

Aufgabe 3: (4 Punkte)

Bei der *affinen Chiffre* über \mathbb{Z}_n ist die Verschlüsselung gegeben durch

$$E(x, K) = (ax + b) \bmod n, \quad a, b \in \mathbb{Z}_n$$

Der Schlüssel ist das Paar $K = (a, b) \in \mathbb{Z}_n^2$.

Man nennt einen Schlüssel K in einem Kryptosystem *selbstinvers*, wenn die Verschlüsselungsfunktion $E(x, K)$ und die Entschlüsselungsfunktion $D(y, K)$ identisch sind, d.h. wenn gilt $E(x, K) = D(x, K)$. Daraus folgt auch $E(E(x, K), K) = x$.

Zeigen Sie, dass bei der affinen Chiffre der Schlüssel $(a, b) \in \mathbb{Z}_n^2$ genau dann selbstinvers ist, wenn gilt:

$$a = a^{-1} \bmod n \quad \text{und} \quad b \cdot (a + 1) = 0 \bmod n$$

Aufgabe 4: (6 Punkte)

- (a) Betrachten Sie eine zweifache Vigenère-Verschlüsselung, bei der der Klartext zunächst mit einem Schlüsselwort der Länge k_1 und danach mit einem Schlüsselwort der Länge k_2 Vigenère-verschlüsselt wird. Entspricht diese zweifache Verschlüsselung einer einfachen Vigenère-Verschlüsselung? Wenn ja, bestimmen Sie Schlüssellänge und Schlüsselwort; wenn nein, geben Sie ein Gegenbeispiel an!

- (b) Bestimmen Sie den kleinsten und größten Wert, den der Index $I' = \sum_{i=1}^{26} \left(\frac{n_i}{n}\right)^2$ (siehe Skript, S. 21f) für einen Text über einem Alphabet mit 26 Buchstaben annehmen kann (mit Beweis!).

Programmieraufgabe P2: (14 Punkte)

Die im Folgenden zu schreibenden Programme sollen Texte bestehend aus Klein- und Großbuchstaben korrekt verarbeiten können, wobei alle anderen Zeichen zu ignorieren sind. Der Start soll jeweils über die Kommandozeile erfolgen, wobei eine Parameterhilfe (Usage-Information) gezeigt werden soll, wenn der Benutzer einen syntaktisch ungültigen Aufruf macht.

- (a) Implementieren Sie die Vigenère-Chiffre.
- (b) Implementieren Sie den Friedman-Test.
- (c) Implementieren Sie den Kasiski-Test.
- (d) Entschlüsseln Sie den folgenden deutschen Text, der mit der Vigenère-Chiffre verschlüsselt wurde. Beschreiben Sie Ihre Vorgehensweise beim Angriff und bestimmen Sie das verwendete Schlüsselwort.

```
FQTCMXGVTYITJQUMVVKAIWSCAIAWLRDMIPWTJLPKYIEPZHREFMGZICDMZSEIVMMAFLEP
HAESGICCIUUKWPIUGVTUWKGALRRWNJUXVTAROMVFTXJLVIMWLMVMMADVKKWLRDDOTI
MCFMIDIIFMCLMEGSGFTKCVPSJCJGQHAJLGHVPTJMROMWHTZTUMDCTANIDGQCLRJEPLPII
KOTYECUJTPQFPWPSTYJCJTAMJEPTUZVTAROPLGAHLPLPOTUHRUDTYJRJZTUMJVVPJLSNI
XZIUGDXNIEGZTIECVCAHVTQBZITJHTORKGVYHLIJCKIIVTTIX
```