Name: Gruppe:

**Verschlüssele und entschlüssele das Wort: FINAL**

1. Text in Zahlen umwandeln: ASCII Code erzeugen

F I N A L

*Python Programm Umwandlung von Text in ASCII: Link*

2. Öffentlichen Schlüssel erzeugen

a) 2 Primzahlen im Bereich von … bis … (Gruppe beachten!)

p= q=

*Python Programm Überprüfung, ob p und q Primzahlen sind: Link*

3. Berechnung von n und phi

n= phi=

4. Ermittlung einer teilerfremden Zahl e zu phi

e=

*Python Programm Überprüfung Teilerfremdheit von e zu phi: Link*

5. Verschlüsselung des Wortes Final mit dem öffentlichen Schlüssel (n,e)

c1=

c2=

c3=

c4=

c5=

*Python Programm für die Berechnung der Einwegfunktion: Link*

6. Privater Schlüssel. Ermittlung des modularen Inversen d

d=

*Python Programm für die Berechnung von d*

7. Entschlüsselung der Nachricht durch den privaten Schlüssel (n,d)

m1=

m2=

m3=

m4=

m5=

*Python Programm für die Berechnung der Einwegfuktion: Link*