1. Aufgabe: RSA und das Entschlüsseln

m … Message-Text (der sog. Klartext: A→ 1, B→ 2, C→ 3, ...)
n … der RSA-Modul
c … Cipher-Text (der verschlüsselte Text)
(e,N) … der Public-Key (wird zum Verschlüsseln verwendet)
(d,N) … der Private-Key (wird zum Entschlüsseln verwendet)
phi(N) … Eulersche phi-Funktion (wird zum Berechnen von e und d verwendet)

1.1. Entschlüssle "8 1 4 7 2 5 6"

☑ Gegeben: a) Cipher-Text: c= "8 1 4 7 2 5 6" b) public Key(e,n): (3,10)

☑ **Gesucht: Message: m="? ? ? ? ? ? ?" (im Klartext; also in Form v. Buchstaben)**

Lösung:

☑ Entschlüsseln mit (Formel angeben): m= _____

☑ Berechne: d , wenn N=10 und e=3 bekannt sind:

☐ es gilt: e*d ≡ _____

☐ es gilt: phi(n) = _____

☐ Berechne nun d durch Einsetzen von d=1,2,3,4,… in die Formel zur Berechnung des multiplikativ Inversen zu e. Die Formel lautet: 3*d_____.

☑ Finde ein d , sodass 3.d (mod _____) die Zahl 1 ergibt.

d	3*d mod _____	Ergebnis
1	3*1 mod _____	
2		
3		

→ d= _____

☑ Entschlüssle nun den Text: m= c^d mod N

c	8	1	4	7	2	5	6
berechne: c^d							
m= c^d mod N							
Buchstabenfolge							

☑ Probe: Verschlüsseln: c= m^e mod N

m							
berechne: m^e							
c= m^e mod N							

1.2. Euklidischer Algorithmus zur Berechnung von d

☑ Zeige die Berechnung von d durch den erweiterten Euklidischen Algorithmus. Es gelten die Werte von oben.
☑ Es gilt: ggT(a,b)=ggT(b,a) und ggT(a,1)= 1 und ggT(a,b)= ggT(b,a%b)

ggT	Division	Modulo	Linearkombination	Rest explizit schreiben
ggT(__ , __)	__ /__ = __	__ % __ = __	__ = __ * __ + __	__ = __ - __ * __
				rückwärts einsetzen

→ k= _____ → d= _____

1.3. Weitere Fragen

☐ n,p,q sind Zahlen, die geheim,öffentlich,prim oder nicht prim sein können? Was gilt?

n:	**O prim,**	**O nicht prim,**	**O geheim,**	**O öffentlich**
p:	**O prim,**	**O nicht prim,**	**O geheim,**	**O öffentlich**
q:	**O prim,**	**O nicht prim,**	**O geheim,**	**O öffentlich**

☐ Wie können p und q geheim sein, wenn doch n= p*q öffentlich bekannt ist?
Antwort:

_____

_____

☐ Für die Zahl **e** , den öffentlichen Schlüssel, muss gelten
ggT(e, phi(n))= _____

Hierbei ist phi(n), die _____

_____

☐ Gib eine math. Erklärung für
phi(n) = (p – 1)(q – 1)

☐ Wie wählt man e? Was muss für e gelten?
e wird gewählt unter folg. Bedingungen: _____

_____