

Klausur Wahrscheinlichkeitsrechnung und Kryptographie

Zugelassen sind alle Hilfsmittel (außer Kommunikationsmitteln)

Sie können maximal 60 Punkte erreichen, aber 5 davon sind "Zusatzpunkte". Sie erhalten also für 55 Punkte eine "1", und ab 28 Punkten (> 50% von 55) haben Sie bestanden.

- 1) Gegeben sei das Wort BANANEN.
 - a) Wie viele Worte kann man hieraus durch Buchstabenvertauschungen erzeugen? (2 P)
 - b) Wie viele dieser Worte beginnen und enden mit einem A? (2 P)
 - c) Wie viele dieser Worte enthalten die drei N's direkt hintereinander? (2 P)

- 2) Ein Florist hat Rosen in 4 verschiedenen Farben vorrätig.
Auf wie viele Weisen können Sie Sträuße aus 6 Rosen zusammenstellen, wenn
 - a) genau 2 rote und 2 gelbe Rosen dabei sein sollen, (2 P)
 - b) jede der 4 Farben vorkommen soll, (2 P)
 - c) die Farbzusammenstellung beliebig ist? (3 P)

- 3) Drei Junge und drei Mädchen verteilen sich zufällig auf sechs nebeneinanderliegende Sitzplätze.
Wie groß ist die Wahrscheinlichkeit, dass
 - a) die drei Mädchen zusammen sitzen, (3 P)
 - b) sich Jungen und Mädchen in der Reihe abwechseln? (3 P)

- 4) Ein Würfel wird dreimal hintereinander geworfen.
Wie groß ist die Wahrscheinlichkeit dafür, dass
 - a) keine 6 gewürfelt wird, (2 P)
 - b) höchstens eine 6 gewürfelt wird, (2 P)
 - c) das Produkt der Augenzahlen weder durch 2 noch durch 3 teilbar ist? (3 P)

- 5) Die Wahrscheinlichkeit, dass Schützenkönig Müller die Zielscheibe trifft, beträgt $\frac{1}{3}$.
Wie oft muss er schießen, damit er die Scheibe mit einer Wahrscheinlichkeit von mindestens 90% trifft? (6 P)

Klausur Wahrscheinlichkeitsrechnung und Kryptographie

- 6) Die kontinuierliche Zufallsvariable X besitze die Dichtefunktion

$$f(x) = \begin{cases} cx & 0 \leq x \leq a \\ c \cdot (2a - x) & a < x \leq 2a \\ 0 & \text{sonst} \end{cases} \quad (a > 0)$$

- a) Skizzieren Sie den Verlauf von $f(x)$. (1 P)
- b) Welchen Wert muss der Faktor c haben? (2 P)
- c) Wie groß ist der Erwartungswert von X ? (2 P)
- d) Wie groß ist die Standardabweichung von X ? (2 P)

- 7) a) Wie lautet die letzte Dezimalstelle von 7^{222} ? (3 P)
- b) Bestimmen Sie mittels des euklidischen Algorithmus ganze Zahlen x und y mit
- $$322x + 189y = 7$$
- unter Angabe aller Einzelschritte. (4 P)
- c) Warum gibt es keine ganzen Zahlen x und y mit
- $$322x + 189y = 5?$$
- (1 P)

- 8) Eine monoalphabetische, monographische Chiffrierung eines deutschen Textes, der nur aus den Großbuchstaben $\mathbf{V} = \{ A, B, \dots, Z \}$ besteht (Satzzeichen und Wortzwischenräume wurden weggelassen), funktioniert wie folgt:

Den Buchstaben $\in \mathbf{V}$ seien wie üblich die Zahlen $\{ 0, 1, \dots, 25 \}$ zugeordnet, damit man mit ihnen „rechnen“ kann. Die Verschlüsselung eines Klartextbuchstaben $x \rightarrow f(x)$ erfolgt über die Formel

$$f(x) = (ax + b) \bmod 26$$

mit ganzen Zahlen $a, b \in \{ 0, 1, \dots, 25 \}$.

Verlässlichen Quellen ist zu entnehmen, dass bei dieser Verschlüsselung das "E" in das "C" übergeht und das "M" in sich selbst.

Welche Werte haben a und b ?

Hinweis: Die Lösung ist nicht eindeutig – alle Lösungen sind gefragt! (7 P)

- 9) In einem Public-Key-System nach dem RSA-Verfahren fangen Sie als böser Lauscher den Geheimtext $c = 24$ ab, der an einen Empfänger gerichtet ist, dessen öffentlicher Schlüssel aus $e = 11$ und $m = 77$ (das ist der Modul) besteht.

Wie lautet die Klarnachricht z , die sich hinter dem Geheimtext c verbirgt? (6 P)