A12

A12:
Bob wählt p , q und Verschlüsselungsexponent e. Warum ist e ein zulässiger Verschlüsselungsexponent? Wie heißt der öffentliche, wie der private Schlüssel von Bob? Alice will an Bob die Nachricht n verschlüsselt übermitteln. Welche Zahl schickt sie an Bob? Wie entschlüsselt Bob die Nachricht?
a. $p = 3, q = 11, e = 7, n = 6$.
b. $p = 7, q = 11, e = 47, n = 2$

a.

Bob: $m = p \cdot q = 33$ $\quad \tilde{m} = (p-1)(q-1) = 2 \cdot 10 = 20$

$ggT(e, \tilde{m}) = ggT(7,20) = 1 \Rightarrow$ 7 ist ok.

öffentlicher Schlüssel : $(33, 7)$

privater Schlüssel : d mit $1 < d < \tilde{m}$: $7 \cdot d \equiv 1 \mod \tilde{m}$,

$\equiv \frac{1}{7} \mod 20$

$(33, 3)$

durch Hinsehen $3 \cdot 7 - 1 \cdot 20 = 1$

durch Ausprobieren $7, 14, 21$ ✓

oder mittels erweiterten Euklidschen Algorithmus

Alice: Verschlüsseln der Nachricht :

$N = n^e \mod m$ $\quad N = 6^7 \mod 33$

$6^1 \equiv 6$
$6^2 \equiv 3$
$6^4 \equiv 9$
$\Big\} \; 6^7 \equiv 6 \cdot 3 \cdot 9 \equiv -36 \equiv -3 \equiv 30$ ($27 \equiv -6$)

$N = 30$ verschlüsselte Nachricht

Bob: Entschlüsseln:

$n = N^d \mod m$ $\quad n = 30^3 \mod 33$

$30^1 \equiv -3$
$30^2 \equiv 9$
$\Big\} \; 30^3 \equiv -27 \equiv 6$

$n = 6$ entschlüsselte Nachricht

b.

Bob: $m = p \cdot q = 77$ $\quad \tilde{m} = 6 \cdot 10 = 60$

$ggT(47, 60) = 1$ ✓

öffentlicher Schlüssel : $(77, 47)$

privater Schlüssel : $47 \cdot d = 1 \mod 60$ $\quad (77, 23)$

a	b	q	r	x	y
60	47	1	13	-18	5 + 18 = 23
47	13	3	8	5	-3 - 15 = -18
13	8	1	5	-3	2 + 3 = 5
8	5	1	3	2	-1 - 2 = -3
5	3	1	2	-1	1 + 1 = 2
3	2	1	1	1	0 - 1 = -1
2	1	2	0	0	1

$1 = -18 \cdot 60 + 47 \cdot 23$
$\Rightarrow d = 23$

Alice: Verschlüsselung von $n = 2$:

Vorbereitung: 47 binär darstellen und 77er Reihe hinschreiben

$2^{47} \mod 77 = 18$

$N = 18$

1	77
2	154
3	231
4	308
5	385
6	462
7	539
8	616
9	693

47	$= (101111)_2$
23	1
11	1
5	1
2	1
1	0
0	1

$2^1 \equiv 2 \mod 77$
$2^2 \equiv 4$
$2^4 \equiv 16$
$2^8 \equiv 256 \equiv 25$
$2^{16} \equiv 625 \equiv 9$
$2^{32} \equiv 81 \equiv 4$

$2^{47} \equiv 2 \cdot 4 \cdot 16 \cdot 25 \cdot 4 \equiv 2 \cdot 25 \cdot 25 \equiv 18$
($256 \equiv 25$, 9)

Bob: Entschlüsseln :

$23 = (10111)_2$
$11 \quad 1$

$18^1 \equiv 18$

Bob: Entschlüsseln:

$n = 18^{23} \bmod 77$

$n = 2$

$23 = (10111)_2$

11	1
5	1
2	1
1	0
0	1

$256 \equiv 25 \qquad 9$

$18^1 \equiv 18$

$18^2 \equiv 324 \equiv 16$

$18^4 \equiv 256 \equiv 25$

$18^8 \equiv 9$

$18^{16} \equiv 81 \equiv 4$

$18^{23} \equiv 18 \cdot 16 \cdot 25 \cdot 4 \equiv -5 \cdot$

$4 \cdot 18 \equiv 72 \equiv -5$

$16 \cdot 25 \equiv 400 \equiv 15$

$\} -75 = 2$