$p = 11$

$q = 5$ $\rightarrow n = 55$ | Chosen 2 primes

$k = 4$ | Random

$$\varphi = (p-1)(q-1)$$
$$= (11-1)(5-1)$$
$$= 40$$

$$(k \cdot \varphi + 1) \bmod e = 0 \Leftrightarrow (k \cdot 40 + 1) \bmod 7 = 0 \Leftrightarrow k = 4$$ | Start with k=1, then iterate until condition true

$$d = \frac{k \cdot \varphi + 1}{e} = \frac{4 \cdot 40 + 1}{7} = 23$$

→ Private key $(d, n) = (23, 55)$

Public key $(e, n) = (7, 55)$

$m = 42$

Encrypt: $c = m^e \bmod n = 42^7 \bmod 55 = 48$

Decrypt: $m = c^d \bmod n = 48^{23} \bmod 55 = 42$

$$\left.\begin{matrix} p = 89 \\ q = 107 \end{matrix}\right\rangle n = 9523$$ | Chosen 2 primes

$$\varphi = (p-1)(q-1)$$

$$= (89-1)(107-1) = 9328$$

$$(k \cdot \varphi + 1) \bmod e = 0 \iff (k \cdot 9328 + 1) \bmod 3 = 0 \iff k = 2$$ | Start with k=1, then iterate until condition true

$$d = \frac{k \cdot \varphi + 1}{e} = \frac{2 \cdot 9328 + 1}{3} = 6219$$

→ Private key $(d, n) = (6219 . 9523)$

Public key $(e, n) = (3, 9523)$

$m = 42$

Encrypt: $c = m^e \bmod n = 42^3 \bmod 9523 = 7427$

Decrypt: $m = c^d \bmod n = 7427^{6219} \bmod 9523 = 42$

$p = 151$

$q = 157$ — $n = 23\,707$ | Chosen 2 primes

$$\varphi = (p-1)(q-1)$$
$$= (151-1)(157-1)$$
$$= 23\,400$$

$$\varphi \bmod e \neq 0 \Leftrightarrow e = 7$$

$$(k \cdot \varphi + 1) \bmod e = 0 \Leftrightarrow (k \cdot 23400 + 1) \bmod 7 = 0 \Leftrightarrow k = 8$$ | Start with k = 1, then iterate until condition true

$$d = \frac{k \cdot \varphi + 1}{e} = \frac{8 \cdot 23400 + 1}{7} = 26743$$

Private key $(d, n) = (26\,743,\ 23\,707)$

Public key $(e, n) = (7, 23\,707)$

$m = 18537$

Encrypt: $c = m^e \bmod n = 18537^7 \bmod 23\,707 = 10850$

Decrypt: $m = c^d \bmod n = 10850^{26\,743} \bmod 23\,707 = 18537$

$$\left.\begin{aligned} p &= 151 \\ q &= 157 \end{aligned}\right\} n = 23707$$

Chosen 2 primes

$$\begin{aligned} \varphi &= (p-1)\cdot(q-1) \\ &= (151-1)\cdot(157-1) \\ &= 23\,400 \end{aligned}$$

$\varphi \bmod e \neq 0 \Leftrightarrow 23400 \bmod e \neq 0 \Leftrightarrow e = 7$

$(k \cdot \varphi + 1) \bmod e = 0 \Leftrightarrow (k \cdot 23400 + 1) \bmod 7 = 0 \Rightarrow k = 1$

$$d = \frac{k \cdot \varphi + 1}{e} = \frac{1 \cdot 23400 + 1}{7} = 3343$$

Private key $(d, n) = (3343, 23707)$

Public key $(e, n) = (7, 23707)$

$m = 1337$

Encrypted: $c = m^e \bmod n = 1337^7 \bmod 23707 = 21078$

Decrypted: $m = c^d \bmod n = 21078^{3343} \bmod 23707 = 1337$

Private key $(d, n) = (3343, 23707)$

Public key $(e, n) = (7, 23707)$

$m = $ "RS"

$R = 82_{(10)} = 0101\ 0010$

$S = 83_{(10)} = 0101\ 0011$

$0101\ 0010\ 0101\ 0011_{(2)} = 21075 = m_{Raw}$

Encrypt: $c = m_{Raw}^{e} \bmod n = 21075^{7} \bmod 23707 = 23046$

Decrypt: $m_{Raw} = c^{d} \bmod n = 23046^{3343} \bmod 23707 = 21075_{(10)}$

$= 0101\ 0010 \rightarrow 82_{(10)} = R$

$ 0101\ 0011_{(2)} \rightarrow 83_{(10)} = S$ → "RS"

$$\left.\begin{array}{l} p = 43 \\ q = 29 \end{array}\right\} n = 1247$$

$$\varphi = (p-1)\cdot(q-1)$$
$$= (43-1)\cdot(29-1)$$
$$= 1176$$

$$\varphi \bmod e \neq 0 \iff 1176 \bmod e \neq 0 \iff e = 5$$

$$(k\cdot\varphi+1) \bmod e = 0 \iff (k\cdot 1176+1) \bmod 5 = 0 \iff k = 4$$

$$d = \frac{k\cdot\varphi+1}{e} = \frac{4\cdot 1176+1}{5} = 941$$

Private key $(d,n) = (941, 1247)$

Public key $(e,n) = (5, 1247)$

$m = 22$

Encrypt: $c = m^e \bmod n = 22^5 \bmod 1247 = 1028$

Decrypt: $m = c^d \bmod n = 1028^{941} \bmod 1247 = 22$

$$\left.\begin{array}{l} p = 173 \\ q = 227 \end{array}\right\rangle n = 39271$$

$$\varphi = (p-1)(q-1)$$
$$= (173-1)(227-1)$$
$$= 38\,872$$

$$\varphi \bmod e \neq 0 \iff 38872 \bmod e \neq 0 \iff e = 3$$

$$(k \cdot \varphi + 1) \bmod e = 0 \iff (k \cdot 38872 + 1) \bmod 3 = 0 \iff k = 2$$

$$d = \frac{k \cdot \varphi + 1}{e} = \frac{2 \cdot 38872 + 1}{3} = 25\,915$$

Private key $(d, n) = (25\,915, 39271)$

Public key $(e, n) = (3, 39271)$

$m = 42$

Encrypted: $c = m^e \bmod n = 42^3 \bmod 39271 = 34\,817$

Decrypted: $m = c^d \bmod n = 34\,817^{25\,915} \bmod 39271 = 42$

$$\left.\begin{array}{l} p = 73 \\ q = 157 \end{array}\right\rangle n = 11\,461$$

$$\begin{aligned} \varphi &= (p-1)\cdot(q-1) \\ &= (73-1)\cdot(157-1) \\ &= 11\,232 \end{aligned}$$

$$\varphi \bmod e \neq 0 \Leftrightarrow 11\,232 \bmod e \neq 0 \Leftrightarrow e = 5$$

$$(k\cdot\varphi+1) \bmod e = 0 \Leftrightarrow (k\cdot 11\,232+1) \bmod 5 = 0 \Leftrightarrow k = 2$$

$$d = \frac{k\cdot\varphi+1}{e} = \frac{2\cdot 11\,232+1}{5} = 4493$$

Private key $(d,n) = (4493, 11\,461)$

Public key $(e,n) = (5, 11\,461)$

$m = 69$

Encrypt: $c = m^e \bmod n = 69^5 \bmod 11\,461 = 5984$

Decrypt: $m = c^d \bmod n = 5984^{4493} \bmod 11\,461 = 69$