RSA encryption proof and explanation using math :

First we select 2 prime numbers to be p and q

$p = 11$ and $q = 17$

$n = p \times q$

$\therefore n = 11 \times 17 = 187$

$\varphi(n) = n - 1$ [Every number below a prime number ~~except itself~~ is coprime with the prime numbers]

$\varphi(n) = \varphi(p \times q)$

$= \varphi(p) \times \varphi(q)$

$= (p-1) \times (q-1) \quad \because \varphi(n) = n-1$

* φ means phi

in our case - $\varphi(n) = (11-1) \times (17-1)$

$= 160$

Calculating e :

$2 < e < \varphi(n)$ such that $\gcd(e, \varphi(n)) = 1$

in other words, the number must be coprime

In our case : $2 < e < 160$ such that $(e, 160) = 1$

$e = 7$ satisfies the conditions $\therefore e = 7$ is the public key

Calculating d :

Condition states that $(e \times d) = 1 \bmod \varphi(n)$

in other words $(e \times d) \% \varphi(n) == 1$

In our case : $(7 \times d) \% 160 == 1$

$d = 23$ satisfies the condition $\therefore d = 23$ is the private key.

Proof of encryption :

In order to encrypt : Use the formula $message^e \bmod n$ ((m**e)%.n where m is the message)

In order to decrypt : Use the formula $message^d \bmod n$ ((m**d)%.n where m is the ~~message~~ encrypted message)

Suppose we send the letter 'A', convert to ASCII value $\therefore A = 65$

Encrypted = $(65^7) \% 187 = 142 \quad \because e = 7$ and $n = 187$

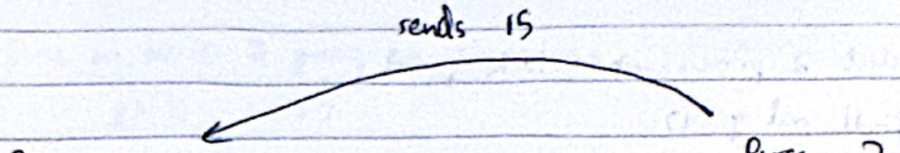
~~Decrypt~~ Decrypt = $(142^{23}) \% 187 = 65 \quad \because d = 23$ and $n = 187$

We get the original value of 65 back and $65 = A$

So 'A' is obtained after decrypting the ~~encrypted~~ encrypted message.

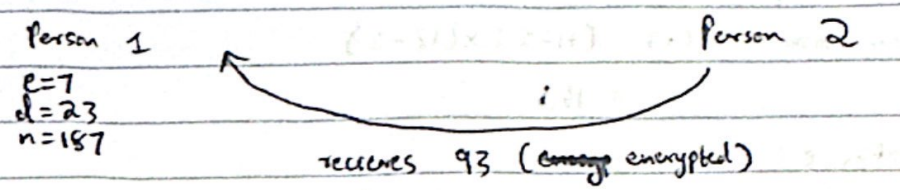
$\therefore$ RSA has been proved.

RSA Diagrammatic Explanation:

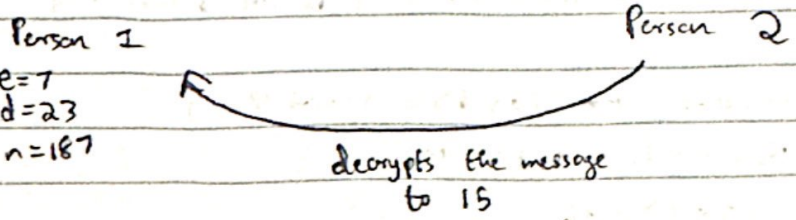


e = 7
d = 23
n = 187

When Person 2 sends 15
15 becomes $15^7 \% 187 = 93$



The received 93 is decrypted
93 becomes $93^{23} \% 187 = 15$



Process Complete. This would work both ways.
Each person would have their own e, d and n values.
In our case, we only did the calculation for person 1.

* Note that in computers, much larger values are used in the RSA algorithm.