1. Người A chọn các thông số p =37, q = 3, e = 31. Hỏi khóa riêng của A là gì theo thuật mã RSA?  
n = p\*q = 37\*3 = 111  
∅n = (37-1)(3-1)=72  
d = e^-1 (mod ∅n) = 7  
→ PR = {d, n} = {7, 111}  
  
•2. Người A chọn các thông số p =23, q =17, e = 39. Hỏi cặp khóa công khai, khóa riêng của A theo thuật mã RSA là gì ?  
n = p\*q = 23\*17 = 391  
∅n = (23-1)(17-1)=352  
d = e^-1 (mod ∅n) = 343  
→ PU = {39, 391}  
→ PR = {343, 391}  
  
•3. Cho bản rõ x = 18, khóa công khai n = 221, e = 47. Mã hóa với khóa trên theo hệ mã RSA, các em hãy tìm bản mã ?  
Để mã hóa ta cần tính được C = 1847mod 221  
18^47mod 221 = [(18^4mod 221)^11\*(18^2mod 221)\*(18^1mod 221)] mod 221  
18^1mod 221 = 18  
18^2mod 221 = 324 mod 221 =103  
18^4mod 221 = 104976 mod 221 =1  
→ C = 18^47 mod 221 = (1\*103\*18) mod 221 =1854 mod 221 =86  
  
•4. Người A chọn các thông số p =31, q =37, e = 397. Khi ta giải mã bản mã C = 509 theo thuật mã RSA ta sẽ thu được bản rõ nào ?  
n = p\*q = 31\*37 = 1147  
∅n =(31-1)(37-1)=1080  
d = e^-1 (mod ∅n) = 253  
Để giải mã ta cần tính được M = 509^253 mod 1147  
509^253 mod 1147 = [509 \* (509^126 mod 1147)^2] mod 1147  
509^126 mod 1147 = (509^63 mod 1147)^2 mod 1147  
509^63 mod 1147 = [509 \* (509^31 mod 1147)^2] mod 1147  
509^31 mod 1147 = [509 \* (509^15 mod 1147)^2] mod 1147  
509^15 mod 1147 = [509 \* (509^7 mod 1147)^2 ]mod 1147  
509^7 mod 1147 = [509 \* (509^3 mod 1147)^2] mod 1147  
509^3 mod 1147 = 492  
Tính ngược lên dần ta được M = 879  
  
•5. Theo thuật mã RSA. Giả sử người A chọn các thông số p =23, q =17, e = 13. Hỏi cặp khóa riêng, khóa công khai của A là gì?  
n = p\*q = 391  
∅n =(23-1)(17-1)=352  
d = e^-1 (mod ∅n) = 325  
PU = {13 , 391}  
PR = { 325 , 391 }  
  
•6. Tìm bản rõ của câu 5 với trường hợp chúng ta có kết quả bản mã y= 75 ?  
Để giải mã ta cần tính được M = 75^325 mod 391  
75^325 mod 391 = [75 \* (75^162 mod 391)^2] mod 391  
75^162 mod 391 = (75^81 mod 391)^2 mod 391  
75^81 mod 391 = [75 \* (75^40 mod 391)^2] mod 391  
75^40 mod 391 = (75^20 mod 391)^2 mod 391  
75^20 mod 391 = (75^10 mod 391)^2 mod 391  
75^10 mod 391 = (75^5 mod 391)^2 mod 391  
75^5 mod 391 = 232  
Tính ngược lên dần ta được M = 334  
  
•7. Giả sử rằng cho 2 người A,B chọn 2 số nguyên tố chung là g = 10 , p = 541, với a=5, b=7 . Tính khóa công khai, khóa riêng của người gửi và người nhận A,B theo thuật mã Diffie-Hellman ?  
A = 10^5 mod 541 = 456  
B = 10^7 mod 541 = 156  
A tính s = 156^5 mod 541 = 193  
B tính s = 456^7 mod 541 = 193  
->Khóa công khai của A là 456, của B là 156  
->Khóa bí mật: 193  
  
•8. Giả sử A,B chọn 2 số nguyên tố chung là g=2 , p = 997, a=11, b= 13. Tính khóa công khai, khóa riêng của người gửi và người nhận A, B theo thuật mã Diffie-Hellman?  
A = 2^11 mod 997 = 54  
B = 2^13 mod 997 = 216  
A tính s = 216^11 mod 997 = 113  
B tính s = 54^13 mod 997 = 113  
->Khóa công khai của A là 54, của B là 216  
->Khóa bí mật: 113  
  
•9 Cho A,B chọn 2 số nguyên tố chung là g=2 , p = 23, a=5, b= 13. Tính khóa công khai, khóa riêng của người gửi và người nhận A, B theo thuật mã Diffie-Hellman?  
A = 2^5 mod 23 = 9  
B = 2^13 mod 23 = 4  
A tính s = 4^5 mod 23 = 12  
B tính s = 9^13 mod 23 = 12  
->Khóa công khai của A là 9, của B là 4  
->Khóa bí mật: 12  
  
•10. Người A,B chọn 2 số nguyên tố chung là g=2 , p = 997, a=47, b= 43. Tính khóa công khai, khóa riêng của người gửi và người nhận A, B theo thuật mã Diffie-Hellman ?  
A = 2^47 mod 997 = 135  
B = 2^43 mod 997 = 320  
A tính s = 320^47 mod 997 = 370  
B tính s = 135^43 mod 997 = 370  
->Khóa công khai của A là 135, của B là 320  
->Khóa bí mật: 370