

Aufgabe 1: (6 Punkte)

- (a) Betrachten Sie einen Brute-Force-Angriff auf ein Verschlüsselungsverfahren mit einem 1024-Bit-Schlüssel. Berechnen Sie die mittlere Zeit zum Knacken des Verfahrens unter der Annahme, dass pro Sekunde $5 \cdot 10^{15}$ Schlüssel getestet werden können.
- (b) Betrachten Sie eine Blockchiffre, bei der jeweils ein Block der Größe 1024 Bit mit einem 1024-Bit-Schlüssel verschlüsselt wird. Berechnen Sie die mittlere Zeit zum Knacken der Blockchiffre mit einem Brute-Force-Angriff unter der Annahme, dass ein Klartext-Geheimtext-Paar der Größe 1024 Bit vorliegt und sich pro Sekunde 128 KByte verschlüsseln lassen.

Aufgabe 2: (10 Punkte)

Betrachten Sie folgendes Verschlüsselungsverfahren über einem gegebenen Alphabet A .

- Schlüssel: natürliche Zahl $t \in \{1, \dots, |A|\}$ mit $\text{ggT}(t, |A|) = 1$
 - Verschlüsseln: Ersetze das Klartextzeichen mit der Nummer $\lambda \in \{1, \dots, |A|\}$ durch das Geheimtextzeichen mit der Nummer $(\lambda \cdot t) \bmod |A|$.
- (a) Was passiert, wenn die Forderung $\text{ggT}(t, |A|) = 1$ nicht erfüllt ist?
 - (b) Wie sieht die zugehörige Entschlüsselungsfunktion aus?
 - (c) Wie viele verschiedene Chiffren der angegebenen Art gibt es für das natürliche Alphabet?
 - (d) Zeigen Sie, dass bei jeder dieser Chiffren der Klartextbuchstabe ‘m’ auf das Geheimtextzeichen ‘M’ und ‘z’ auf ‘Z’ abgebildet wird.
 - (e) Betrachten Sie folgende verallgemeinerte Verschlüsselung:

$$\lambda \mapsto (\lambda \cdot t_1 + t_2) \bmod |A| \text{ mit } t_1, t_2 \in \{1, \dots, |A|\} \text{ und } \text{ggT}(t_1, |A|) = 1.$$

Wie viele verschiedene Chiffren dieser Art gibt es für das natürliche Alphabet?

Programmieraufgabe P1: (8 Punkte)

Implementieren Sie den Euklidischen Algorithmus und den erweiterten Euklidischen Algorithmus jeweils in einer rekursiven und einer iterativen Variante. Der Algorithmus soll zwei Zahlen von der Kommandozeile einlesen und den ggT ausgeben. Testen Sie die Algorithmen an verschiedenen Beispielen.