ZUNAME: .....

VORNAME: .....

MAT. NR.: .....

Prüfung 389.153 B
Datenkommunikation

Institute of Telecommunications
Görtz, Goiser, Hlawatsch, Matz, Mecklenbräuker, Rupp, Zseby
TU-Wien 24.11.2015

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.):	32	33	35	100
Punkte:				

Aufgabe 1: (32 Punkte)

Ein Öltank mit Fassungsvermögen 4Mio Liter sei am Tag 0 halbvoll. Zu Mitternacht wird der Tagesverbrauch festgestellt: es werden täglich 50 Prozent seines Volumens abgelassen. Um dies zu kompensieren werden, werden alle zwei Tage (k=2,4,6...) 600.000 Liter nachgefüllt.

Hinweis:

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

$$\sum_{n=0}^{\infty} (-z)^{-n} = \frac{1}{1+z^{-1}} = \frac{z}{z+1} = V(z)$$

(a) (3 Punkte) Gib eine Zeitreihe für die ersten 10 Tage an, die den Füllstand $y(k)$ um 23:59Uhr des Tages $k = 0, 1, ..., 10$ angibt.

(b) (3 Punkte) Gib die Füllstände nach unendlich langer Zeit an. Unterscheide gerade und ungerade Tage.

(c) (5 Punkte) Stelle eine rekursive Gleichung im Zeitbereich für den Füllstand des Speichers $y(k)$ am jeweiligen Abend um 23:59Uhr des Tages k in der Einheit Mio. Liter dazu auf.

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

(e) (4 Punkte) Berechne nun einen Ausdruck für Y(z), der Z-Transformierten von $y(k)$.

(f) (5 Punkte) Berechne in Folge die Rücktransformierte $y(k)$. Hierzu muss man den Ausdruck

$$\frac{z^3}{(z-\frac{1}{2})(z-1)(z+1)} = \frac{Az}{z-\frac{1}{2}} + \frac{Bz}{z-1} + \frac{Cz}{z+1}$$

für A, B, C lösen. *Falls es nicht gelingt, kann man auch mit* $A = -1/4, B = 1, C = 1/3$ *weiterrechnen.*

(g) (3 Punkte) Gib einen Signalflussgraphen dazu an, der als Eingang den Anfangsfüllstand und als Ausgang $Y(z)$ enthält.

Berechne nun folgende Aufgaben:

(h) (1 Punkte) Nach wie vielen Tagen sinkt der Speicherstand zum ersten Mal unter die Hälfte?

(i) (3 Punkte) Kann der Speicherstand unter 10% sinken? Erkläre deine Antwort anhand der analytischen Lösung für $y(k)$

Aufgabe 2: (33 Punkte)

An der Stelle, an der sich die Trainingssequenz befindet, wird in einem WLAN Empfänger die Datenfolge:

```
+3 -1 +1 -1 -3 +1 +3 +3 -1 +1
```

empfangen. Die verwendete Trainingssequenz zur Kanalschätzung basiert auf der binären Folge

```
1 0 1 1 0 0 0
```

und diese wird periodisch fortgesetzt.

(a) (7 Punkte) Der Korrelator verwendet nicht direkt die oben angegebene binäre Trainingssequenz, sondern die binären Werte werden zuerst auf die beiden reellen Werte -1, +1 abgebildet. Wie lautet die Abbildung und wie lautet die resultierende Trainingsfolge?

(b) (8 Punkte) Bestimmen Sie die Korrelationsfolge y_n.

(c) (9 Punkte) Wieviele Ausbreitungspfade sind signifikant? Hinweis: kleine Korrelationswerte und negative Korrelationswerte bedeuten, dass kein signifikanter Pfad vorliegt.

(d) (9 Punkte) Entwerfen Sie ein einfaches Blockdiagramm, dass die arithmetischen Operationen des Korrelators implementiert. Ihr Blockdiagramm nimmt die Datenfolge x_n am Eingang und bildet daraus die Korrelationsfolge y_n. (Sie brauchen nicht mit einzelnen bits zu rechnen, sondern dürfen einen Block [+] zur Addition zweier Zahlen als Baustein verwenden und einen Block, der das Vorzeichen wechselt.)

Aufgabe 3: (35 Punkte)

Alice möchte mittels **RSA** Verfahren mit Bob verschlüsselt kommunizieren. Dazu denkt sie sich zwei Primzahlen $p = 3, q = 17$ aus und berechnet $n = p \cdot q = 51$.

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 p, q verwendet werden.

(a) (2 Punkte) Hätte Alice auch die Zahlen 18 und 4 auswählen können, um ein geeignetes n zu berechnen? Begründen Sie Ihre Antwort.

(b) (2 Punkte) Was genau berechnet die eulersche Phi-Funktion $\varphi(n)$?

(c) (4 Punkte) Berechnen Sie $\varphi(n)$ mit den von Alice gewählten Zahlen (Formel und Berechnung).

(d) (4 Punkte) In welcher Beziehung müssen die Zahlen e und d (die beiden Schlüssel) stehen, damit das RSA Verfahren funktioniert? (Formel)

(e) (5 Punkte) Alice wählt $d = 3$ als geheimen Schlüssel. Bestimmen Sie den zugehörigen **öffentlichen** Schlüssel e.

(f) (4 Punkte) Warum kann ein Angreifer (Eve) den **geheimen** Schlüssel d nicht berechnen?

(g) (4 Punkte) Kreuzen Sie an (x) welche Zahlen Alice **öffentlich** bekannt gibt, damit das RSA Verfahren angewendet werden kann.

Zahl	d	e	q	p	$\varphi(n)$	n
öffentlich?						

(h) (5 Punkte) Alice bekommt von Bob eine verschlüsselte Nachricht $c = 4$. Wie berechnet sie daraus die unverschlüsselte Nachricht m? (Formel und Berechnung)

(i) (5 Punkte) Alice möchte die Nachricht $m = 5$ signieren. Wie berechnet Alice die Signatur *sig*? (Formel und Berechnung)