Spezielle Aspekte: Kryptographie *SoSe 2011*
Barbara Baumeister

10. Präsenzübungsblatt

Aufgabe 1 Sei $n = 667$. Fakorisieren Sie n in seine Primfaktoren

(a) mit Hilfe von Pollards $(p-1)$-Methode;

(b) mit dem Verfahren von Fermat.

Aufgabe 2 Alice verschlüsselt die Nachricht m mit Bobs öffentlichen RSA-Schlüssel $(899, 11)$. Der Chiffretext ist 468. Bestimmen Sie den Klartext.

Aufgabe 3 Wieviele Operationen erfordert der RSA-Verschlüsselung mit Verschlüsselungsexponent $e = 2^{16} + 1$?