Kryptographie

Fragen?

RSA. $p = 61$, $q = 53$, $e = 17$. Ver- und Entschlüsseln Sie die Nachrichten $T = 61$ und $T = 65$.
(Bemerkung: Bei https ist T meist der AES-Schlüssel, der ausgetauscht wird.)

Lösung.

$N = 61 \cdot 53 = 3233$

$\varphi(N) = 60 \cdot 52 = 3120$

$e = 17 ; p = 61 ; q = 53$

public key $= (17; 3233)$

privat key $= (2753 ; 3233)$

$17 \cdot d \equiv 1 \mod 3120 \quad d = -367 \equiv 2753$

$17x + 3120y = 1$

$-367 + z \cdot 3120 \quad z = 1$

$17 = 0 \cdot 3120 + 17 \qquad -367 \quad 2$

$3120 = 183 \cdot 17 + 9 \qquad 2 \quad -367$

$17 = 1 \cdot 9 + 8 \qquad -1 \quad 2$

$9 = 1 \cdot 8 + 1 \qquad 1 \quad -1$

$8 = 8 \cdot 1 + 0 \qquad 0 \quad 1$

Verschlüsseln $T = 61$

$61^{17} \mod 3233$

$61^{17} \equiv (61^2)^8 \cdot 61 \equiv (488^2)^4 \cdot 61 \equiv (2135^2)^2 \cdot 61 \equiv 2328^2 \cdot 61$

$\equiv 2501 \cdot 61 \equiv 610 \mod 3233$

Entschlüsseln

$610^{2753} \mod 3233$

$$610^{2753} \equiv (610^2)^{1376} \cdot 610 \equiv (305^2)^{688} \cdot 610 \equiv (2051^2)^{344} \cdot 610$$

$$\equiv (2373^2)^{172} \cdot 610 \equiv (1831^2)^{86} \cdot 610 \equiv (183^2)^{43} \cdot 610$$

Eigener Lösungsversuch.

$$\equiv (1593^2)^{21} \cdot 1593 \cdot 610 \equiv (1586^2)^{10} \cdot 1586 \cdot 2196$$

$$\equiv (122^2)^5 \cdot 915 \equiv (1952^2)^2 \cdot 1952 \cdot 915 \equiv 1830^2 \cdot 1464$$

$$\equiv 2745 \cdot 1464 \equiv \underline{\underline{61}}$$

Verschlüsseln – it $T = 65$ public key $(17; 3233)$

$65^{17} \bmod 3233$

$$65^{17} \equiv (65^2)^8 \cdot 65 \equiv (992^2)^4 \cdot 65 \equiv (1232^2)^2 \cdot 65 \equiv 1547^2 \cdot 65$$

$$\equiv 783 \cdot 65 \equiv \underline{2730} \bmod 3233$$

Entschlüsseln

$2730^{2753} \bmod 3233$

$$2730^{2753} \equiv (2730^2)^{1376} \cdot 2730 \equiv (2269^2)^{688} \cdot 2730 \equiv (1425^2)^{344} \cdot 2730$$

$$\equiv (301^2)^{172} \cdot 2730 \equiv (77^2)^{86} \cdot 2730 \equiv (2636^2)^{43} \cdot 2730$$

$$\equiv (632^2)^{21} \cdot 632 \cdot 2730 \equiv (1765^2)^{10} \cdot 1765 \cdot 1295 \equiv (1846^2)^5 \cdot 3177$$

$$\equiv (134^2)^2 \cdot 134 \cdot 3177 \equiv 1791^2 \cdot 2135 \equiv 545 \cdot 2135 \equiv 65 \bmod 3233$$