Câu 1: Trong giải thuật RSA, để tạo khóa công khai, ta cần chọn hai số nguyên tố p và q. Nếu p = 3 và q = 5, thì n bằng bao nhiêu?

Giải: n = p* q = 3 * 5 = 15

Câu 2: Cho n =10000, a = 10023, b = 10004. Giá trị của biểu thức (a*b) mod n là bao nhiêu?

Giải: a *b mod n = 10023 * 10004 mod 10000 = 92

Câu 3: Trong hệ mật mã RSA, Alice chọn 2 số nguyên tố p =13, q =23. Hỏi Alice phải chọn e bằng bao nhiêu là hợp lệ?

Giải:

n = p * q = 13 * 23 = 299

ϕ(n) = 12 * 22 = 264

Chọn e = 5 vì e =5 nguyên tố cùng nhau với ϕ(n)

Câu 4: Trong hệ mật mã RSA, Alice chọn 2 số nguyên tố p =37, q =43. Hỏi Alice phải chọn e bằng bao nhiêu là hợp lệ?

n = p * q = 37 * 43 = 1591

ϕ(n) = 36 * 42 = 1512

Chọn e = 5 vì e =5 nguyên tố cùng nhau với ϕ(n)

Câu 5: Trong hệ RSA, Với n = 15 và Phi(n) = 8, giá trị e hợp lệ phải thỏa mãn điều kiện gì?

Giải: chọn e = 3 vì e = 3 nguyên tố cùng nhau với ϕ(n)

Câu 6: Trong RSA, để mã hóa thông điệp m ở chế độ bảo mật, ta sử dụng công thức nào?

Giải: C = M ^e mod n

Câu 7: Để giải mã bản mã c trong RSA hoạt động ở chế độ xác thực, ta sử dụng công thức nào?

Giải: M = C^d mod n

Câu 8: Trong hệ mật mã RSA hoạt động ở chế độ bảo mật, Với n = 21, e = 5, để mã hóa thông điệp m = 2, bản mã c sẽ là:

Giải: C = M ^e mod n = 2^5 mod 21 = 11

Câu 9: Trong hệ mật mã RSA hoạt động ở chế độ bảo mật, Alice chọn 2 số nguyên tố p =19, q =5 và e = 5. Bob muốn gửi cho Alice bản tin M = 15. Hỏi bản mã mà Alice gửi đến Bob là bao nhiêu?

Giải: n = p * q = 95

C = M ^e mod n = 15 ^5 mod 95 = 40

Câu 10: Trong hệ mật mã RSA hoạt động ở chế độ bảo mật, Alice chọn 2 số nguyên tố p =11, q =7 và e = 13. Bob muốn gửi cho Alice bản tin M = 25. Hỏi bản mã mà Alice gửi đến Bob là bao nhiêu?

Giải: n = p * q = 77

C = M ^e mod n = 25^13 mod 77 = 60

Câu 11: Trong hệ mật mã RSA, Alice chọn 2 số nguyên tố p =7, q =37 và e = 173. Bob chọn 2 số nguyên tố p =19, q =23 và e = 17. Hỏi khoá bí mật d của Alice và Bob tương ứng là bao nhiêu?

Giải:

Alice: n = 7 * 37 = 259

$\phi(n) = 6 * 36 = 216$

e.d đồng dư 1 mod $\phi(n)$ => d = 29

Bob: n = 19 * 23 = 437

$\phi(n) = 18 * 22 = 396$

e.d đồng dư 1 mod $\phi(n)$ => d = 233

Câu 12: Trong hệ mật mã RSA, Alice chọn 2 số nguyên tố p =3, q =29 và e = 3. Bob chọn 2 số nguyên tố p =11, q =13 và e = 23. Hỏi khoá bí mật d của Alice và Bob tương ứng là bao nhiêu?

Giải:

Alice: n = 3 * 29 = 87

$\phi(n) = 2 * 28 = 56$

e.d đồng dư 1 mod $\phi(n)$ => d = 19

Bob: n = 11 * 13 = 143

$\phi(n) = 10 * 12 = 120$

e.d đồng dư 1 mod $\phi(n)$ => d = 47

Câu 13: Trong hệ mật mã RSA, Alice chọn 2 số nguyên tố p =41, q =11 và e = 23. Bob chọn 2 số nguyên tố p =23, q =5 và e = 7. Hỏi khoá bí mật d của Alice và Bob tương ứng là bao nhiêu?

Khóa bí mật của Alice: d=87

Khóa bí mật của Bob: d=63

Câu 14: Trong hệ mật mã RSA, Alice chọn 2 số nguyên tố p =41, q =11 và e = 23. Bob chọn 2 số nguyên tố p =23, q =5 và e = 7. Alice muốn gửi cho Bob bản tin M=256 một cách bảo mật, bản mã tương ứng là bao nhiêu?

n(Bod) =115

C= me mod n = 71