

Arbeitsblatt zum RSA-Algorithmus

Hinweis: Eingaben bitte nur in grau hinterlegten Felder

p **3**
q **5**

n=p*q **15** **wird veröffentlicht**
J(n)=(p-1)*q-1 **8**
kleinstes e **6**
größtes e **7**

e gewählt **7** OK **Hinweis: e darf auch kein Vielfaches von p oder q sein**
d gewählt **7** **wird veröffentlicht**
(d*e)modJ(n) **1** OK

© Prof. H. Kühn

Knacken des Schlüssels:
durch Primfaktorzerlegung von n
15 = 3 * 5

Tabelle zur Wahl von d			Beispiel einer Kodierung:			Beispiel der Dekodierung		
d	d*e	(d*e)modJ(n)	M	M exp e	C = (M exp e) mod n	C	C exp d	M = (C exp d) mod n
1	7	7	1	1	1	1	1	1
2	14	6	2	128	8	8	2097152	2
3	21	5	3	2187	12	12	35831808	3
4	28	4	4	16384	4	4	16384	4
5	35	3	5	78125	5	5	78125	5
6	42	2	6	279936	6	6	279936	6
7	49	1 OK	7	823543	13	13	62748517	7
8	56	0	8	2097152	2	2	128	8
9	63	7	9	4782969	9	9	4782969	9
10	70	6	10	10000000	10	10	10000000	10
11	77	5	11	19487171	11	11	19487171	11
12	84	4	12	35831808	3	3	2187	12
13	91	3	13	62748517	7	7	823543	13
14	98	2	14	105413504	14	14	105413504	14
15	105	1 OK	15	170859375	0	0	0	0
16	112	0						
17	119	7						
18	126	6						
19	133	5						
20	140	4						
21	147	3						
22	154	2						

Bedingung: M <= n

längere (größere) Nachrichten M
müssen in Teilstücken kodiert werden !