Codierung und Decodierung mithilfe des RSA-Verfahrens

vorgegeben sind folgende Werte:

M = HELAU
p = 13
→ N = p*q = 143
q = 11
e = 7

Verschlüsselung:

1. Zuerst wird M codiert (eigentlich in ASCII, hier aber vereinfacht)

   H E L A U
   08 05 12 01 21

2. Nun kann man die Nachricht bzw. die Zahlen mit der Formel M^e mod N = C codiert werden

   Zunächst das „H“ bzw. „08“

   08^7 mod 143 = C
   2097152 mod 143 = C
   C = 57

   Nun für die restlichen

   05^7 mod 143 = 47
   12^7 mod 143 = 12
   01^7 mod 143 = 1
   21^7 mod 143 = 109

3. Die Verschlüsselte Nachricht lautet also

   57 47 12 1 109

Entschlüsselung:

1. Zum entschlüsseln benötigt man den privaten Schlüssel d, den man mit folgender Formel ausrechnen kann:

$$\frac{k*(p-1)(q-1)+1}{e} = d$$

z.B. $\frac{1*(13-1)(11-1)+1}{7} = 17{,}29$

Hier muss man nun die eine ganze Zahl für den Wert „d“ rausbekommen. Dies ist bei k = 6 der Fall.

$$\frac{6*(13-1)(11-1)+1}{7} = 103$$

d.h. d = 103

2. Jetzt kann man die verschlüsselte Nachricht mithilfe der Formel C^d mod N = M entschlüsseln.

Zunächst das „H“ bzw. „57“

57^103 mod 143 = 8

Jetzt die restlichen:

47^103 mod 143 = 5
12^103 mod 143 = 12
1^103 mod 143 = 1
109^103 mod 143 = 21

Ergebnis: 8 5 12 1 21

Diese Zahlen kann man jetzt in Buchstaben „umwandeln“ und raus kommt: HELAU