Qu. Perform encryption and decryption using the RSA algorithm for the following:

1. p=3; q=11; e=7; M=5

Answer:

n = p * q = 3 * 11 = 33

f(n) = (p-1) * (q-1) = 2 * 10 = 20

Now, we need to compute $d = e^{-1} \bmod f(n)$ by using backward substitution of GCD algorithm:

According to GCD:

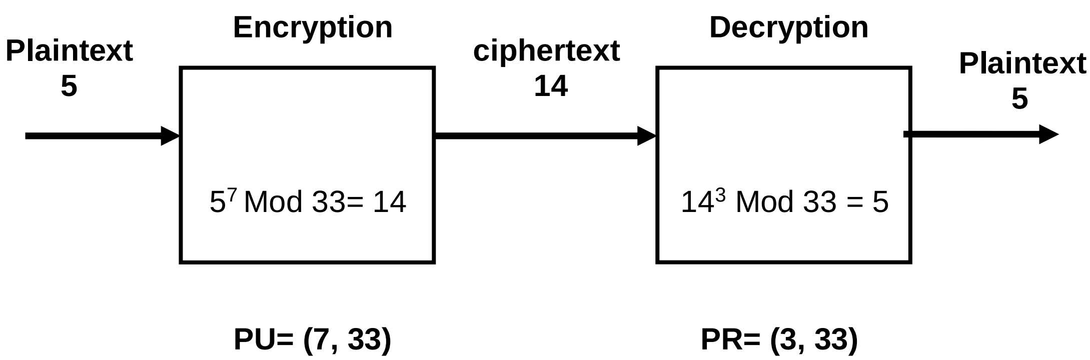
$$20 = 7 * 2 + 6$$
$$7 = 6 * 1 + 1$$
$$6 = 1 * 6 + 0$$

Therefore, we have:

$$\begin{aligned} 1 &= 7 - 6 \\ &= 7 - (20 - 7 * 2) \\ &= 7 - 20 + 7 * 2 \\ &= -20 + 7 * 3 \end{aligned}$$

Hence, we get $d = e^{-1} \bmod f(n) = e^{-1} \bmod 20 = 3 \bmod 30 = 3$

So, the public key is {7, 33} and the private key is {3, 33}, RSA encryption and decryption is following:



2. p=5; q=11; e=3; M=9

Answer:

n = p * q = 5 * 11 = 55

f(n) = (p-1) * (q-1) = 4 * 10 = 40

Now, we need to compute $d = e^{-1} \bmod f(n)$ by using backward substitution of GCD algorithm:

According to GCD:

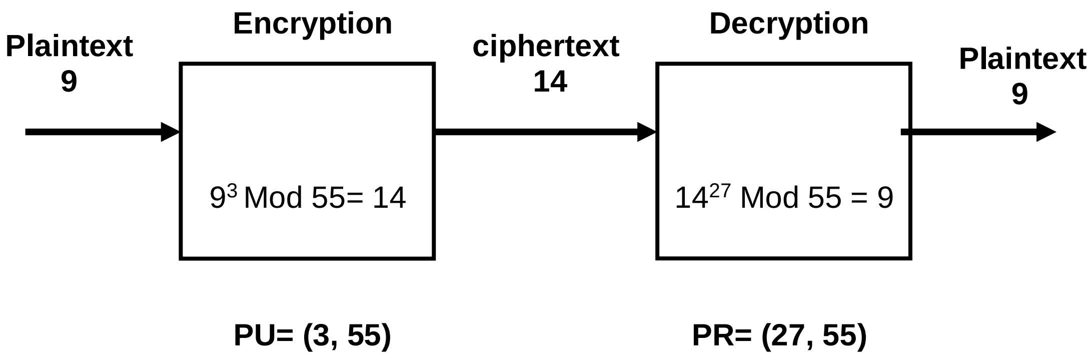
$$40 = 3 * 13 + 1$$
$$13 = 1 * 13 + 0$$

Therefore, we have:

$$1 = 40 - 3 * 13$$

Hence, we get $d = e^{-1} \bmod f(n) = e^{-1} \bmod 40 = -13 \bmod 40 = (27 - 40) \bmod 40 = 27$

So, the public key is {3, 55} and the private key is {27, 55}, RSA encryption and decryption is following:



3. p=7; q=11; e=17; M=8

Answer:

n = p * q = 7 * 11 = 77

f(n) = (p-1) * (q-1) = 6 * 10 = 60

Now, we need to compute d = e^{-1} mod f(n) by using backward substitution of GCD algorithm:

According to GCD:

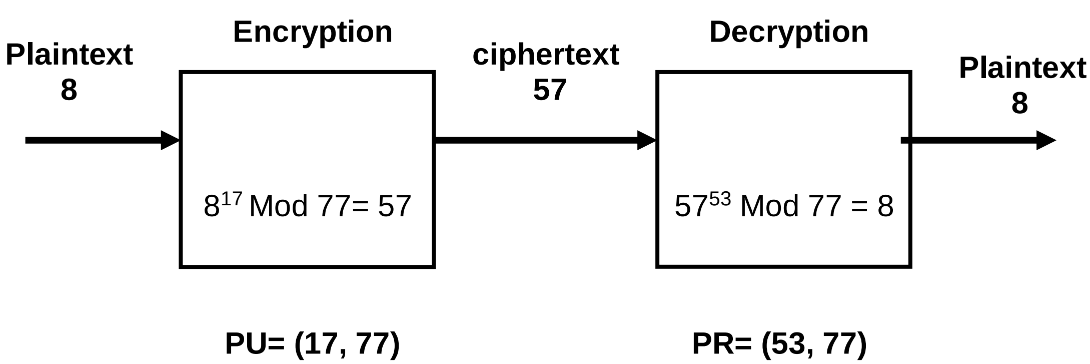
$$
\begin{aligned}
60 &= 17 * 3 + 9 \\
17 &= 9 * 1 + 8 \\
9 &= 8 * 1 + 1 \\
8 &= 1 * 8 + 0
\end{aligned}
$$

Therefore, we have:

$$
\begin{aligned}
1 &= 9 – 8 \\
&= 9 – (17 – 9) \\
&= 9 – (17 – (60 – 17 * 3)) \\
&= 60 – 17*3 – (17 – 60 + 17*3) \\
&= 60 – 17 *3 + 60 – 17*4 \\
&= 60*2 – 17*7
\end{aligned}
$$

Hence, we get d = e^{-1} mod f(n) = e^{-1} mod 60 = -7 mod 60 = (53-60) mod 60 = 53

So, the public key is {17, 77} and the private key is {53, 77}, RSA encryption and decryption is following:



4. p=11; q=13; e=11; M=7

Answer:

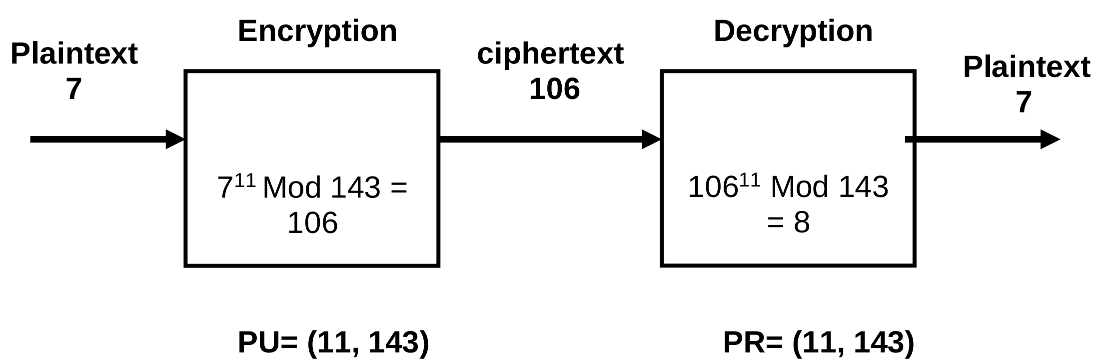
$n = p * q = 11 * 13 = 143$
$f(n) = (p-1) * (q-1) = 10 * 12 = 120$
Now, we need to compute $d = e^{-1} \bmod f(n)$ by using backward substitution of GCD algorithm:
According to GCD:

$$120 = 11 * 10 + 10$$
$$11 = 10 * 1 + 1$$
$$10 = 1 * 10 + 0$$

Therefore, we have:

$$\begin{aligned} 1 &= 11 - 10 \\ &= 11 - (120 - 11 * 10) \\ &= 11 - 120 + 11 * 10 \\ &= -120 + 11 * 11 \end{aligned}$$

Hence, we get $d = e^{-1} \bmod f(n) = e^{-1} \bmod 120 = 11 \bmod 120 = 11$
So, the public key is {11, 143} and the private key is {11, 143}, RSA encryption and decryption is following:



5. p=17; q=31; e=7; M=2
$n = p * q = 17 * 31 = 527$
$f(n) = (p-1) * (q-1) = 16 * 30 = 480$
Now, we need to compute $d = e^{-1} \bmod f(n)$ by using backward substitution of GCD algorithm:
According to GCD:

$$480 = 7 * 68 + 4$$
$$7 = 4 * 1 + 3$$
$$4 = 3 * 1 + 1$$
$$3 = 1 * 3 + 0$$

Therefore, we have:

$$\begin{aligned} 1 &= 4 - 3 \\ &= 4 - (7 - 4) \\ &= 4 - (7 - (480 - 7*68)) \\ &= 4 - (7 - 480 + 7*68) \\ &= 480 - 7*68 - 7 + 480 - 7*68 \\ &= 480*2 - 7*137 \end{aligned}$$

Hence, we get d = e^{-1} mod f(n) = e^{-1} mod 480 = -137 mod 480 = (343 – 480) mod 480 =343

So, the public key is {7, 527} and the private key is {343, 527}, RSA encryption and decryption is following: