RSA

1. randomly choose two prime numbers p and q
p=11; q=13

2. compute n=pq
n=143

3. randomly choose an odd number e in the range 1<e<phi(n)
phi(n) is the totient function (number of positive integers <=n that are relatively prime to n)
relatively prime means they do not contain any common factors
1 is relatively prime to all numbers
phi(24)=8 since there are 8 totatives of 24: 1,5,7,11,13,17,19,23

phi(n)=phi(p)*phi(q)
phi(11)=10 (1,2,3,4,5,6,7,8,9,10)
phi(13)=12 (1,2,3,4,5,6,7,8,9,10,11,12)
phi(n)=10*12=120
1<e<120; we pick 7

4. compute d=e^-1 (mod phi(n)) by Euclid's algorithm
thus de=1 (mod phi(n))
d=7^-1 (mod phi(143))
d=7^-1 (mod 120)
d is the inverse of 7 (mod 120)
so 7d = 1 (mod 120)
so we can do euclidean's algorithm on 120 and 7 (we find that t=-17)
-17+120=103; so t=103

5. publish (n,e) as the public key; keep d as the secret ket
(143,7) is the public key
(143,103) is the secret key

\----------
encryption
E = encryption algorithm
A = user
m = message (0<=m<n_A)
c = ciphertext (0<=c<=n_A)
c = E_a(m) = m^(e_a) % n_A

encrypt m=3
c=m^(e_A) % n_A
c=3^7 % 143
c=2187 % 143
c=42

\----------
decryption

m = D_A(c) = c^(d_A) % n_A

decrypt c=42
m=c^(d_A) % n_A
m=42^103 % 143
too large so use: a = bc mod n = (b mod n)(c mod n) mod n
42^103 = 42^(2+2+...+2+1) (power of 2, 51 times)
m=([(42^2 % 143)^51]*42) % 143
m=3

==========

the euclidean algorithm gives us the gcd of 2 integers
we repeatedly divide the divisor by the remainder until the remainder is 0
gcd is the last non-zero remainder
gcd(81,57): 81 = 1(57) + 24
57 = 2(24) + 9
24 = 2(9) + 6
9 = 1(6) + 3
6 = 2(3) + 0
so gcd(81,57)=3

if gcd(a,b)=r then there exists integers s and t such that s(a)+t(b)=r
we can get s and t by reversing the steps of euclidean's algorithm
start with the non-0 remainder line and rewrite: 3 = 9 - 1(6)
substitute for 6 by using the line above that: 3 = 9 - 1(24 - 2(9)) = 3(9) - 1(24)
substitute for 9 by using the line above that: 3 = 3(57 - 2(24)) - 1(24) = 3(57) - 7(24)
substitute for 24 by using the line above that: 3 = 3(57) - 7(81 - 1(57)) = 10(57) - 7(81)
so s=-7 and t=10

find gcd(120,23): 120 = 5(23) + 5
23 = 4(5) + 3
5 = 1(3) + 2
3 = 1(2) + 1
2 = 2(1) + 0
so gcd(120,23)=1 (coprime)
now find s and t: 1 = 3 - 1(2)
1 = 3 - 1(5 - 1(3)) = 2(3) - 1(5)
1 = 2(23 - 4(5)) - 1(5) = 2(23) - 9(5)
1 = 2(23) - 9(120 - 5(23)) = 47(5) - 9(120)
so s=-9 and t=47

now we can say that: s is inverse of a (mod b)
as = 1 (mod b)
and: t is the inverse of b (mod a)
bt = 1 (mod a)