# RSA_A_Working_Example

September 27, 2020

1. Choose two random prime numbers.

[1]:
```
p = 61; q = 53;
```

2. Calculate their product.

[2]:
```
n = p * q;
```

3. Compute the totient.

[3]:
```
phi_n = (p - 1) * (q - 1);
```

4. Choose a number $e$ satisfying $1 < e < \phi(n)$ and $e$ is coprime to $\phi(n)$.

[4]:
```
e = 17;
```

5. Choose a number $d$ satisfying $de \equiv 1 \ (mod \ \phi(n))$.

[5]:
```
d = 2753; out = (d * e) % phi_n;
```

The expected value for `out` is 1. The calculated value for `out` as above is {{out}}.

The **public key** is n = {{n}}, e = {{e}}.

The procedure to encode a certain piece of message $m$ becomes,

$c = m^{17} \ mod \ 3233$.

The **private key** is n = {{n}}, d = {{d}}.

The procedure to decode a certain piece of encoded message $c$ becomes,

$m = c^{2753} \ mod \ 3233$.

[6]:
```
m = 123; c = m**e % n; print(c)
```

```
855
```

For example, if the message to send is $m = 123$, the encoded message $c$ is calculated, as shown above, to be,

$c = 123^{17} \ mod \ 3233 = 855$

[7]:
```
m = c**d % n; print(m)
```

```
123
```

To decode the message, we calculate $m = 855^{2753}$ $mod$ 3233, which gives, as shown above, m = 123.