Aufgabe 3

a)

Gegeben sind folgende Primzahlen:
p = 23
q = 7

1. Modul n berechnen

n = p * q
n = 23 * 7
n = 161

2. Eulersche Funktion + Bedingung

$\varphi(n)=(p-1)(q-1)$
$\varphi(n)= (23 - 1) * (7 - 1)$
$\varphi(n) = 132$

Bedingung:

$1 < e < \varphi(n)$ & $ggT(e, \varphi(n)) = 1$

Der ggT zweier Zahlen wird mit dem euklidischen Algorithmus berechnet

Wir prüfen für e = 5 bei $\varphi(n) = 132$

1. Schritt 132 : 5 = 26 Rest 2
2. Schritt 5 : 2 = 2 Rest 1
3. Schritt 2 : 1 = 2 Rest 0

Da der letzte nicht-Null-Rest 1 ist, handelt es sich bei der 5 um die gesuchte Zahl e.
Der öffentliche Schlüssel lautet somit
(5, 161)

Jetzt muss der private Schlüssel d mit Hilfe des euklidischen Algorithmus berechnet werden.

Es gilt:
$1 < d < \varphi(n)$ & $d \cdot e \equiv 1 \mod \varphi(n)$

Wir wissen bislang, dass ein Inverses von 5 mod 132 vorhanden ist. Somit können wir d berechnen.

Wir nutzen den obigen Rechenweg des euklidischen Algorithmus. Wir beginnen bei dem 2. Schritt mit Rest = 1

1)
Aus Schritt 2
5 : 2 = 2 Rest 1
Also:
5 = 2 * 2 + 1
1 = 5 – 2 * 2

2)
Aus Schritt 1
132 : 5 = 26 Rest 2
Also:
132 = 5 * 26 + 2
2 = 132 – 5 * 26

Jetzt Einsetzen von 2 in 1

1 = 5 - 2 * (132 – 5 * 26)
1 = 5 - 2 * (132 - 5 * 26)
1 = 5 - 2 * 132 + 2 * 5 * 26
1 = 5 - 2 * 132 + 52 * 5
1 = 53 * 5 - 2 * 132

53 * 5 ≡ 1 mod 132
d = 53

Privater Schlüssel ist somit
(53, 161)

Aufgabe 3

b)