RSA – Public – Key – Verfahren Lösung

1. **Anton** wählt **p= 5** und **q = 13** als Primzahlen und berechnet damit **phi** und **n**

Anton berechnet also:

phi=(p-1)(q-1) = 4*12 = 48

n = pq = 65
Wir wählen **e** nun frei als **43** (da es kleiner als **phi** und teilerfremd zu **phi** sein muss)
d ist das Inverse von e im Modulo **phi** und hier aus der Tabelle zu bestimmen**.**

Maltabelle (phi) (nur teilerfremde)

1	5	7	11	13	17	19	23	25	29	31	35	37	41	43	47
5	25	35	7	17	37	47	19	29	1	11	31	41	13	23	43
7	35	1	29	43	23	37	17	31	11	25	5	19	47	13	41
11	7	29	25	47	43	17	13	35	31	5	1	23	19	41	37
13	17	43	47	25	29	7	11	37	41	19	23	1	5	31	35
17	37	23	43	29	1	35	7	41	13	47	19	5	25	11	31
19	47	37	17	7	35	25	5	43	23	13	41	31	11	1	29
23	19	17	13	11	7	5	1	47	43	41	37	35	31	29	25
25	29	31	35	37	41	43	47	1	5	7	11	13	17	19	23
29	1	11	31	41	13	23	43	5	25	35	7	17	37	47	19
31	11	25	5	19	47	13	41	7	35	1	29	43	23	37	17
35	31	5	1	23	19	41	37	11	7	29	25	47	43	17	13
37	41	19	23	1	5	31	35	13	17	43	47	25	29	7	11
41	13	47	19	5	25	11	31	17	37	23	43	29	1	35	7
43	23	13	41	31	11	1	29	19	47	37	17	7	35	25	5
47	43	41	37	35	31	29	25	23	19	17	13	11	7	5	1

(d hält Anton streng geheim)
Hier: d=19 weil in der Spalte von 43 die 1 zum ersten Mal bei der Zeile von 19 auftaucht.
Eins ist der Rest von 19*43 beim Teilen durch 48, also 1= 19*43 modulo 48

Antons öffentliches Schlüsselpaar :

(43,65) nämlich (e,n)

2. **Berta** will die Nachricht **m=3** senden, die ausschließlich Anton lesen kann.

Berta berechnet **c**: Sie weiss, dass gilt: Ord(3,65)=12

Das heißt, sie weiß $3^{12} \underset{65}{\equiv} 1$.

$$c = m^e \underset{n}{\equiv} 3^{43} \underset{65}{\equiv} ?$$

$3^{43} = 3^{36+7} \underset{65}{\equiv} 3^7$ mit der Ordnung 12 können wir die Vielfachen von 12 abtrennen.

$mit: \_ 3^7 = 2187$

$2187 \bmod 65 = 42$

Also $c = m^e \underset{n}{\equiv} 3^{43} \underset{65}{\equiv} 42$

Berta sendet also c=42 an Anton.

3. Anton erhält **c** und entschlüsselt die Nachricht:

Wenn Sie das Inverse richtig bestimmt haben, haben Sie d=19. In Ermangelung besserer Taschenrechner teilen wir dies mit.
Alle 19. Potenzen hat er in der folgenden Tabelle. Z.B. heißt [12,38], dass 12^{19} mod 65 =38 ist.

[1, 1], [2, 63], [3, 42], [4, 4], [5, 60], [6, 46], [7, 58], [8, 57], [9, 9], [10, 10], [11, 41], [12, 38], [13, 52], [14, 14], [15, 50], [16, 16], [17, 43], [18, 47], [19, 59], [20, 45], [21, 31], [22, 48], [23, 62], [24, 54], [25, 25], [26, 26], [27, 53], [28, 37], [29, 29], [30, 30], [31, 21], [32, 33], [33, 32], [34, 44], [35, 35], [36, 36], [37, 28], [38, 12], [39, 39], [40, 40], [41, 11], [42, 3], [43, 17], [44, 34], [45, 20], [46, 6], [47, 18], [48, 22], [49, 49], [50, 15], [51, 51], [52, 13], [53, 27], [54, 24], [55, 55], [56, 56], [57, 8], [58, 7], [59, 19], [60, 5], [61, 61], [62, 23], [63, 2], [64, 64]

$$M = c^d \underset{n}{\equiv} 42^{19} \underset{65}{\equiv} 3$$

Anton liest M M=3

4.Brunhilde will nun auch eine Nachricht schicken. Berechnen Sie nun die Botschaft für m=2. Was sendet Brunhilde an Anton? Es ist auch Ord(2,65)=12.

Das heißt, sie weiß $2^{12} \underset{65}{\equiv} 1$.

$$c = m^e = 2^{36+7} \underset{65}{\equiv} 2^7 = 128 \underset{65}{\equiv} 63$$

Sie sendet ihm die 63.

Wie rechnet Anton?

Die Tabelle mit den 19-ten Potenzen zeigt: $63^{19} \underset{65}{\equiv} 2$

Das passt zur Nachricht von Brunhilde.