LANDESPRÜFUNGSAMT

FÜR ERSTE STAATSPRÜFUNGEN FÜR LEHRÄMTER AN SCHULEN
- GESCHÄFTSSTELLE SIEGEN -

LPA I NRW, Geschäftsstelle Siegen
Hölderlinstr. 3 57068 Siegen

Herrn
Prof. Dr. Nils-Peter Skoruppa
Fakultät 4
im Hause

EINGEGANGEN
24. MRZ. 2011

Hölderlinstr. 3
57068 Siegen
Universität

Telefon: 0271/ 740-3370
Durchwahl: 0271/740-3370/-4120
0271/740-2342 (Fax)

Siegen, den 22.03.2011
Az: jk
(Bei Antwort bitte angeben)

Betr.: Schriftliche Arbeiten unter Aufsicht (Klausurarbeiten)

hier: Bestellung zum Erstgutachter / zur Erstgutachterin

Anlg.: Klausurarbeiten / Übersichtsliste

Sehr geehrter Herr Prof. Dr. Skoruppa,

hiermit bitte ich Sie, die anliegenden Klausurarbeiten zu begutachten und die Arbeiten mit Ihrem Gutachten anschließend an mich zurückzuschicken, und zwar spätestens bis zum:

23.04.2011

Die Gutachten sollen den Grad selbständiger Leistung, den sachlichen Gehalt, Planung, Methodenbeherrschung, Aufbau, Gedankenführung und sprachliche Form bewerten sowie die Vorzüge und Mängel der Arbeit deutlich bezeichnen. Sie sind mit einer Note abzuschließen.

Die zulässigen Notenstufen lauten:
sehr gut (1,0; 1,3) / gut (1,7 ; 2,0 ; 2,3) / befriedigend (2,7 ; 3,0 ; 3,3) / ausreichend (3,7 ; 4,0) / mangelhaft (5,0 ; 5,3) / ungenügend (5,7 ; 6,0)

Die Noten "ausreichend minus (4,3)" und "mangelhaft plus (4,7)" dürfen bei der Bewertung nicht vergeben werden.

gem. LPO 2003:
Die zulässigen Notenstufen lauten:
sehr gut (1,0; 1,3) / gut (1,7 ; 2,0 ; 2,3) / befriedigend (2,7 ; 3,0 ; 3,3) / ausreichend (3,7 ; 4,0) / mangelhaft (5,0) / ungenügend (6,0)
Die Noten 0,7, 4,3, 4,7 5,3 5,7 und 6,3 dürfen bei der Bewertung nicht vergeben werden.

Überprüfen Sie bitte, ob Sie die Klausurarbeiten aller auf der Liste genannten Kandidaten mit dieser Sendung auch tatsächlich erhalten haben. Verständigen Sie mich bitte sofort bei etwaigen Unstimmigkeiten.

Mit freundlichem Gruß
Im Auftrag

Klingebiel (Reg.-Inspektorin)

LANDESPRÜFUNGSAMT
FÜR ERSTE STAATSPRÜFUNGEN FÜR LEHRÄMTER AN SCHULEN

Versanddatum: **22.03.2011**

Herrn
Prof. Dr. Skoruppa
Fakultät 4
im Hause

Kandidat(in)	Kennung	Fach	Lehramt
Michael Seidel	W	M	27

Umschlagseite 1

LANDESPPRÜFUNGSAMT
FÜR ERSTE STAATSPRÜFUNGEN FÜR LEHRÄMTER AN SCHULEN

ARBEIT UNTER AUFSICHT (KLAUSUR)

☐ G-H-R/Schw.p. G ☐ G-H-R/Schw.p. H/R ☒ Gymnasium/Ges.sch.
☐ Berufskolleg ☐ Sonderpädagogik

Kandidat/in: Michael Seidel

Prüfungsfach: Mathematik

Prüfer/in: Prof. Dr. Skorupka (Erstgutachten)

Prüfungstag: 22.03.2011

Prüfungsbeginn: 8:00 **Prüfungsende:** 12:17

Thema:
Siehe Anlage

Zweitgutachter/in:

V2
Modul des o. g. Themas (gem. Aufgabenblatt):

Drittgutachter/in:

Hinweise für die Prüflinge

0 **Das vorgelegte Thema ist unverändert zu bearbeiten**. In Fächern, deren Besonderheiten dies erfordern, sind andere Formen der Aufgabenstellung zugelassen.
1 Die Bearbeitungszeit beträgt vier Zeitstunden.
2 Arbeits- und Hilfsmittel sind nur dann erlaubt, wenn sie vom Prüfer angegeben und vom Prüfungsamt zur Verfügung gestellt worden sind. Das Mitbringen unerlaubter Hilfsmittel gilt bereits als Täuschungsversuch.
3 Nummerieren Sie die Seiten der Reinschrift durchgehend und versehen Sie die einzelnen Bogen mit Ihrem Namen.
4 Füllen Sie die Umschlagseite 1 (obere Hälfte) vollständig aus.
5 Unleserliche Arbeiten werden behandelt wie nicht abgegebene Klausuren.
6 Geben Sie Ihre Arbeit (Klausurtasche mit Aufgabenblatt, Reinschrift, Konzept, ggf. zur Verfügung gestellte Arbeits- und Hilfsmittel) persönlich beim Aufsichtführenden ab. Nicht benutztes Reinschrift- oder Konzeptpapier ist ebenfalls abzugeben. Fehlende Unterlagen bzw. fehlendes Papier legen den Verdacht eines Täuschungsversuches nahe.
7 **Unterschreiben Sie bitte folgende Erklärung:**
Ich versichere, dass ich die Arbeit unter Aufsicht heute selbstständig angefertigt und keine anderen als die mir zur Verfügung gestellten Arbeits- und Hilfsmittel benutzt habe. Mir ist bekannt, dass ordnungswidriges Verhalten oder Täuschungsversuch zum Abbruch des Prüfungsverfahrens führen. Über weitere Folgen entscheidet der Leiter des Prüfungsamtes. Mir ist ferner bekannt, dass die Prüfung wegen eines schwerwiegenden Täuschungsversuchs auch nach Aushändigung des Zeugnisses für nicht bestanden erklärt werden kann.

Seidel
(Unterschrift des Kandidaten / der Kandidatin)

Umschlagseite 2

Erstgutachten gem. § 14 Abs. 3 LPO (ggf. besonderes Blatt)

(,)

Leistungsnote | Datum | Unterschrift

Leistungsnoten: sehr gut (1); gut (2); befriedigend (3); ausreichend (4); mangelhaft (5); ungenügend (6)
Zur differenzierten Bewertung können Zwischenwerte durch Absenken oder Anheben der einzelnen Note um 0,3 gebildet werden. Die Noten 0,7/4,3/4,7/5,3/5,7/6,3 sind dabei ausgeschlossen.

Als Zweitgutachter/in schlage ich vor: _____

Zweitgutachten* gem. § 14 Abs. 3 LPO (ggf. besonderes Blatt)

(,)
Leistungsnote

Datum

Unterschrift

Leistungsnoten: sehr gut (1); gut (2); befriedigend (3); ausreichend (4); mangelhaft (5); ungenügend (6)
Zur differenzierten Bewertung können Zwischenwerte durch Absenken oder Anheben der einzelnen Note um 0,3 gebildet werden. Die Noten 0,7/4,3/4,7/5,3/5,7/6,3 sind dabei ausgeschlossen.

Entscheidung des Landesprüfungsamtes gem. § 14 Abs. LPO:

(,)
Leistungsnote

Datum

Unterschrift

* gem. § 14 LPO ist ein selbständiges Zweitgutachten zu erstellen; eine Gegenzeichnung des Erstgutachtens ist nicht zulässig

Drittgutachten gem. § 14 Abs. 3 LPO (ggf. besonderes Blatt)

Gemäß § 14 Abs. 3 LPO wird auf der Grundlage des obigen Gutachtens im Rahmen der beiden Vornoten folgende Note endgültig festgelegt:

(,)		
Leistungsnote	Datum	Unterschrift

LANDESPRÜFUNGSAMT FÜR ERSTE STAATSPRÜFUNGEN FÜR LEHRÄMTER AN SCHULEN - ESSEN
- Geschäftsstelle Siegen -

Dieses Formular ist bitte von der Themenstellerin/dem Themensteller auszufüllen.

Mitteilung: Thema der schriftlichen Prüfung

rosa

Landesprüfungsamt
für Erste Staatsprüfungen
für Lehrämter an Schulen
Geschäftsstelle Siegen
Hölderlinstr. 3

im Hause

Prüfer/-in: Prof Dr. Skoruppa

Lehramt an: Gym

Kandidat/-in: Seidel Michael
(Name, Vorname)

Schriftliche Prüfung

☒ Unterrichtsfach/berufliche Fachrichtung: Mathematik
☒ Fachwissenschaft ☐ Fachdidaktik
☐ Erziehungswissenschaft
☐ Berufspädagogik
☐ didaktisches Grundlagenfach:
(Fach: Deutsch oder Mathematik)

Aufgabenstellung der schriftlichen Prüfung: (bezogen auf Modul V2)

→ *Besonderheit nur für Fremdsprachen:* Die Anfertigung der Klausur erfolgt in der Zielsprache: ja ☐ nein ☐

Hilfsmittel: — keine Hilfsmittel —
(Hinweis für Themensteller/-in: Falls Hilfsmittel zugelassen werden, bitten wir, dies hier entsprechend zu vermerken und zur Verfügung zu stellen. Andernfalls bitte streichen.)

Siegen, 14-01-2011
(Ort, Datum)

Vit-Peter Skoruppa
(Unterschrift der Themenstellerin/des Themenstellers)

Hinweis für die Aufgabenstellung: Die Aufgaben beziehen sich auf die Inhalte des gesamten Moduls. Die Aufgaben sind so zu stellen, dass bei der Bearbeitung grundlegende Kenntnisse zur Thematik der entsprechenden Lehrangebote und zur Methodik des Faches oder der betreffenden Fächer sowie die Fähigkeit nachgewiesen werden können, Wissen im Sinne der gestellten Aufgabe anzuwenden (§ 14 Abs. 2 LPO).

Dieses Formular wird i.d.R. von der Antragstellerin/dem Antragsteller nach Anmeldung und Zulassung zur schriftlichen Prüfung der Themenstellerin/dem Themensteller vorgelegt. Da eine Anforderung des Klausurthemas durch das Prüfungsamt nicht mehr erfolgt, werden die benannte Prüferin/der benannte Prüfer dringend gebeten, das Thema rechtzeitig dem Prüfungsamt zuzuleiten.
Besonderer Hinweis: Bis auf Weiteres folgt das Landesprüfungsamt dem Wunsch der Hochschule, die Themenanforderungsformulare für die schriftlichen Prüfungen – wie bisher auch – gebündelt an die Prüfenden weiterzuleiten.

Themenvorschläge

Mathematische Grundbegriffe der Datensicherheit

Prüfer: Prof. Dr. N-P. Skoruppa

Bearbeiten Sie die nachstehenden Aufgaben gemäß folgender Anweisung:

1. *Bearbeiten Sie entweder Aufgabe 1 oder Aufgabe 2. Bearbeiten Sie auf keinen Fall beide Aufgaben.*
2. *Wählen Sie frei sechs der Aufgaben 3 bis 11. Bearbeiten Sie auf keinen Fall mehr als sechs dieser Aufgaben.*
3. *Geben Sie zu Beginn Ihrer Reinschrift an, welche der Aufgaben 1 und 2 und welche sechs der übrigen Aufgaben Sie zur Bearbeitung gewählt haben.*

Stellen Sie Ihre Schlussweisen mittels vollständiger und grammatikalisch korrekter Sätze der natürlichen Sprache dar und benutzen Sie auf keinen Fall logische Kürzel wie Äquivalenzpfeile oder Implikationspfeile. Ergänzen Sie Ihre symbolischen Rechnungen durch Kommentare zum logischen Ablauf. Die Klarheit der Darstellung ist Teil der zu benotenden Leistung, und die Bemühung darum wird Ihnen bei Ihren Aufgaben helfen.

Bearbeiten Sie eine der beiden folgenden Aufgaben:

Aufgabe 1. Fertigen Sie einen Aufsatz zum Thema *Asymmetrische Verschlüsselungsverfahren (Public Key Verschlüsselungsverfahren)* an. Geben Sie mindestens zwei Public Key Verschlüsselungsverfahren an und erklären Sie diese mit Beispielen. Erklären Sie die mathematischen Hintergründe dieser Verfahren, und insbesondere, warum sie Asymmetrische Verschlüsselungsverfahren darstellen. Diskutieren sie die Sicherheit dieser Verfahren. Sie sollten mindestens zwei nicht-triviale Aussagen Ihres Aufsatzes beweisen. Der fertige Aufsatz sollte in etwa einem Zeitaufwand von 90 Minuten entsprechen.

Aufgabe 2. Fertigen Sie einen Aufsatz zum Thema *Gewichtszähler eines Codes* an. Dabei erörtern Sie insbesondere die Definition des Gewichtszähler eines Codes mit Beispielen, die MacWilliams Identität und die Struktur des Ringes der Gewichtzähler selbstdualer Codes. Sie sollten mindestens zwei nicht-triviale Aussagen Ihres Aufsatzes beweisen. Der fertige Aufsatz sollte in etwa einem Zeitaufwand von 90 Minuten entsprechen.

Bearbeiten Sie sechs der folgenden Aufgaben:

Aufgabe 3. Sei $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ eine affine Chiffre über dem Alphabet $\Sigma = \mathbb{Z}/26\mathbb{Z}$. Berechnen Sie die Anzahl $|\mathcal{K}|$ der Schlüssel.

Aufgabe 4. Sei $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ eine affine lineare Blockchiffre mit der Blocklänge 3 über dem Alphabet $\Sigma = \{0, 1\}$. Bestimmen Sie die Kardinalität des Schlüsselraums $\mathcal{K}$.

Aufgabe 5. Sei $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ eine Hill-Chiffre der Blocklänge n über dem Alphabet $\Sigma = \mathbb{Z}/m\mathbb{Z}$ $(m \in \mathbb{Z}_{>0})$. Sei $k \in \mathcal{K}$ ein Schlüssel und sei $[m_i, c_i] \in \mathcal{P} \times \mathcal{C}$ $(i = 1, .., l)$ ein Klartext-Chiffretext Paar, wobei $c_i = E_k(m_i)$ gelte. Unter welcher Bedingung an die Matrix $(m_1, ..., m_l)$ kann man den Schlüssel k berechnen? (Wir betrachten die m_i als Spaltenvektoren.)

Aufgabe 6. Sei $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ eine Verschiebungschiffre mit $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}/m\mathbb{Z}$ $(m \in \mathbb{Z}_{>0})$. Wir nehmen an, dass die Wahrscheinlichkeitsverteilung $\mu_{\mathcal{K}}$ eine Gleichverteilung ist. Beweisen Sie, dass dieses Kryptosystem perfekt sicher ist.

Aufgabe 7. Sei $\mathcal{C}$ der ISBN-13 Code, d.h.

$$\mathcal{C} := \{(c_1, ..., c_{13}) \in \mathcal{A}^{13} \mid \sum_{i=0}^{6} c_{2i+1} + 3\sum_{i=1}^{6} c_{2i} \equiv 0 \mod 10\}$$

wobei $\mathcal{A} = \{0, 1, ..., 9\}$ ist. Berechnen Sie die Informationsrate, den Minimalabstand und den relativen Minimalabstand von $\mathcal{C}$.

Aufgabe 8. Wir betrachten den Hamming-Code

$$H_7 = \left\{ c \in {\mathbb{F}_2}^7 \mid \begin{pmatrix} 1&0&0&1&1&0&1 \\ 0&1&0&1&0&1&1 \\ 0&0&1&0&1&1&1 \end{pmatrix} c^t = (0,0,0)^t \right\}$$

Beweisen Sie, dass H_7 ein perfekter Code ist. Dekodieren Sie das empfangene Wort $(1, 0, 1, 0, 1, 0, 1)$.

Aufgabe 9. Bestimmen Sie alle Maximum-Distanz-Codes (MDS-Codes oder im Englischen Maximum Distance Separable Codes) in ${\mathbb{F}_2}^4$.

Aufgabe 10. Sei $\mathcal{C} \subseteq {\mathbb{F}_2}^6$ ein 1-Fehler-Korrigierender Code. Zeigen Sie, dass $|\mathcal{C}| \leq 9$.

Aufgabe 11. Sei $\mathcal{C} \subseteq \mathbb{F}_2^{2n}$ ein binärer selbstdualer Code der Länge $2n$. Beweisen Sie, dass $\mathcal{C}$ das Codewort $(1, 1, ..., 1)$ enthält.

Reinschrift

Landesprüfungsamt für Erste Staatsprüfungen für Lehrämter an Schulen

Sickel, Michael
(Name, Vorname)

Ausgewählte Aufgaben:
- Aufgabe 1

- Aufgabe 5
- Aufgabe 7
- Aufgabe 8
- Aufgabe 9
- Aufgabe 10
- Aufgabe 13

Aufgabe 1:

Public-Key-Verschlüsselungsverfahren heißen so, da der Verschlüsselungsschlüssel öffentlich ist. Der Entschlüsselungs-Schlüssel läßt sich nicht leicht aus dem Verschlüsselungsschlüssel berechnen. Beispiele solcher Verschlüsselungen sind RSA- und ElGamal-Verfahren. Zunächst werde ich auf RSA eingehen, indem ich den Ablauf und die Funktionsweise beschreibe.

Zunächst wählt man zwei sehr große Primzahlen p und q. Dann bildet man $n := p \cdot q$. Weiter wird ein zufälliges e aus $\left(\mathbb{Z}/\varphi(n)\mathbb{Z}\right)^*$ gewählt.

(n, e) ist der öffentliche Schlüssel, mit dem man einen Klartext verschlüsseln kann. Dabei ist

$$c = m^e \bmod n.$$

Der geheime Entschlüsselungs-Schlüssel $(\varphi(n), d)$ beinhaltet ein d für das gilt

$$e \cdot d \equiv 1 \bmod \varphi(n).$$

Da e aus $(\mathbb{Z}/\varphi(n)\mathbb{Z})^*$, also invertierbar ist, kann man

$$d \equiv e^{-1} \bmod \varphi(n)$$

berechnen.

Es gilt $c^d \equiv (m^e)^d \equiv m^{ed} \equiv m \bmod n$. Auf diese weise lässt sich der empfangene Text entschlüsseln.

Dies geht jedoch nur mittels des Private-Keys $(\varphi(n), d)$, der nicht bekannt sein sollte.

$\varphi(n) = \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1)$ und damit nur berechenbar, wenn man n faktorisieren kann. Dafür gibt es jedoch keine ausreichend effizienten Verfahren, so dass bei genügend großen Zahlen p und q $\varphi(n)$ nicht berechnet werden kann. Dadurch lässt sich auch $d \equiv e^{-1} \bmod \varphi(n)$ nicht bestimmen.

Reinschrift

Landesprüfungsamt für Erste Staatsprüfungen für Lehrämter an Schulen

Seidel, Michael
(Name, Vorname)

Wählen wir $n = p \cdot q = 5 \cdot 7 = 35$. Dann ist $\varphi(35) = (5-1) \cdot (7-1) = 4 \cdot 6 = 24$. Darüber hinaus sei $e = \bar{5}$. $e \in (\mathbb{Z}/\varphi(n)\mathbb{Z})^*$, da $\text{ggT}(5, 24) = 1$ ist.

Wir verschlüsseln einen Klartext $m = 2$, indem wir $c \equiv m^e \bmod n$ berechnen. Also $c \equiv 2^5 \equiv 32 \bmod n$.

$d \equiv e^{-1} \bmod \varphi(n)$ berechnungsweise $ed \equiv 1 \bmod \varphi(n)$. Damit also $5 \cdot d \equiv 1 \bmod 24$. Mit dem erweiterten Euklidischen Algorithmus lässt sich d bestimmen. Hier sieht man, dass für $d = \bar{5}$ gilt $\bar{5} \cdot \bar{5} \equiv 1 \bmod 24$.

Aus dem Chiffretext c können wir also m gewinnen, indem wir $m \equiv c^d \bmod n$ berechnen. Also $(2^5)^5 \equiv 2^{25} \equiv 2^{24} \cdot 2 \equiv 2 \bmod 35$. Dabei ist zu beachten, dass nach dem kleinen Satz von Fermat $2^{24} \equiv 1 \bmod 35$ ist.

Das ElGamal-Kryptosystem benutzt den Diffie-Hellmann-Schlüsselaustausch. Zu einer Primitivwurzel g wählen Alice und Bob jeweils eine Zahl a respektive b und

bilden damit $\alpha \equiv g^a \bmod p$ und $\beta \equiv g^b$ jeweils modulo einer Primzahl p, für die g eine Primitivwurzel ist.
α und β können über einen öffentlichen Kanal versendet werden. Der Schlüssel wird von Alice und Bob durch die Berechnung von

$$k = \alpha^b \equiv (g^a)^b \equiv g^{ab} \equiv (g^b)^a \equiv \beta^a \bmod p$$

gebildet. Ein Angreifer kennt weder a noch b. Eine Berechnung wäre nur möglich, wenn man den Diskreten Logarithmus effizient berechnen könnte. Dafür sind jedoch keine Verfahren bekannt.

Ein Klartext m wird verschlüsselt, indem man $c \equiv m \cdot k \bmod p$ berechnet. Dieser lässt sich wieder entschlüsseln durch

$$c \cdot k^{-1} \equiv m \cdot k \cdot k^{-1} \equiv m \bmod p.$$

Seien $p = 11$, $a = 2$, $b = 3$ und $g = 5$.
Dann ist $\alpha = 5^2 \equiv 3 \bmod 11$
und $\beta = 5^3 \equiv 4 \bmod 11$. Der gemeinsame Schlüssel ist entsprechend

$$k = \underbrace{\alpha^3}_{3^3=27} \equiv \underbrace{\beta^2}_{4^2=16} \equiv 5 \bmod 11.$$

Reinschrift

Landesprüfungsamt für Erste Staatsprüfungen für Lehrämter an Schulen

Seidel, Michael
(Name, Vorname)

Ein Klartext $m = 2$ wird damit verschlüsselt durch $c \equiv m \cdot k \equiv 2 \cdot 5 \bmod 11$.

Der erweiterte Euklidische Algorithmus liefert als Lösung von
$5k \cdot k^{-1} \equiv 1 \bmod 11$
entsprechend $k^{-1} \equiv 9 \bmod 11$.

$$\left[\begin{array}{l} 5 \cdot k^{-1} + 11y = 1 \\ 11 = 2 \cdot 5 + 1 \qquad 1 = 11 - 2 \cdot 5 \\ 5 = 5 \cdot 1 + 0 \end{array}\right]$$

Damit lässt sich c entschlüsseln durch $10 \cdot 9 \equiv 2 \bmod 11$.

Die Sicherheit der Verfahren beruht im Wesentlichen auf der Tatsache, dass eine Einwegfunktion nicht umgekehrt werden kann. Sobald sich jedoch passende Algorithmen finden sollten, oder die Rechenleistung für eine brute-force-Methode ausreichen sollte, Stichwort Quanten-Computer, sind die Verfahren nicht mehr sicher. Dann müsste man auf andere Gruppen ausweichen. Denkbar sind elliptische Kurven in der projektiven Ebene, oder auch Zopfgruppen.

Aufgabe 5:

Die Hill-Chiffre ist eine spezielle Form einer Affinen linearen Block-Chiffre, bei der gilt:

$$C = M \cdot K$$

wo M die m Matrix $(m_1, \ldots, m_e)$ und K die Verschlüsselungsmatrix darstellen. Die Matrix K lässt sich aus gegebenem C und M berechnen mit

$$M^{-1} C = M^{-1} M K = K.$$

Dies ist jedoch nur möglich, wenn M^{-1} existiert. Eine Matrix ist genau dann invertierbar, wenn ihre Determinante invertierbar ist. Hier lässt sich K also genau dann berechnen, wenn $(\det(M))^{-1}$ existiert.

Reinschrift

Landesprüfungsamt für Erste Staatsprüfungen für Lehrämter an Schulen

Seidel, Michael
(Name, Vorname)

Aufgabe 8:

$H_7 \subset \mathbb{F}_2^7$ und H_7 hat den Minimalabstand 3. Damit ist H_7 dann $t = \left\lfloor \frac{d-1}{2} \right\rfloor = 1$ Fehler-korrigierend. H_7 ist ein $[7,4,3]$ Code.

$$|\mathbb{F}_2^7| = 2^7 = |C| \cdot |B_t| = 2^4 \left(\binom{7}{0} + \binom{7}{1} \right) = 2^4 \cdot 2^3 = 2^7$$

wobei $B_t(c)$ der Ball um das Codewort c mit Radius t ist.

H_7 ist also perfekt, da die $\bigcup_{c \in C} B_t(c)$ (disjunkt) eine Überdeckung von $\mathbb{F}_2^7$ ist.

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \cdot (1,0,1,0,1,0,1)^t = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

Da H_7 1-Fehler-korrigierend ist und das Ergebnis der siebten Spalte der Kontrollmatrix entspricht, ergibt sich ein Syndrom $s = (0,0,0,0,0,0,1)^t$ als Fehlervektor.

$c + e$ ist das dekodierte Wort $(1,0,1,0,1,0,0)^t$.

Aufgabe 10:

$C \subseteq \mathbb{F}_2^6$ und 1-Fehler-korrigierend.

$|C| \cdot |B_{4,1}| \leq 2^6$ und damit gilt dann
$|C| \cdot \left(\binom{6}{0} + \binom{6}{1}\right) \leq 2^6$ also auch
$|C| \cdot 7 \leq 2^6$ also auch
$|C| \leq \frac{64}{7}$.

$|C|$ ist eine natürliche Zahl.
Damit ist insgesamt $|C| \leq 9$. ☒

Aufgabe 7:

$$C := \left\{ (c_1, \ldots, c_{13}) \in \mathbb{A}^{13} \mid \sum_{i=0}^{6} c_{2i+1} + 3 \sum_{i=1}^{6} c_{2i} \equiv 0 \bmod 10 \right\}$$

$$c_{13} \equiv \sum_{i=0}^{5} c_{2i+1} + 3 \sum_{i=1}^{6} c_{2i} \bmod 10.$$

Also $\dim(C) = 12$ und damit $R_C = \frac{12}{13}$.
Es lassen sich Codewörter a, b finden, so dass $d(a,b) = 2$, also gilt $d_C \leq 2$.
[Seien $a = (0,0,0,0,0,0,0,0,0,0,0,0,0)$ und $b = (1,3,0,0,0,0,0,0,0,0,0,0,0)$]
Bleibt zu zeigen, dass es keine Codewörter p, q gibt mit $d(p,q) = 1$.
Verfälscht wird eine Ziffer mit geradem oder ungeradem Index.

Reinschrift

Landesprüfungsamt für Erste Staatsprüfungen für Lehrämter an Schulen

Seidel, Michael
(Name, Vorname)

Es gibt jedoch keine Abweichung e, so dass $1 \cdot e \equiv 0 \bmod 10$ oder $3 \cdot e \equiv 0 \bmod 10$, da $ggT(1,10) = ggT(3,10) = 1$. und $e < 10$.

Also gilt $1 < d_c \leq 2$ und damit $d_c = 2$.

$$\delta_c = \frac{d}{n} = \frac{2}{13}$$

Aufgabe 9:

$$R_c + \delta_c = 1 + \frac{1}{n}$$ (Gleichheit bei der Singleton-Schranke)

ist die Bedingung für einen MDS-Code. Also gilt:

$$\dim C + d_c = n + 1.$$

Daraus ergibt sich für $C \leq \mathbb{F}_2^4$, dass C ein $[n, n-d+1, d]_2$ sein kann.

Konkret also ein $[4,4,1]_2$- oder ein $[4,3,2]_2$- oder ein $[4,2,3]_2$- oder ein $[4,1,4]_2$- Code.

Aufgabe 3:

Bei der affinen Chiffre besteht der Schlüssel hier aus zwei Teilen $a, b \in (\mathbb{Z}/26\mathbb{Z})^*$ wobei $a \in (\mathbb{Z}/26\mathbb{Z})^*$ und $b \in (\mathbb{Z}/26\mathbb{Z})$ ist.

$$E_{(a,b)}(x) = ax + b$$

$$D_{(a,b)}(y) = a^{-1}(y - b)$$

a muss also invertierbar sein.

$$|K| = |(a,b)| = \left|(\mathbb{Z}/26\mathbb{Z})^* \times (\mathbb{Z}/26\mathbb{Z})\right|$$

Also $|K| = \varphi(26) \cdot 26 = \varphi(2) \cdot \varphi(13) \cdot 26$ und damit $|K| = 1 \cdot 12 \cdot 26 = \underline{312}$.

Seidel

$$R_c + \delta_c = 1 + \frac{1}{4}$$

$\dim C + d_c = n + 1$

$[n, n-d+1, \cancel{n=}(n-d+1)+1]$

$[n, n-d+1, d]$

$[4, 4, 1]$

$[4, 3, 2]$

$[4, 2, 3]$

$[4, 1, 4]$