^e \bmod n = 5^7 \bmod 33 = (-8)(-2).5 \bmod 33 = 14$;
  - Giải mã: $M = C^d \bmod n = 14^3 \bmod 33 = (-2).14 \bmod 33 = 5$.

- Cho p = 5; q = 11; khoá riêng e = 3; thông điệp M = 9.
  - N = 5.11 = 55 ; $\Phi(N) = 4.10 = 40$;
  - $d = e^{-1} \bmod \Phi(N) = 3^{-1} \bmod 40 = 27$, khóa công khai d = 27;
  - Ký: $C = M^e \bmod n = 9^3 \bmod 55 = 26.9 \bmod 55 = 14$;
  - Kiểm tra chữ ký: $M = C^d \bmod n = 14^{27} \bmod 55 = (14^{16}.14^8.14^2.14) \bmod 55$
    $= (36.16.31.14) \bmod 55 = (26(-6)) \bmod 55 = 9$;
  - $14^2 \bmod 55 = 31$, $14^4 \bmod 55 = 26$, $14^8 \bmod 55 = 16$, $14^{16} \bmod 55 = 36$.
- Cho p = 7; q = 11; khoá công khai e = 13; thông điệp M = 3.
  - N = 7.11 = 77; $\Phi(N) = 6.10 = 60$;
  - Khóa riêng $d = e^{-1} \bmod \Phi(N) = 13^{-1} \bmod 60 = 37$;
  - Mã: $C = M^e \bmod n = 3^{13} \bmod 77 = (3^8 3^4 3) \bmod 77 = (4^2.4.3) \bmod 77 = 38$;
  - Giải mã: $M = C^d \bmod n = 38^{37} \bmod 77 = 3$.
- Có thể dùng định lý phần dư Trung Hoa để giải mã cho nhanh:
  - Tính $C^d \bmod 7 = 38^{37} \bmod 7 = 3^{37} \bmod 7 = 3^{36}.3 \bmod 7 = 3$;
  - Tính $C^d \bmod 11 = 38^{37} \bmod 11 = 5^{37} \bmod 11 = 5^{30}.5^7 \bmod 11 = 3$;
  - Tính $a_1 = 11^{-1} \bmod 7 = 4^{-1} \bmod 7 = 2$;
  - Tính $a_2 = 7^{-1} \bmod 11 = 8$;
  - $c_1 = 11.(11^{-1} \bmod 7) = 11.2 = 22$;
  - $c_2 = 7(7^{-1} \bmod 11) = 7.8 = 56$;
- Vậy $M = (a_1c_1 + a_2c_2) \bmod 77 = (3.22 + 3.56) \bmod 77 = 3$.

5.3. Trao đổi khóa DIFFIE - HELLMAN

- Mọi người dùng thỏa thuận dùng tham số chung:
  - Lấy số nguyên tố rất lớn q;
  - Chọn α là căn nguyên thủy của q.
- Mỗi người dùng (A chẳng hạn) tạo khoá của mình:
  - Chọn một khoá mật (số) $x_A < q$;
  - Tính khoá công khai $y_A = \alpha^{x_A} \bmod q$
  - Mỗi người dùng thông báo công khai khóa của mình y_A
- Khóa bộ phận dùng chung cho hai người sử dụng A, B là K_{AB}
  - $K_{AB} = \alpha^{x_A.x_B} \bmod q$
    $= y_A^{x_B} \bmod q$ (mà B có thể tính)
    $= y_B^{x_A} \bmod q$ (mà A có thể tính)
- Hai người dùng A và B muốn trao đổi khoá phiên:
  - Đồng ý chọn số nguyên tố q = 11 và α = 2;
  - A chọn khoá riêng $x_A = 9$; B chọn khóa riêng $x_B = 3$;
  - Tính các khoá công khai:

$y_A = \alpha^{X_A} \bmod q = 2^9 \bmod 11 = 6$

$y_B = \alpha^{X_B} \bmod q = 2^3 \bmod 11 = 8$

- Tính khoá phiên chung:

$K_{AB} = y_B^{x_A} \bmod q = 8^9 \bmod 11 = 7$ (A)

$K_{AB} = y_A^{x_B} \bmod q = 6^3 \bmod 11 = 7$ (B)

- Hai người sử dụng A và B muốn trao đổi khoá phiên:
  - Đồng ý chọn số nguyên tố $q = 13$ và $\alpha = 6$
  - A chọn khoá riêng $x_A = 5$; B chọn khóa riêng $x_B = 7$
  - Tính các khoá công khai:

$y_A = \alpha^{X_A} \bmod q = 6^5 \bmod 13 = 2$

$y_B = \alpha^{X_B} \bmod q = 6^7 \bmod 13 = 7$

- Tính khoá phiên chung:

$K_{AB} = y_B^{x_A} \bmod q = 7^5 \bmod 13 = 11$ (A)

$K_{AB} = y_A^{x_B} \bmod q = 2^7 \bmod 13 = 11$ (B)

5.4. Chữ ký điện tử DSA

Bài tập:

- Chọn $p = 23$, $q = 11$, $h = 7$,

  chọn $g = h^{(p-1)/q} \pmod p$,

  ở đó $h < p-1$; $h^{(p-1)/q} \pmod p > 1$.

- $g = h^2 \bmod 23 = 3$
- Chọn $x = 4$, $y = 3^4 \bmod 23 = 12$.

Tạo chữ ký điện tử

- $k = 5$, $H(M) = 8$
- $r = (g^k \pmod p) \pmod q$

  $r = (3^5 \bmod 23) \bmod 11 = (12.3 \bmod 23) \bmod 11 = 2$
- $s = (k^{-1}(H(M) + x.r)) \pmod q$

  $s = (5^{-1}.(8 + 4.r)) \bmod 11 = (5^{-1}.(8 + 4.2)) \bmod 11 = 1$

- Chữ ký điện tử $(r,s) = (2,1)$

Kiểm tra chữ ký điện tử

$w = s^{-1} (\text{mod } q)$

$u_1 = (H(M).w) (\text{mod } q)$

$u_2 = (r.w) (\text{mod } q)$

$v = (g^{u_1}.y^{u_2} \ (\text{mod } p)) \ (\text{mod } q)$

- $w = 1^{-1} \text{ mod } 11 = 1$
- $u_1 = 8.1 \text{ mod } 11 = 8$
- $u_2 = 2.1 \text{ mod } 11 = 2$
- $v = \ (38.122 \text{ mod } 23) \ \text{ mod } 11 = 2$
- v = r, chữ ký điện tử đúng.

TÓM LƯỢC CUỐI BÀI

Với bài ứng dụng các thuật toán đã rèn luyện cho anh/chị kỹ năng về:

- Các thuật toán về số học:
  - Số học đồng dư;
  - Thuật toán Euclid và Euclid mở rộng;
  - Thuật toán bình phương và nhân liên tiếp;
  - Căn nguyên thủy và logarit rời rạc;
  - Hàm Euler và các định lý cơ bản về số học;
- Mã công khai RSA.
- Trao đổi khóa Diffie-Hellman.
- Chữ ký điện tử DSA.

CÂU HỎI TỰ LUẬN

1. Tại sao cần tập số hữu hạn, ở đó có thể cộng, trừ, nhân, chia cho số khác 0, để áp dụng vào mã công khai?

2. Khi thực hiện các phép toán đồng dư, có nhất thiết phải thực hiện trên các đại diện của nó không?

3. Nêu cách tính lũy thừa theo modulo bằng thuật toán bình phương và nhân liên tiếp.

4. Mô tả thuật toán Euclid mở rộng tìm số nghịch đảo theo modulo. Tại sao gọi là Euclid mở rộng?

5. Khi có số nguyên lớn có độ dài cỡ 500 bit, bạn dùng thuật toán nào để kiểm tra với xác suất tương đối lớn xem nó có phải là số nguyên tố không?

6. Muốn thực hiện nhanh phép tính theo modulo số lớn mà là tích của các số nguyên tố cùng nhau, thì ta có thể tính như thế nào?

7. Muốn kiểm tra 1 số có là căn nguyên thủy của một số khác không bạn làm gì?

8. Muốn tính logarit rời rạc cơ số a của một số b theo modulo p, bạn cần phải làm gì?

9. Mô tả ý tưởng dùng cặp bài toán thuận-dễ, nghịch-khó trong bài toán mã công khai.

10. Hay người sử dụng trao đổi khoá dùng thủ tục Diffie-Hellman có cần đến bên thứ 3 không? Hai người cùng tính được khóa mật dùng chung,1 người có thể tìm khóa riêng của người kia được không?

11. Bạn mô tả cách dùng bản băm để xác thực thông điệp.

12. Nêu các thao tác trong một vòng của SHA1.

13. Mô tả cách dùng và kiểm tra chữ ký điện tử RSA.

14. Mô tả cách dùng và kiểm tra chữ ký điện tử DSA.

15. Nêu các bối cảnh, người sử dụng dùng chữ ký điện tử.

BÀI TẬP TRẮC NGHIỆM

1. Cho P = (15 – 23) mod 52. Hỏi

(A) P = 43;
(B) P = 42;
(C) P = 44;
(D) P = 46.

2. Cho $Q = 23^{-1} \bmod 206$. Hỏi

(A) Q = 8;
(B) Q = 11;
(C) Q = 9;
(D) Q = 13.

3. Cho $Q = 25^{-1} \bmod 274$. Hỏi

(A) Q = 10;
(B) Q = 12;
(C) Q = 11;
(D) Q = 13.

4. Cho $Q = 3^{10} \bmod 16$. Hỏi

(A) Q = 8;
(B) Q = 11;
(C) Q = 7;
(D) Q = 9.

5. Cho X mod 25 = 5 và X mod 23 = 15 . Khi đó

(A) X mod 25.23= 80;
(B) X mod 25.23 = 130;
(C) X mod 25.23 = 105;
(D) X mod 25.23 = 155.

6. Tìm ra kết luận đúng về hàm Euler

(A) $\Phi(9) = 7$, $\Phi(17) = 16$, $\Phi(33) = 18$;
(B) $\Phi(9) = 6$, $\Phi(17) = 15$, $\Phi(33) = 20$;
(C) $\Phi(9) = 7$, $\Phi(17) = 15$, $\Phi(33) = 18$;
(D) $\Phi(9) = 6$, $\Phi(17) = 16$, $\Phi(33) = 20$.

7. Tìm ra kết luận đúng về hàm Euler:

(A) $\Phi(10) = 4$, $\Phi(23) = 20$, $\Phi(39) = 22$;
(B) $\Phi(10) = 5$, $\Phi(23) = 22$, $\Phi(39) = 23$;
(C) $\Phi(10) = 4$, $\Phi(23) = 22$, $\Phi(39) = 24$;
(D) $\Phi(10) = 6$, $\Phi(23) = 21$, $\Phi(39) = 25$.

8. Tìm ra kết luận sai:

(A) $2^6 \bmod 12 = 1$;
(B) $4^{12} \bmod 21 = 1$;
(C) $8^{12} \bmod 21 = 1$;
(D) $5^4 \bmod 12 = 1$.

9. Tìm ra kết luận sai:

(A) $2^6 \bmod 7 = 1$;
(B) $3^4 \bmod 5 = 1$;
(C) $2^5 \bmod 11 = 1$;
(D) $5^{10} \bmod 11 = 1$.

10. Tìm ra kết luận sai:

(A) 2 là căn nguyên của 3;
(B) 2 là căn nguyên của 4;
(C) 2 là căn nguyên của 5;
(D) 3 là căn nguyên của 5.

11. Tìm ra kết luận đúng:

(A) 2 là căn nguyên của 6;
(B) 2 là căn nguyên của 4;
(C) 2 là căn nguyên của 5;
(D) 3 là căn nguyên của 6.

12. Tìm kết luận đúng:

(A) $\text{Log}_2\ 5 \bmod 9 = 2$;
(B) $\text{Log}_2\ 6 \bmod 9 = 3$;
(C). $\text{Log}_2\ 7 \bmod 9 = 4$;
(D) $\text{Log}_2\ 4 \bmod 9 = 5$.

13. Cho p = 11; q = 13; A chọn khoá công khai 7, tính khóa riêng của A. Giả sử B sử dụng khoá công khai của A mã hoá bản tin M = 5. Tính bản mã và giải mã

(A) $P_{RA} = 23$; C = 37;
(B) $P_{RA} = 103$; C = 47;
(C) $P_{RA} = 53$; C = 27;
(D) $P_{RA} = 73$; C = 57.

14. Trao đổi khóa Diffie-Hellman: cho q = 17, α = 10, $x_A = 7$, $x_B = 5$. Tính y_A ; y_B và khoá chung K_{AB}.

(A) $y_A = 5$; $y_B = 4$; $K_{AB} = 11$;
(B) $y_A = 2$; $y_B = 7$; $K_{AB} = 9$;
(C) $y_A = 5$; $y_B = 11$; $K_{AB} = 14$;
(D) $y_A = 5$; $y_B = 6$; $K_{AB} = 15$.

15. Cho p = 47 và q = 23 và h = 7. Tính g. Bạn chọn khoá riêng x = 13, rồi tính khoá công khai y. Bạn gửi bức thư có bản băm H(M) = 11 và chọn một số ngẫu nhiên k = 5, rồi ký. Nêu cách người nhận kiểm tra chữ ký.

Sinh chữ ký

(A) g = 3, y = 15, r = 7, s = 13;
(B) g = 2, y = 20, r = 10, s = 11;
(C) g = 2, y = 20, r = 9, s = 15;
(D) g = 2, y = 20, r = 10, s = 19.

16. Kiểm tra chữ ký trong câu 15

(A) w = 17, u1 = 3, u2 = 7, v = 10;
(B) w = 15, u1 = 4, u2 = 9, v = 11;
(C) w = 17, u1 = 3, u2 = 9, v = 10;
(D) w = 17, u1 = 3, u2 = 8, v = 10.