CÂU HỎI VÀ BÀI TẬP CHƯƠNG III
Môn: MẬT MÃ VÀ AN NINH MẠNG
-o0o-

I. Câu hỏi

1. b là ước số của a có nghĩa là gì?
2. Số nguyên tố là gì?
3. Hàm phi Euler là gì?
4. Căn nguyên thủy của một số là gì?
5. Các yếu tố chủ yếu của một hệ mã khóa công khai là gì?
6. Bao nhiêu khóa là cần thiết để hai bên giao tiếp với nhau dùng mã hóa khóa công khai?
7. Hãy cho biết vai trò của khóa công khai và khóa riêng.
8. Trình bày ba loại ứng dụng của mã hóa khóa công khai.
9. Mô tả chung chung một thủ tục hiệu quả để chọn một số nguyên tố.
10. Mô tả ngắn gọn lược đồ trao đổi khóa Diffie-Hellman.

^1=7
^2=10
^3=5
^4=9
^5=11
^6=12
^7=6
^8=3
^9=8
^10=4
^11=2
^12=1

II. Câu hỏi trắc nghiệm

1. Hãy cho biết kết quả của (7^{2010} mod 13):

a. 1
b. 12

2010 % 12 = 8
=> 7^8 % 13

c. 7
d. Các giá trị trên đều sai

2. Cho biết giá trị hàm phi Euler ϕ(440) là:

a. 439
b. 240

440 = 2^3 * 5 * 11
=> (2-1) *2^(3-1) * (5-1) * (11-1)

c. 160
d. Tất cả các câu trên đều sai

3. Hãy cho biết kết quả của (3^{2086} mod 440):

a. 1 b. 3 c. 81 d. 289

4. Đối với mã hóa khóa công khai, khóa nào được sử dụng để tạo chữ ký số trên một thông điệp:

a. Khóa công khai của người nhận
b. Khóa riêng của người nhận
c. Khóa công khai của người gửi
d. Khóa riêng của người gửi

5. Đối với mã hóa khóa công khai, khóa nào được sử dụng để mã hóa một thông điệp:

a. Khóa công khai của người nhận
b. Khóa riêng của người nhận
c. Khóa công khai của người gửi
d. Khóa riêng của người gửi

n = p*q = 33
phi = (p-1)*(q-1) = 20
de % phi = 1 => d = 3

(Dữ liệu dùng cho câu 6 và 7)
Thực hiện mã hóa và giải mã với thuật toán RSA và p = 3; q = 11, e = 7; bản mã C = 5

6. Giá trị của d là:

a. 7 b. 5 c. 3 d. 2

7. Giá trị của bản rõ M tương ứng là: M = C^d % n

a. 26 b. 24 c. 5 d. 1

(Dữ liệu dùng cho câu 10, 11, 12)
A và B dùng kỹ thuật trao đổi khóa Diffie-Hellman với q = 71 và α = 7. Ya = a^Xa % q

8. Nếu A có khóa riêng X_A = 5, hãy cho biết khóa công khai của A (Y_A)?

a. 4 b. 5 c. 30 d. 51

9. Nếu B có khóa riêng X_B = 12, hãy cho biết khóa công khai của B (Y_B)? Yb = a^Xb % q

a. 4 b. 5 c. 30 d. 51

10. Nếu A có khóa riêng X_A = 5 và B có khóa riêng X_B = 12, hãy cho biết khóa bí mật dùng chung giữa A và B(K_{AB})? Kab = Yb ^ Xa % q

a. 4 b. 5 c. 30 d. 51

III. Bài tập

1. **Tìm các số nguyên dương x nhỏ nhất mà:**
   a. $5x \equiv 4 \pmod 3$
   b. $7x \equiv 6 \pmod 3$
   c. $9x \equiv 8 \pmod 3$

2. **Dùng thuật toán Euclid mở rộng tính nghịch đảo nhân của:**
   a. 1234 mod 4321
   b. 24140 mod 40902
   c. 550 mod 1769

3. **Dùng định lý Fermat tính 3^{201} mod 11.**

4. **Dùng định lý Euler tính 7^{1000} mod 10.**

5. **Tính các hàm phi Euler sau:**
   a. $\phi(41)$
   b. $\phi(27)$
   c. $\phi(231)$
   d. $\phi(440)$

6. **Dùng mã hóa RSA, cho biết bản mã C trong các trường hợp sau:**
   a. p = 3; q = 11, e = 7; M = 5
   b. p = 5; q = 11, e = 3; M = 9
   c. p = 7; q = 11, e = 17; M = 8
   d. p = 11; q = 13, e = 11; M = 7
   e. p = 17; q = 31, e = 7; M = 2.

7. **Với hệ mã khóa công khai RSA, bạn lấy được bản mã C = 10 gởi đến một người có khóa công khai (e,n) = (5, 35). Bản rõ M là gì ?**

8. **Xem xét lược đồ trao đổi khóa Diffie-Hellman với số nguyên tố q = 11 và $\alpha = 2$.**
   a. Chứng minh 2 là một căn nguyên thủy của 11.
   b. Nếu A có khóa công khai là $Y_A = 9$. Hãy cho biết khóa riêng của A(X_A)?
   c. Nếu B có khóa công khai là $Y_B = 3$. Hãy tính toán khóa bí mật dùng chung giữa A và B(K_{AB})?