

## Aufgabe 2: RSA

[14 Punkte]

Betrachten Sie RSA mit öffentlichen Schlüssel  $P = (7, 15)$  und geheimen Schlüssel  $S = (7, 15)$ .

- (a) [6 Punkte] Ist das gegebene Schlüsselpaar mathematisch korrekt? Welche notwendigen mathematischen Eigenschaften werden eingehalten?

$e = 7$   
 $d = 7$   
 $n = 15 = p * q$   
 $p = 3$   
 $q = 5$   
 $m = (p-1)*(q-1) = 8$

$e * d \bmod m == 1$   
 $49 \bmod 8 == 1$  STIMMT  
 $6 * 8 = 48$

e ist teilerfremd mit m

- (b) [2 Punkte] Ist die Wahl dieser Schlüsselpaare für den praktischen Einsatz sinnvoll? Begründen Sie Ihre Antwort mit einem Satz.

NEIN, weil die zwei Schlüssel gleich sind.

- (c) [6 Punkte] Verschlüsseln Sie die Zahl 2 ohne ein Zwischenergebnis größer als 100 zu verwenden. Geben Sie die Berechnungsschritte an!

Ö:  $(e, n)$   
Geheime Nachricht = (Originelle Nachricht) $^e \bmod n$   
 ~~$= 2^7 \bmod 15$~~   $= (2 * 2^6) \bmod 15 = (2 \bmod 15) * (64 \bmod 15) = 2 * 4 = 8$

$2^7 = 2 * 2^6$

P:  $(d, n)$   
 $(7, 15)$

P:  $(d, n)$   
Entschlüsselte Nachricht = (Geheime) $^d \bmod n$   
 $= 8^7 \bmod 15 = 2$