

RSA – Public – Key – Verfahren Aufgabe

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

Anton berechnet also:

$\phi =$

$n =$

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

Gegeben ist hier die Maltabelle von (ϕ) (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)

Antons öffentliches Schlüsselpaar : (43,n)

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

Berta berechnet c : Sie weiss, dass gilt: $\text{Ord}(3,65)=12$ und berechnet c :

$c =$ _____ und sendet c 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 $12^{19} \bmod 65 = 38$ 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]

Er berechnet $M =$ _____

4. Brunhilde will nun auch eine Nachricht schicken. Berechnen Sie nun die Botschaft für $m=2$.

Was sendet Brunhilde an Anton? Es ist auch $\text{Ord}(2,65)=12$.

Wie rechnet Anton?

Leuphana Universität Lüneburg	Bearbeitet von Team 24/10/2008
Team Aufgabe	Grunddatum Okt 08 Prof. Dr. Haftdorn