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 seien die Ziffern 1, 1, 2, 2, 3, 3, 3.

a) Wie viele verschiedene Anordnungen dieser Ziffern gibt es? (2 P)

b) Wie viele dieser Ziffernfolgen beginnen mit einer 1 und enden mit einer 2? (2 P)

c) Wie viele dieser Ziffernfolgen gibt es, bei denen die beiden Einsen nebeneinander stehen? (2 P)

2) Ein Student muss in einer Prüfung 10 von 13 Fragen beantworten.

a) Auf wie viele verschiedene Weisen kann er 10 Fragen auswählen (und beantworten)? (1 P)

b) Auf wie viele Weisen, falls er auf jeden Fall die beiden ersten Fragen beantworten muss? (2 P)

c) Auf wie viele Weisen, falls er **genau** 3 der ersten 5 Fragen beantworten muss? (2 P)

d) Auf wie viele Weisen, falls er **mindestens** 3 der ersten 5 Fragen beantworten muss? (3 P)

3) In einem Sack befinden sich 2 rote, 2 blaue, 2 gelbe und 2 weiße Bälle. Sie greifen blind hinein und holen gleichzeitig 3 Bälle heraus.

Wie groß ist die Wahrscheinlichkeit dafür, dass

a) die gezogenen Bälle alle verschiedenfarbig sind, (2 P)

b) Sie genau zwei gleichfarbige Bälle und einen andersfarbigen Ball ziehen, (3 P)

c) mindestens ein roter Ball dabei ist? (3 P)

4) Sie werfen zwei faire Würfel (alle Augenzahlen sind also gleich wahrscheinlich).

a) Welche der möglichen Augenzahlen $\in \{ 2, 3, 4, \dots 11, 12 \}$ erscheint mit der größten Wahrscheinlichkeit, und wie groß ist diese? (3 P)

b) Mit welcher Wahrscheinlichkeit zeigt mindestens einer der Würfel eine „1“ oder eine „2“? (3 P)

5) Eine seltene Krankheit tritt mit einer Wahrscheinlichkeit von 10^{-5} auf. Ein Antikörpertest für diese Krankheit erkennt eine Infektion mit einer Wahrscheinlichkeit von 95%. Gesunde Probanden werden mit einer Wahrscheinlichkeit von 0,5% irrtümlich als krank eingestuft (positives Testergebnis).

Wie groß ist die Wahrscheinlichkeit, dass bei einem positiven Testergebnis tatsächlich eine Infektion vorliegt? (5 P)

6) Die kontinuierliche Zufallsvariable X besitze die Dichtefunktion

$$f(x) = \begin{cases} Cx & 0 \le x \le a \\ 0 & \text{sonst} \end{cases} \qquad (a > 0)$$

a) Skizzieren Sie den Verlauf von f(x). (1 P)

b) Welchen Wert muss der Faktor C haben? (1 P)

c) Wie groß ist der Erwartungswert von X? (2 P)

d) Wie groß ist die Standardabweichung von X? (3 P)

7) a) Berechnen Sie per Hand möglichst effizient 5^{292} mod 16.

Hinweis: das Euler'sche Theorem ist hier hilfreich. (3 P)

b) Bestimmen Sie ganze Zahlen x und y mit

$$482\,x + 192\,y = 4 \,. \qquad (4\ P)$$

Stellen Sie dabei ausführlich alle Einzelschritte dar.

c) Warum gibt es keine ganzen Zahlen x und y mit

$$482\,x + 192\,y = 3\ ? \qquad (1\ P)$$

8) Eine monoalphabetische, monographische Chiffrierung eines deutschen Textes, der nur aus den Großbuchstaben **V** = { A, B, … , Z } besteht (Satzzeichen und Wortzwischenräume wurden weggelassen), funktioniere wie folgt:

Den Buchstaben ∈ **V** seien wie üblich die Zahlen { 0, 1, … , 25 } zugeordnet, damit man mit ihnen „rechnen" kann. Die Verschlüsselung eines Klartextbuchstaben x → f(x) erfolgt über die Formel

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

mit ganzen Zahlen a, b ∈ { 0, 1, … 25 }.

Verlässlichen Quellen ist zu entnehmen, dass bei dieser Verschlüsselung das „E" in das „O" übergeht und das "O" in das „W".

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 das Kryptogramm C = 10 ab, das an einen Empfänger gerichtet ist, dessen öffentlicher Schlüssel aus e = 5 und m = 35 (das ist der Modul) besteht.

Wie lautet die Klarnachricht Z, die sich hinter dem Kryptogramm C verbirgt? (5 P)