HOW RSA WORKS

- select two distinct large prime numbers p and q
- compute their product N = pq
- Let T =(p-1)(q-1) this is called euler totient
- Choose two integers where (e * d) mod T = 1
  Where e must be an odd number
- Now publish P=(e,N) which is the public key
- And the secret key S =(d,N)
- $C= M^e \bmod N$
  Where M is the encoded message,
  C is the encrypted message
- $M = C^d \bmod N$

For example:
Lets use primes 2 and 5
N= 2 * 5 = 10
To find T,
T = 1 * 4 = 4
Find 2 integers where e * d mod 4 = 1
e could be 3 and d could be 3
but we would use 7 .
3 * 7 mod 4 = 1 is true
N= 10, e = 3 , d = 7
Let A= 1 , B=2, C= 3
And lets make B our message
M = 2
Our public key is P=(3,10)
$C= M^e \bmod N$
$C = 2^3 \bmod 10$
C = 8
8 is our encrypted message
The secret key is S=(7,10)
$M = C^d \bmod N$
$M = 8^7 \bmod 10$
M = 2097152 mod 10
M = 2
The letter B