Objective: apply RSA encryption and decryption

we will try to encrypt and decrypt a simple message.

Public Key Creation:

Let's choose two primes as follows,

$$\begin{aligned}&p = 11 \ , q = 13. \Rightarrow \\ &N = p \times q = 11 \times 13 = 143 \\ &(p-1) = 10 \ , (q-1) = 12\end{aligned}$$

Now, we need to create the public key, $\boldsymbol{e}$. Since e is `relatively prime` to $(p-1)(q-1)$, we try from $\mathbf{3, 5, \ldots}$ until we find the first such number. In this case, $\mathbf{7}$ is relatively prime to $\mathbf{120}$, so we choose that.

$$e = 7 \tag{1}$$

Based on this, we have the public key as,

$$\text{public key} = (e, N) = (7, 143) \tag{2}$$

Private Key:

This is simply the inverse of $e \bmod (p-1)(q-1)$ and is computed using `extended Euclid's algorithm` as follows,

$$\begin{aligned}&(120, 7) \Rightarrow \\ &\text{We repeatedly take } (x, y) \rightarrow (y, x \mod y) \rightarrow \ldots \text{ until we reach y} = 0 \\ &(120, 7) = \\ &(7, 1) = \\ &(1, 0) = \\ &\text{ Now we climb up from the bottom returning appropriate values of (x,y,d),} \\ &\text{ where x is the coefficient of a, first number \& y is the co-efficient of b, second num} \\ &\text{ the values are returned as } (y', x' - \lfloor a/b \rfloor . y', d), where \\ &\text{ a=first number, b=second number, x',y'=previous iteration co-efficients} \\ &\text{ on the last step, the values returned are, } (x', y', d) = (1, 0, 1) \\ &(1, 0) = 1, 0, 1 \\ &(7, 1) = (0, 1, 1) \\ &(120, 7) = (1, -17, 1) \\ &\text{ Therefore, } d = ax + by \\ &1 = 120.x + 7.y \\ &\text{ y is the inverse of 7 mod (p-1)(q-1) or 120 is ,} \\ &y = -17 \\ &\text{ Now, we need to convert this to a non-negative number,} \\ &\text{ by adding 120 till we reach non-negative} \\ &y = 120 - 17 = 103\end{aligned}$$

Hence, the private key is,

$$\text{private key, } d = 103 \tag{3}$$

Message:

Let's choose a simple message,

$$m = \mathbf{41} \tag{4}$$

Encryption:

In order to encrypt, we `raise the message to the power of` **e** and take `mod N` of that.

$$\begin{array}{l} y = \text{encrypted message} \\ = m^e \mod N \\ = 41^7 \mod 143 \end{array}$$

This is computed using `fast modular exponentiation`. Writing $\mathbf{7}$ in binary, we have $\mathbf{111}$

We can express the power $\mathbf{7}$ as $\mathbf{4+2+1}$.

Therefore, using the modular exponentiation, we compute the powers up to 4, giving us the final answer.

$$\begin{array}{l} x = 41 \mod 143 = 41 \\ x^2 = 41 \times 41 \mod 143 = 108 \\ x^4 = x^{2^2} = 108 \times 108 \mod 143 \\ \text{Simplifying,} \\ = \underline{54 \times 54} \times \underline{2 \times 2} \mod 143 \\ = 56 \times 4 \mod 143 \text{ , 'cause 54 x 54 mod 143} = \text{56 mod 143} \\ = 81 \\ \text{Therefore, } x^4 = 81 \text{ , } x^2 = 108 \text{ , } x = 41 \\ x^7 \mod 143 \\ = (81 \times 108 \times 41) \mod 143 \\ = \underline{9 \times 9} \times \underline{54 \times 2} \times 41 \\ = \underline{54 \times 9} \times \underline{41 \times 9} \times 2 \\ \text{Now taking mod with 143} \\ = 57 \times 83 \times 2 \\ = 23 \times 57 \\ = 24 \end{array}$$

Hence, the encrypted message is,

$$y = e(m) = \mathbf{24} \tag{5}$$

Decryption:

To decrypt, we raise the encrypted message to the power of d and take $\mod N$

```
\begin{array}{0}
y^d\mod N\\
= (24) ^{103} \mod 143\\
\end{array}
```

Preview

OK

$$\begin{array}{l} y^d \mod N \\ = (24)^{103} \mod 143 \end{array}$$

Now, we can raise this number to $\mathbf{103}$ using fast modular exponentiation,

Now, $\mathbf{103}$ is 1100111 in binary. Therefore, we can express the power of 103 as,

$x^{103} = x^{64}.\, x^{32}.\, x^{4}.\, x^{2}.\, x$

Therefore, we need to compute up to $\mathbf{64^{th}}$ power.

$$
\begin{aligned}
&x = 24 \mod 143 = \mathbf{24} \\
&x^2 \\
&= 24 \times 24 \mod 143 \\
&= 12 \times 2 \times 12 \times 2 \mod 143 \\
&= \underline{12 \times 12} \times \underline{2 \times 2} \mod 143 \\
&= 1 \times 4 \mod 143 \\
&x^2 = \mathbf{4} \\
\\
&x^4 = x^2 = 4^2 \mod 143 = \mathbf{16} \\
&x^8 = (x^4)^2 = 16^2 \mod 143 = 113 \\
\\
&x^{16} = 113^2 \mod 143 = 42 \\
\\
&x^{32} = 42 \times 42 \mod 143 = \mathbf{48} \\
\\
&x^{64} = 48 \times 48 \mod 143 = \mathbf{16}
\end{aligned}
$$

Therefore, $\mathbf{103^{rd}}$ power is as follows,

$$
\begin{aligned}
&y^{103} \mod N \\
&= 24^{103} \mod 143 \\
&= (16 \times 48 \times 16 \times 4 \times 24) \mod 143 \\
&= \underline{48 \times 4} \times \underline{16 \times 16} \times 24 \mod 143 \\
&= 192 \times 113 \times 24 \mod 143 \\
&= 49 \times 113 \times 12 \times 2 \mod 143 \\
&= \underline{113 \times 2} \times \underline{49 \times 12} \mod 143 \\
&= 83 \times 16 \mod 143 \\
&= \underline{83 \times 2} \times 8 \mod 143 \\
&= 23 \times 8 \mod 143 \\
&= 184 \mod 143 \\
&= \mathbf{41}
\end{aligned}
$$

Therefore,

$$\text{decrypted message}, m = \mathbf{41} \tag{6}$$