

Klausur

Aufgabe 1. (über den Miller-Rabin Primtest)

- a) Finden Sie alle Elemente der Menge L_n für $n = 35$.
- b) Mit welcher Wahrscheinlichkeit erhalten wir die Antwort “ n ist eine Primzahl” im Miller-Rabin-Primtest für die Zahl $n = 35$ und den Parameter $s = 2$?

Aufgabe 2.

- a) Geben Sie die Definition der Carmichael-Zahl.
- b) Beweisen Sie, daß 5307 keine Carmichael-Zahl ist.

Aufgabe 3. Finden Sie alle natürlichen Zahlen, für die ρ in der Pollard- ρ -Faktorisierungsmethode genau 3 Zahlen enthält.

Aufgabe 4. (über das RSA-Kryptosystem)

Der öffentliche Schlüssel (n, e) von Bob ist $(1457, 637)$. Bob erhält einen Chiffretext $s = 2$ von Alice. Wie sieht ihr Klartext t aus?

Aufgabe 5. Beschreiben Sie das Diffie-Hellman-Schlüsselaustausch-Verfahren.