1. **隨意選兩個質數(選擇p=5, q=7)，以產生RSA公鑰與密鑰。 (e 必須與phi(n)互質且大於1小於phi(n))**n = 5x7 = 35  
   Ø(*n*) = 4x6 = 24  
   選e = 7與 Ø(*n*)互質  
   公鑰(e,n) = (7,35)  
   exd ≡ 1(mod Ø(*n*))  
   d = 7+24 = 31  
   密鑰(d,n) = (31,35)
2. **B. 隨意選兩個質數(選擇p=3, q=11)，以產生RSA公鑰與密鑰。 (e必須與phi(n)互質且大於1小於phi(n))**n = 3x11 = 33  
   Ø(*n*) = 2x10 = 20  
   選e = 9與 Ø(*n*)互質  
   公鑰(e,n) = (9,33)  
   exd ≡ 1(mod Ø(*n*))  
   d = 9+20 = 29  
   密鑰(d,n) = (29,33)

**C. 隨意選兩個質數(選擇p=3, q=7)，以產生RSA公鑰與密鑰。 (e必須與phi(n)互質且大於1小於phi(n))**n = 3x7 = 21  
Ø(*n*) = 2x6 = 12  
選e = 5與 Ø(*n*)互質  
公鑰(e,n) = (5,21)  
exd ≡ 1(mod Ø(*n*))  
d = 5+12 = 17  
密鑰(d,n) = (17,21)

**D. 隨意選兩個質數(選擇p=5, q=11)，以產生RSA公鑰與密鑰。 (e必須與phi(n)互質且大於1小於phi(n))**n = 5x11 = 55  
Ø(*n*) = 4x10 = 40  
選e = 9與 Ø(*n*)互質  
公鑰(e,n) = (9,55)  
exd ≡ 1(mod Ø(*n*))  
d = 9+40 = 49  
密鑰(d,n) = (49,55)

**E. 若(23, 143)為RSA公鑰，(47, 143)為RSA私鑰，若明文M=12，求以公鑰加密的密文C=?驗證你求出的密文以私鑰解密後得到明文12。**

加密:  
C = 12^23(mod 143)   
因為 12^2≡ 1 (mod 143)  
=> 12^23 ≡ 12^(2\*11+1) ≡ 12(mod 143)  
(by 費馬小定理)  
C = 12  
解密:  
M = 12^47(mod 143)  
因為 12^2≡ 1 (mod 143)  
=> 12^23 ≡ 12^(2\*23+1) ≡ 12(mod 143)

M = 12

**F. 若(23, 143)為RSA公鑰，(47, 143)為RSA私鑰，若明文M=34，求以公鑰加密的密文C=?驗證你求出的密文以私鑰解密後得到明文34。**34^23(mod 11) => Ø(*11*) = 10 => 34^10≡ 1 (mod 11)  
34^23 (mod 13) => Ø(13) = 12 => 34^12≡ 1 (mod 13)  
=> 34^(2\*10+3) ≡ 1(mod 11)、34^(12+11) ≡ 5(mod 13) (此用34r/13餘1 反推)  
by 中國餘式定理:  
13y1≡ 1(mod 11)、11y2≡ 1(mod 13) => (y1,y2) = (6,6)  
34^23≡13\*6\*1+11\*6\*5≡408≡122 (mod 143)  
驗證:

122^47(mod 11) => Ø(*11*) = 10 => 122^10≡ 1 (mod 11)  
122^47 (mod 13) => Ø(13) = 12 => 122^12≡ 1 (mod 13)  
=> 122^(4\*10+7) ≡ 1(mod 11)、122^(12\*3+11) ≡ 8(mod 13) (此用122r/13餘1 反推)  
by 中國餘式定理:  
13y1≡ 1(mod 11)、11y2≡ 1(mod 13) => (y1,y2) = (6,6)  
122^47≡13\*6\*1+11\*6\*8≡342≡34 (mod 143)

**G. 若(23, 143)為RSA公鑰，(47, 143)為RSA私鑰，若密文C=56，求以私鑰解密後得到明文M=?驗證你求出的明文以公鑰加密後得到密文56。**56^47(mod 11) => Ø(*11*) = 10 => 56^10≡ 1 (mod 11)  
56^47(mod 13) => Ø(13) = 12 => 56^12≡ 1 (mod 13)  
=> 56^(4\*10+7) ≡ 1(mod 11)、56^(3\*12+11) ≡ 10(mod 13) (此用56r/13餘1 反推)  
by 中國餘式定理:  
13y1≡ 1(mod 11)、11y2≡ 1(mod 13) => (y1,y2) = (6,6)  
56^47≡13\*6\*1+11\*6\*10≡738≡23 (mod 143)  
驗證:

23^23(mod 11) => Ø(*11*) = 10 => 56^10≡ 1 (mod 11)  
23^23 (mod 13) => Ø(13) = 12 => 56^12≡ 1 (mod 13)  
=> 23^(2\*10+3) ≡ 1(mod 11)、23^(12+11) ≡ 4(mod 13) (此用23r/13餘1 反推)  
by 中國餘式定理:  
13y1≡ 1(mod 11)、11y2≡ 1(mod 13) => (y1,y2) = (6,6)  
23^23≡13\*6\*1+11\*6\*4≡342≡56 (mod 143)

**H. 若(23, 143)為RSA公鑰，(47, 143)為RSA私鑰，若密文C=99，求以私鑰解密後得到明文M=?驗證你求出的明文以公鑰加密後得到密文99。**

99^47(mod 11) => Ø(*11*) = 10 => 99^10≡ 1 (mod 11)  
99^47(mod 13) => Ø(13) = 12 => 99^12≡ 1 (mod 13)  
=> 99^(4\*10+7) ≡ 0(mod 11)、99^(3\*12+11) ≡ 5(mod 13) (此用99r/13餘1 反推)  
by 中國餘式定理:  
13y1≡ 1(mod 11)、11y2≡ 1(mod 13) => (y1,y2) = (6,6)  
56^47≡13\*6\*0+11\*6\*5≡330≡44 (mod 143)  
驗證:

44^23(mod 11) => Ø(*11*) = 10 => 56^10≡ 1 (mod 11)  
44^23 (mod 13) => Ø(13) = 12 => 56^12≡ 1 (mod 13)  
=> 44^(2\*10+3) ≡ 0(mod 11)、44^(12+11) ≡ 8(mod 13) (此用44r/13餘1 反推)  
by 中國餘式定理:  
13y1≡ 1(mod 11)、11y2≡ 1(mod 13) => (y1,y2) = (6,6)  
44^23≡13\*6\*0+11\*6\*8≡342≡99(mod 143)

**I. 依據歐拉定理，求7^9999的個位數?**7互質 10 by 歐拉定理 Ø(*10*)=4 => 7^4 ≡ 1(mod 10)  
7^9999 ≡ 7^(4\*2499+3) ≡ 7^3 ≡ 3(mod 10)  
因此個位數為3

**J. 給定一0/1背包問題，其中背包容量W=10，三物品重量分別為10, 3, 5，而物品利潤分別為40, 20, 30，使用動態規劃法來解此0/1背包問題。(你必須列出表格的變化細節)  
1**: W:10 P:40 **2**.W:3 P:20 **3**.W:5 P:30

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 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 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 40 |
| 2 | 0 | 0 | 0 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 40 |
| 3 | 0 | 0 | 0 | 20 | 20 | 30 | 30 | 30 | 50 | 50 | 50 |

最大值:50

**K. 已知0/1背包問題是一個NPC問題，說明為何0/1背包問題也是一個弱NPC問題(weakly NPC problem)。**0/1背包問題時間複雜度為O(nW)  
input W為numeric value  
若 W改為 number of bits x  
時間複雜度變為: O(n2x)就變為指數時間  
因此0/1背包問題為偽多項式時間複雜度,且為NPC問題,因此為弱NPC問題  
\*每個演算法輸入定義都不同,若輸入為轉為bits也為多項式時間,才是真的多項式時間

**L. 以下為子集合加總(subset sum problem)問題的描述：給定一非零整數集合S以及一特定整數M，是否存在一個S的非空子集合其元素加總值等於M？例如，給定集合S={−7, −3, −2, 5, 8}及一特定整數0；或給定集合S={1,3, 4, 6, 8}及一特定 整數8。說明子集合加總問題可以變轉為0/1背包問題。  
輸入:**M為背包容量, 集合S為各物品價值和重量(意思是重量和價值相等)  
以集合S={1,3, 4, 6, 8}及一特定 整數8為例:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 0 | 1 | 1 | 3 | 4 | 4 | 4 | 4 | 4 |
| 3 | 0 | 1 | 1 | 3 | 4 | 5 | 5 | 7 | 8 |
| 4 | 0 | 1 | 1 | 3 | 4 | 5 | 6 | 7 | 8 |
| 5 | 0 | 1 | 1 | 3 | 4 | 5 | 6 | 7 | 8 |

**輸出:**若存在重量為8價值也為8，則代表存在非空子集合其元素加總值等於M  
參考: The subset sum problem is a special case of the decision and **0-1** problems where each kind of item, the weight equals the value: w_i=v_i (wiki knapsack problem)