ZUNAME: .....

VORNAME: .....

MAT. NR.: .....

Prüfung 389.153 B
Datenkommunikation

Institute of Telecommunications
Görtz, Goiser, Hlawatsch, Matz, Mecklenbräuker, Rupp, Zseby
TU-Wien 05.04.2016

Bitte beachten Sie:

- Die Dauer dieser Klausur beträgt **zwei Zeitstunden**.
- Bitte legen Sie Ihren **Studierendenausweis auf Ihrem Tisch** zur Überprüfung bereit.
- **Mobiltelefone** müssen während der Prüfung **ausgeschaltet** sein und dürfen **nicht auf dem Tisch** liegen!
- Es sind (außer Schreibwerkzeugen) **keine Hilfsmittel** erlaubt, auch keine Taschenrechner!
- **Wichtig:** Bitte beachten Sie, dass Schummeln, wie z.B. die Verwendung nicht erlaubter Hilfsmittel, studienrechtliche und prüfungsrelevante Konsequenzen hat.
- Bitte verwenden Sie einen **permanent färbenden, nicht-roten Stift**.
- Die Beispiele sind ausschließlich auf den Seiten dieser Angabe auszuarbeiten. **Mitgebrachte Zusatzblätter werden ignoriert!**
- Sofern weitere Leerseiten zur Bearbeitung der Beispiele benötigt werden, sind diese bei der Klausuraufsicht erhältlich.
- Bitte bearbeiten Sie ***nicht*** **mehr als ein Beispiel auf einem Blatt**.
- Bitte kennzeichnen Sie auf **jeder Seite** eindeutig, welche **Aufgabe** und welcher **Unterpunkt** behandelt wird.
- Schreiben Sie auf **jedes Blatt** Ihren **Namen** und Ihre **Matrikelnummer**!
- Diese **Angabe *muss*, mit Ihrem Namen und Ihrer Matrikelnummer beschriftet,** bei der Klausuraufsicht **abgegeben werden**. **Sie dürfen diese Angabe *nicht* mitnehmen!**
- Sofern Sie nicht wollen, dass Ihre Bearbeitung eines Beispiels gewertet wird, streichen Sie die entsprechenden Seiten klar ersichtlich durch.
- Eine **lesbare Schrift und übersichtliche Darstellung** sind Voraussetzungen für die positive Beurteilung der Arbeit!
- Bitte **bleiben Sie bei Klausurende** so lange **auf Ihrem Platz**, bis alle Klausuren eingesammelt sind und die Klausuraufsicht die Freigabe zum Verlassen der Hörsaals erteilt.
- Sofern Sie während der Klausur zur Toilette müssen, melden Sie sich bitte rechtzeitig bei der Klausuraufsicht. Bitte **verlassen Sie nicht ohne Rücksprache mit der Klausuraufsicht den Hörsaal**.
- Sofern Sie vor dem Klausurende gehen wollen, tun Sie dies bitte **nicht in den letzten 15min** vor dem Ende der Klausur. Melden Sie sich bevor Sie gehen bei der Klausuraufsicht und geben Sie Ihre Angabe ab.

Aufgabe:	1	2	3	Summe
Punkte (max.):	34	33	33	100
Punkte:				

Zuname:..... **Matrikelnummer:.....**

Aufgabe 1: (34 Punkte)

Eindimensionale Betrachtung: Von einem satellitengestützten Positionsbestimmungssystem ist folgendes bekannt: (1) Das Satellitensignal wird aus dem Generatorpolynom $p(x) = x^4 + x + 1$ erzeugt, (2) die Pulsform der Chips sind NRZ-Pulse, (3) die Synchronisationsgenauigkeit liegt unter 10% der Chipdauer.

(a) (7 Punkte) Zeichnen Sie die Schieberegisterrealisierung des Generatorpolynoms.

(b) (7 Punkte) Bestimmen Sie die binäre Folge.

(c) (7 Punkte) Bestimmen Sie die periodische Autokorrelationsfunktion der Folge.

(d) (7 Punkte) Ist die Autokorrelationsfunktion geeignet zur Positionsbestimmung? Wenn ja, warum?

(e) (6 Punkte) Wählen Sie eine Chiprate, sodass die eindimensionale Genauigkeit unter 15 Meter bleibt. Annahme: Ideale Ausbreitungsverhältnisse.

Hinweis: Der NRZ (no-return-to-zero) Puls entspricht einer rechteckigen Kurvenform.

Zuname:..... **Matrikelnummer:.....**

Zuname:..... **Matrikelnummer:.....**

Zuname:..... **Matrikelnummer:.....**

Zuname:..... **Matrikelnummer:.....**

Aufgabe 2: (33 Punkte)

Die Batterie eines Handys entlade sich pro Tag um die Hälfte. Alle drei Tage ($k = 3, 6, 9, ...$) werde das Handy um Mitternacht mit 1Ah aufgeladen. Am Tag 0 sei es mit 0.5Ah nur etwa mittel voll geladen.

Hinweise:

$$\sum_{n=0}^{\infty} z^{-n} = \frac{1}{1 - z^{-1}} = \frac{z}{z-1}$$

$$\cos(x) = \frac{\exp(jx) + \exp(-jx)}{2}$$

$$\sin(x) = \frac{\exp(jx) - \exp(-jx)}{2j}$$

Für jeden Wert $|z| < 1$ erhält man einen endlichen Wert!

(a) (5 Punkte) Gib eine Zeitreihe für die ersten 9 Tage an, die den Batteriefüllstand des Handys $y(k)$ um 23:59Uhr des Tages $k = 0, 1, ..., 9$ angibt.

(b) (5 Punkte) Gib die Füllstände nach unendlich langer Zeit ($l \to \infty$) an für Tage $k = 3l - 2$ und Tage $k = 3l$.

(c) (6 Punkte) Stelle eine rekursive Gleichung im Zeitbereich für den Füllstand der Handybatterie $y(k)$ am jeweiligen Abend um 23:59Uhr des Tages k in der Einheit Ah dazu auf.

(d) (5 Punkte) Gib die zugehörige Gleichung im Z-Bereich an.

(e) (2 Punkte) Berechne nun einen Ausdruck für $Y(z)$, der Z-Transformierten von $y(k)$ in der Form:

$$Y(z) = \frac{Az}{z - \frac{1}{2}} + \frac{Bz}{z-1} + \frac{Cz^2 + Dz + E}{z^2 + z + 1}.$$

Berechne E explizit. Gib ein Bestimmungsgleichungssystem für A, B, C und D an. (Es ist nicht erforderlich A, B, C, D explizit auszurechnen!)

(f) (4 Punkte) Gib die beiden Rücktransformierten zu den Teilen mit A und B an.

(g) (2 Punkte) Betrachte nun den dritten Anteil. Wie lautet die Rücktransformierte zu

$$\frac{z^2}{z^2 + z + 1}?$$

(h) (2 Punkte) Erläutere den prinzipiellen Zeitverlauf der beiden Anteile aus (f) und des Anteils aus (g).

(i) (2 Punkte) Welches sind die kleinsten und größten Ladezustände, welche die Batterie in diesen Ladezyklen jemals einnehmen kann?

Zuname:..... **Matrikelnummer:.....**

Zuname:..... **Matrikelnummer:.....**

Zuname:..... **Matrikelnummer:.....**

Zuname:..... **Matrikelnummer:.....**

Aufgabe 3: (33 Punkte)

Alice möchte mittels **RSA** Verfahren mit Bob verschlüsselt kommunizieren. Dazu denkt sie sich zwei Zahlen $p = 3$, $q = 13$ aus und berechnet $n = p \cdot q = 39$.

Anmerkung: In der Aufgabe soll nur die *reine RSA Trapdoorfunktion* angewendet werden (ohne die in der Praxis verwendete Hashfunktion). In der Praxis müssen zudem wesentlich grössere Zahlen für p und q verwendet werden.

(a) (3 Punkte) Berechnen Sie $\varphi(n)$ mit den von Alice gewählten Zahlen (Formel und Berechnung).

(b) (7 Punkte) Alice wählt $e = 5$ als öffentlichen Schlüssel. Bestimmen Sie den zugehörigen **geheimen** Schlüssel d.

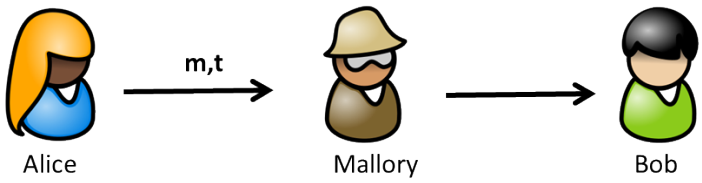
(c) (7 Punkte) Bob möchte eine verschlüsselte Nachricht an Alice senden. Dazu setzt er Buchstaben Ziffern gleich ($A = 1, B = 2, \ldots, Z = 26$) und sendet jeweils pro Buchstaben eine separaten Nachricht. Wie berechnet Bob die verschlüsselten Nachrichten für den Text *D A D*? (Formel und Berechnungen)

(d) (4 Punkte) Was passiert bei dem hier verwendetem einfachen RSA Verfahren (Nutzung der reinen RSA Trapdoorfunktion) mit der Nachricht, wenn ein Man-in-the-Middle Angreifer den erste verschlüsselten Wert c (Ciphertext für den ersten Buchstaben) jeweils mit einem Faktor 0.5^e multipliziert und diese dann an den Empfänger weiterleitet?

$c' = 0.5^e \cdot c$ $\quad m' =$ _____

(e) (4 Punkte) Alice möchte die Nachricht $m = 14$ signieren. Wie berechnet Alice die Signatur *sig*? (Formel und Berechnung)

(f) (4 Punkte) Alice möchte statt der RSA Signatur einen einfachen Message Authentication Code (MAC) verwenden, um die Integrität der Nachricht gegen einen Man-in-the-Middle Angreifer schützen. Sie überlegt eine einfache CRC Berechnung über die Nachricht als MAC zu verwenden. Kann Sie damit die Nachricht gegen einen Angreifer schützen? Begründen Sie Ihre Antwort.



t=CRC(m)

(g) (4 Punkte) Erläutern Sie den Unterschied zwischen einem Message Authentication Code (MAC) und einer digitalen Signatur.

Zuname:..... **Matrikelnummer:.....**

Zuname:..... **Matrikelnummer:.....**

Zuname:..... **Matrikelnummer:.....**

Zuname:..... **Matrikelnummer:.....**