13.23 Aufgabe: RSA Verfahren 1

Für RSA sind folgende Angaben bekannt: p=7, q=11, e=17.

a) Welche Eigenschaft muss e=17 erfüllen, damit ein privater Schlüssel d existiert?
b) Bestimmen Sie den privaten Schlüssel d mittels des erweiterten Euklidischen Algorithmus.
c) Welcher Zahlenbereich kann als Nachricht verwendet werden?
d) Wie lautet der Chiphertext C für die Nachricht P=16?
e) Zeigen Sie, dass die Entschlüsselung von C wieder auf P=16 führt.

a) Das muss gelten

$$e * d \bmod (p-1)(q-1) = 1$$

b)

Zum ggT	Umformen für Inverse:
17*d mod(60)	
ggT(60, 17):	=> (2*60-7*17) mod 60= -7*17 mod 60
60=3*17 + 9	1=(60-3*17)-1*17=2*60-7*17
17=1*9 +8	1=9-(17-1*9)=2*9-1*17
9= 1*8 +1	1= 9-1*8
8=8*1 +0	
ggT(60,17)=1	

Ergebnis: das inverse ist -7
Somit folgt:
(17 * (-7)) mod 60 = -119 mod 60 = 1
Es gilt aber nicht
1 < -7< 60
d.h.
d= -7 +60= 53
(17 * 53) mod 60 = 901 mod 60 = 1
1<54<60
=>d=54

c)
0 <= M < n, M=message

d)
16^17 mod 77
17= 10001
16^0=1
16^1=1*1*16=16
16^10=16*16=25
16^100=25*25=9
16^1000=9*9=4
16^10000= 4*4=16

16^10001=16*16=25

e)

25^54 mod 77
54=110110
25^0=1
25^1=25
25^10=25*25=9
25^11=9*25=71
25^110=71*71=36
25^1100=36*36=64
25^1101=64*25=60
25^11010=60*60=58
25^11011=58*25=64
25^110110= 64*64=16