

1. Übungsblatt

Aufgabe 1. Welche Nachricht verbirgt sich hinter folgender Shift-chiffre?
AMPZTMQKPBHCMVBAKPTCMAAMTV

Aufgabe 2. In einem Vigenere-Chiffre-text finde sich eine wiederholte Zeichenkette bei den Positionen 38, 225, 395 und 718. Welche Schlüssellänge könnte man vermuten?

Aufgabe 3. Wieviele mögliche Affine Chiffren gibt es für ein Alphabet der Größe 64?

Aufgabe 4. Welche Nachricht verbirgt sich hinter folgender Affinen Chiffre?
XFFPCUJLIUXLIGRLIZPCSVPUGRLIQVPRRPQU

Aufgabe 5. Ist es möglich, daß eine Affine Chiffre modulo 26 die Nachricht (17,14,19) auf die Chiffre (20, 13, 3) abbildet? Wie ist es in umgekehrter Richtung?

Aufgabe 6. Das RSA-Verfahren soll (warum auch immer) mit dem Produkt von 3 statt nur 2 Primzahlen berechnet werden. Wird dies ebenfalls funktionieren? (Begründung) Sei $n = 7 \cdot 13 \cdot 19$. Wie lautet $\phi(n)$? Wie lautet der Umkehrschlüssel zu $(5, n)$ (unter Verwendung des erweiterten Euklidischen Algorithmus zu berechnen).

Aufgabe 7. Es sei ein Algorithmus gegeben, der effizient $x^3 \text{ Mod } n$ berechnet. Wie könnte dies bei einer entsprechenden Variante des square-and-multiply Algorithmus benutzt werden? (Demonstration am Beispiel $x^{30} \text{ Mod } n$.)

Aufgabe 8.

Formuliere als Pseudocode einen Algorithmus, der auf Eingabe einer großen Zahl y die nächstgrößere Primzahl findet, dabei soll mit Hilfe des Sieb des Eratosthenes eine Vorauswahl der nächsten 10000 Zahlen erfolgen und dann der Algorithmus von Miller verwendet werden.

Aufgabe 9. Welche Zahlen sind quadratische Residuen modulo 17 ?

Aufgabe 10 Welche Zahlen sind quadratische Residuen modulo 21 ?

Aufgabe 11. Welche Zahlen sind quadratische Residuen modulo 25 ?

Aufgabe 12.

Wieviele quadratische Residuen gibt es modulo p^i für eine Primzahl p ?

Aufgabe 13.

Wieviele quadratische Residuen gibt es modulo $n = p \cdot q$ für Primzahlen p, q ?

Aufgabe 14.

Zeige mittels Lucas's Test, daß 937 prim ist.

Aufgabe 15.

Wie lautet eine Pratt-Sequenz (Primalitätszertifikat) für 937 ?

Aufgabe 16.

Zeige mittels des Eulerschen Kriteriums daß 507 zusammengesetzt ist.

Aufgabe 17.

Untersuche 5051 und 5053 mit Millers Algorithmus auf Primalität

Aufgabe 18. Zur Demonstration der Methode im AKS-Algorithmus berechne das Polynom $(X - 3)^{55}$ modulo dem Polynom $x^3 - 1$ und der Zahl 55.