Esercizio RSA

1. Scegli p tra 2, 3, 5 e q tra: 7, 11, 13
2. Calcola n = p q
3. Calcola m = mcm(p−1,q−1)
4. Scegli un intero c : $1 < c < m$ tale che
   $mcd(c,m) = 1$
5. Trova un intero d: $0 \leq d < m$ tale che
   $(cd) \bmod m = 1$
   Per trovare d devi risolvere l'equazione:
   $c\,d - k\,m = 1$ tramite l'algoritmo di Euclide.
6. Divulga n e c (la chiave pubblica), mentre tieni segreti p, q, m e d (la chiave privata)
7. Per mandare un intero $0 \leq a < n$ (ogni messaggio si può trasformare in questa forma, eventualmente frammentadolo) il mittente calcola $b = (a^c) \bmod n$ e manda b
8. Infine il destinatario calcola $(b^d) \bmod n$ (= a) .

p =	17	q =	11
n =	187		
p - 1 =	16	q - 1 =	10
m =	80		
c =	37		
d =	13		
CHIAVE PUBBLICA			
n =	187	c =	37
CHIAVE PRIVATA			
m =	80	d =	13