Kryptologie

Übung, LVA 405.321
C. Fuchs

7. Übungsblatt, SS 2022

04.05.2022

1. Demonstriere den Diffie-Hellman Schlüsselaustausch anhand eines selbst gewählten Beispiels. Jedoch sollte $\mathbb{F}_q$ so gewählt werden, dass $q > 10^6$ gilt (am Computer vorzuführen).

2. Wir verwenden das RSA-Verfahren. Der Empfänger gibt als öffentlichen Schlüssel $e = 43, n = 77$ bekannt. Eine Nachricht m wird als $c = 5$ zum Empfänger gesandt und abgefangen. Was ist m?

3. Ein Teilnehmer im RSA-Verfahren mit dem öffentlichen Schlüssel $n = 1271, e = 7$ erhält die chiffrierte Nachricht $99, 232, 815, 74, 1047, 196, 384, 196, 384, 196, 1122, 0, 171, 771, 243, 257$. Die Buchstaben der Nachricht im Klartext wurden mit 2 Ziffern codiert, und die sich ergebende Ziffernfolge wurde in Blöcke der Länge 3 eingeteilt. Wie lautet die Nachricht im Klartext?

4. Verschlüssele den Text "DAS_GROSSE_GEHEIMNIS" mit dem RSA-Verfahren. Dabei soll ein passendes Alphabet, ein Modul n und ein Exponent e generiert werden, sodass der Klartext in Blöcke der Länge 4 und der verschlüsselte Text in Blöcke der Länge 5 zerteilt wird.