Aufgabe 1

zu (i) Wir zeigen zuerst $\varphi(n) \leq n-1$ für bel. $n > 1$
Für $n > 1$ kann n nicht zu sich selbst teilerfremd sein (denn $ggT(n,n) = n > 1$). Also $\varphi(n) \leq n-1$
Bleibt zu zeigen: $\varphi(p) = p-1 \iff p$ Primzahl

"$\Rightarrow$" $\varphi(p) = p-1$ heißt gerade, dass alle Zahlen die kleiner als p sind, zu p teilerfremd sein müssen. Also muss p eine Primzahl sein (per Definition von Primzahlen).

"$\Leftarrow$" Ist p eine Primzahl, dann sind (per Definition von Primzahlen) alle Zahlen die kleiner als p sind, zu p teilerfremd. Also $\varphi(p) = p-1$

zu (ii) Für eine Primzahlpotenz p^r und k mit $1 \leq k \leq p^r$ ist $ggT(k, p^r) > 1$ genau dann, wenn k ein Vielfaches von p ist. Die ganzzahligen Vielfachen von p im Intervall $[1, p^r]$ sind gerade die p^{r-1} Zahlen

$$p,\ 2p,\ 3p,\ \dots,\ (p^{r-1}-1)p,\ p^{r-1} \cdot p$$

Also folgt $\varphi(p^r) = p^r - p^{r-1} = p^r\left(1 - \frac{1}{p}\right)$

zu (iii) Nach dem Hauptsatz der elementaren Zahlentheorie lässt sich jede natürliche Zahl (bis auf die Reihenfolge der Faktoren) eindeutig als ein Produkt von Primzahlen darstellen. Also $n = p_1^{r_1} \cdots p_k^{r_k}$ für Primzahlen $p_1, \dots, p_r$ und $r_1, \dots, r_k \geq 1$. Mittels Multiplikativität folgt

$$\varphi(n) = \prod_{i=1}^{k} \varphi(p_i^{r_i}) \overset{(ii)}{=} \prod_{i=1}^{k} p_i^{r_i}\left(1 - \frac{1}{p_i}\right)$$

$$= \prod_{i=1}^{k} p_i^{r_i} \prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right) = n \prod_{p \mid n}\left(1 - \frac{1}{p}\right)$$

Aufgabe 2

Mit $p = 61$, $q = 97$ folgt $n = pq = 5917$
und $\varphi(n) = (p-1)(q-1) = 60 \cdot 96 = 5760$
Wir prüfen die Bedingung $ggT(e, \varphi(n)) = 1$
mittels euklidischem Algorithmus ($e = 47$):

$$5760 = 122 \cdot 47 + 26$$
$$47 = 1 \cdot 26 + 21$$
$$26 = 1 \cdot 21 + 5$$
$$21 = 4 \cdot 5 + 1$$

Also $ggT(5760, 47) = 1$ und die Bedingung ist erfüllt. Als nächstes bestimmen wir d mit $ed \equiv 1 \mod (p-1)(q-1)$, also das multiplikativ Inverse zu $e = 47$, durch den erweiterten euklidischen Algorithmus:

$$\begin{aligned} 1 &= 21 - 4 \cdot 5 \\ &= 21 - 4(26 - 21) = 5 \cdot 21 - 4 \cdot 26 \\ &= 5(47 - 26) - 4 \cdot 26 = 5 \cdot 47 - 9 \cdot 26 \\ &= 5 \cdot 47 - 9(5760 - 122 \cdot 47) \\ &= 1103 \cdot 47 - 9 \cdot 5760 \end{aligned}$$

Also $d = 47^{-1} \mod 5760 = 1103$
Damit sind der öffentliche Schlüssel

$$(e, n) = (47, 5917)$$

und der private Schlüssel

$$(d, n) = (1103, 5917)$$

gegeben.

Wir verschlüsseln nun die Nachricht $m = 348$

$$c = m^e \pmod n = 348^{47} \pmod{5917}$$
$$= 348^{32+8+4+2+1} \pmod{5917}$$
$$= 348^{32}\, 348^{8}\, 348^{4}\, 348^{2}\, 348 \pmod{5917}$$

Als Nebenrechnung

$348^2 \equiv 121.104 \equiv 2764 \pmod{5917}$

$348^4 \equiv 2764^2 = 7.639.696 \equiv 849 \pmod{5917}$

$348^8 \equiv 849^2 \equiv 720.801 \equiv 4844 \pmod{5917}$

$348^{16} \equiv 4844^2 \equiv 23.464.336 \equiv 3431 \pmod{5917}$

$348^{32} \equiv 3431^2 \equiv 11.771.761 \equiv 2848 \pmod{5917}$

Also

$$c = 2848 \cdot 4844 \cdot 849 \cdot 2764 \cdot 348 \pmod{5917}$$
$$= 13.795.712 \cdot 2.346.636 \cdot 348 \pmod{5917}$$
$$= 3185 \cdot 3504 \cdot 348 \pmod{5917}$$
$$= 11.160.240 \cdot 348 \pmod{5917}$$
$$= 778 \cdot 348 \pmod{5917}$$
$$= 270.744 \pmod{5917}$$
$$= 4479$$