Kryptologie

Übung, LVA 405.321
C. Fuchs

8. Übungsblatt, SS 2022

11.05.2022

1. Wieviel Operationen erfordert die RSA-Verschlüsselung mit dem Exponenten $e = 2^{16} + 1$?

2. Bekannt sind der RSA-Modul $n = 57249139981806679451$ der Exponent $e = 29$ und der geheime Schlüssel $d = 5922324823112658653$. Berechne p und q.

3. Können Sie den RSA-Modul $n = 14803$ faktorisieren, wenn sie wissen, dass $\varphi(n) = 14560$ ist?

4. Von einer Bank wird 3 mal die gleiche Nachricht m an 3 verschiedene Kunden geschickt. Die öffentlichen Schlüssel der Kunden sind: $(n_1, e) = (6319, 3), (n_2, e) = (5959, 3), (n_3, e) = (5989, 3)$. Die verschlüsselten Nachrichten sind: $c_1 = 313, c_2 = 966, c_3 = 5759$. Was ist m?