VerteilteWebInf Hausaufgabe 10

Gruppe 6

December 21, 2014

Aufgabe 2

b)
gegeben: verschlüsselte Nachricht $C = 13$, öffentlicher Exponent $e = 3$, $n = p \cdot q = 15$

Der Klartext M kann über $C^d \mod n$ berechnet werden, wobei d der private Exponent des Empfängers ist.
Berechne d: Es muss gelten, dass $e \cdot d \equiv 1 \mod \Phi(n)$ mit $\Phi(n) = (p-1)(q-1)$.
Wir benötigen also Primzahlen p und q, sodass $p \cdot q = n = 15$: $p = 3$, $q = 5$.
Also gilt $\Phi(n) = 4 \cdot 2 = 8$.
Es muss also gelten: $3 \cdot d \equiv 1 \mod 8$, also wähle $d = 3$.
Klartext $M = C^d \mod n = 13^3 \mod 15 = 7$. Der Klartext der Nachricht lautet also 7.