Übung 1

Abgabe: 18.10.2018 **bis** 12:15 Uhr

1. Regeln & Organisatorisches

Durch das Lösen der Übungsaufgaben können Sie sich bis zu **10% Bonus** für Ihre Klausur erarbeiten. Diese Punkte werden Ihnen angerechnet, sobald Sie mehr als 49% in der Klausur erreicht haben. Gleichzeitig stellt das Bearbeiten der Übungsaufgaben eine **ideale Klausurvorbereitung** für Sie dar. Um einen reibungslosen Ablauf zu gewährleisten, **beachten Sie bitte die folgenden Regeln:**

- **Täuschungsversuche führen zu einer Bewertung mit 0 Punkten bei allen Beteiligten.** Im Wiederholungsfall behalten wir uns vor, Ihnen sämtliche Bonuspunkte für die Klausur zu streichen.
- **Zu spät abgegebene Übungsaufgaben können leider nicht gewertet werden**. Bei Krankheit o. ä. kontaktieren Sie bitte den Übungsleiter.
- Die Lösungen können **alleine oder in Zweiergruppen** abgegeben werden. Wenn Sie die Übungslösungen zu zweit abgeben, müssen Sie auch den **Namen und die Matrikelnummer Ihres Teampartners sowie Ihre Gruppennummer** auf dem Zettel angeben. **Eine Abgabe pro Gruppe ist ausreichend.**
- Falls Sie sich für die **Abgabe in einer Zweiergruppe** entscheiden, **wählen Sie bitte bis zum 25.10.18 gemeinsam mit Ihrem Teampartner eine Gruppe in Moodle aus.**
- Die Abgabe der Lösungen sollte aus didaktischen Gründen **handschriftlich** erfolgen. Sie können jedoch auch die in Moodle verfügbare LaTeX-Vorlage verwenden.
- Die Abgaben müssen im **PDF-Format** (also eingescannt, falls die Lösung handschriftlich vorliegt) in Moodle hochgeladen werden. Abgabetermin ist in der Regel vor der Vorlesung.
- Ihre Abgaben sollten **ohne weitere Bearbeitung seitens der Korrekteure korrigierbar sein.** Das bedeutet insbesondere, dass die Seiten nicht auf dem Kopf stehen oder nur ein kleiner Teil des sichtbaren Bereichs Ihre Abgabe enthält. Bei Abgaben, die zusätzliche Arbeit verursachen, behalten wir uns einen Punktabzug vor.
- Die korrigierten Abgaben werden ebenfalls in Moodle einsehbar sein.
- Die Verwendung von Computerprogrammen und Internet-Recherche ist prinzipiell erlaubt, muss aber als solche gekennzeichnet werden (Quellenangabe).
- **Eine aktive Diskussion zu den entsprechenden Übungsaufgaben in Moodle ist explizit erwünscht.** Bei Bedarf werden auch Fragen vom Korrekturteam und vom Übungsleiter beantwortet.

2. Angriff auf eine Substitutionschiffre 50 Punkte

Im Übungsverzeichnis befindet sich ein verschlüsselter Text in der Datei "chiffrat.txt“, der mit der Substitutionschiffre verschlüsselt wurde. Ziel dieser Aufgabe ist es, den Klartext wiederzugewinnen, d.h. das Chiffrat zu entschlüsseln. Gehen Sie dabei wie folgt vor:

a) Geben Sie die absoluten und relativen Häufigkeiten der Buchstaben `A` bis `Z` sowie `Ä`, `Ö`, `Ü`, und ß des Chiffrates an, runden Sie dabei ggf. auf 2 Nachkommastellen und ignorieren Sie alle anderen Zeichen (Leerzeichen, Kommata, ...). (10 Pkt.)

b) Entschlüsseln Sie die Datei „chiffrat.txt“ aus dem Übungsverzeichnis und schreiben Sie **nur** die erste Strophe auf ihre Lösung.
Hinweis: Es handelt sich um einen deutschen Text. (20 Pkt.)

Buchstabe	Häufigkeit	Buchstabe	Häufigkeit	Buchstabe	Häufigkeit	Buchstabe	Häufigkeit
`A`	5,58	`J`	0.24	`S`	6.42	`Ä`	0.54
`B`	1.96	`K`	1.32	`T`	5.79	`Ö`	0.30
`C`	3.16	`L`	3.60	`U`	3.83	`Ü`	0.65
`D`	4,98	`M`	2.55	`V`	0.84	ß	0.37
`E`	16,93	`N`	10.53	`W`	1.78		
`F`	1.49	`O`	2.24	`X`	0.05		
`G`	3.02	`P`	0.67	`Y`	0.05		
`H`	4.98	`Q`	0.02	`Z`	1.21		
`I`	8.02	`R`	6.89				

Tabelle 1: Buchstabenhäufigkeit der deutschen Sprache

c) Geben Sie die verwendete Substitutionstabelle für die Verschlüsselung an. (10 Pkt.)

d) Wie groß ist der Schlüsselraum für diese Substitutionschiffre das vorliegende Alphabet? (Hinweis: ein „Schlüssel“ ist in diesem Fall eine Substitutionstabelle) (5 Pkt.)

e) Wie heißt der vorliegende Text?
In welchem Jahr ist der Text erschienen? (5 Pkt.)

Hinweise:

- Es ist sinnvoll den Text elektronisch zu verarbeiten, z.B. um die Buchstabenhäufigkeit zu ermitteln oder die Substitution vorzunehmen.
- Die Entschlüsselung ist auch per Hand möglich. Es empfiehlt sich hierbei, Kleinbuchstaben für den Klartext und Großbuchstaben für das Chiffrat zu verwenden.
- Die Tabelle gibt nur eine statistische Häufigkeit wieder und weicht in der Praxis oft ab.

3. Exponentielles Wachstum 15 Punkte

Bei einer vollständigen Schlüsselsuche (dem sogenannten Brute-Force-Angriff) wird der gesamte Schlüsselraum einer Chiffre durchsucht, d. h. alle möglichen Schlüssel werden getestet. Um Sicherheit gegen diesen Angriff zu bieten, muss der Schlüsselraum einer jeden Chiffre ausreichend groß

sein. Ein zentrale Beobachtung hierbei ist, dass der Schlüsselraum **exponentiell** mit der Schlüssellänge anwächst. In dieser Aufgabe versuchen wir ein Gefühl für exponentielles Wachstum zu bekommen.

Einer bekannten Anekdote nach soll der Erfinders des Schachspiels auf Nachfrage des König um eine „bescheidene“ Belohnung in Form von Reiskörnern gebeten haben. Auf dem ersten Schachfeld solle ein Korn liegen, auf dem zweiten zwei Körner, auf dem dritten vier Körner usw.

a) Wie viele Körner liegen auf dem letzten Schachfeld? (2,5 Pkt.)

b) Ein Reiskorn wiegt ca. 0,03g. Wie schwer sind die Körner auf dem letzten Schachbrett in Summe? Setzen Sie das Ergebnis ins Verhältnis zu der jährlichen Weltreisernte von etwa 460 Millionen Tonnen. (2,5 Pkt.)

Wir betrachten nun ein Blatt Papier, welches wiederholt gefaltet wird. Die Dicke des gefalteten Papiers wächst hierbei exponentiell an: Wird das Blatt einmal gefaltet, erhält man die doppelte Papierdicke, beim zweimaligen Falten die vierfache usw. Die ursprüngliche Dicke eines Blatts betrage 0,1 mm.

c) Wie dick ist das Papier nach 10-maligem Falten? (2,5 Pkt.)

d) Wie oft müsste man das Papier falten, damit es 1 km dick ist? (2,5 Pkt.)

e) Wie oft müsste man das Papier falten, damit es von der Erde bis zum Mond reicht (Entfernung: 384.400 km)? (2,5 Pkt.)

f) Wie oft müsste man das Papier falten, damit es ein Lichtjahr dick ist, d.h. 9460730472580,8 km? (2,5 Pkt.)

Bemerkung: In der Praxis kann ein Blatt Papier natürlich nicht so oft gefaltet werden, wie es in den obigen Beispielen berechnet wurde.

4. Brute-Force-Angriffe 35 Punkte

Wir betrachten nun Chiffren mit Schlüsseln aus dem binären Alphabet, bestehend aus 1 und 0, mit einer Schlüssellänge von n Bit.

a) Wie viele Schlüssel müssen Sie im Worst Case durchprobieren, um den richtigen Schlüssel zu finden? (Hinweis: „Worst Case“ bedeutet hier, dass erst der letzte überprüfte Schlüssel der richtige ist.) (5 Pkt.)

a) Wieviele Schlüssel müssen Sie im Durchschnitt durchprobieren, um den richtigen Schlüssel zu finden? (5 Pkt.)

b) Für die Schlüsselsuche stehen ihnen nun folgende Hilfsmittel zur Verfügung:

- GPU (CUDA): $15,3 * 10^7$ Schlüssel/Sekunde
  (Grafikkartenprozessor)
- Amazon Cloud: $66 * 10^7$ Schlüssel/Sekunde
  (bei Amazon gemietete Rechenleistung für 1$/h)

- FPGA: $11,25 * 10^8$ Schlüssel/Sekunde
  (FPGAs sind spezielle Hardware-Bausteine, die programmierbar sind.)

Berechnen Sie jeweils für $n = 80$, 112, und 192 Bit, wie lange Sie für die vollständige Schlüsselsuche (1) im Worst Case und (2) im Durchschnitt brauchen, und geben Sie dies in einer Tabelle in sinnvollen Zeiteinheiten an. (Verwenden Sie für Zeitangaben von mehr als 9999 Jahre die wissenschaftliche Notation mit zwei Nachkommastellen, also z.B. $9,99 * 10^3$, der Genauigkeitsverlust durch diese Darstellung spielt bei dieser Größenordnung keine Rolle mehr.) (20 Pkt.)

c) Um das Wievielfache verlängert sich die Zeit für eine Schlüsselsuche, wenn die Schlüssellänge von 80 auf 112 Bit erhöht wird? (5 Pkt.)

d) Im Allgemeinen: Um wieviel langsamer wird ein Brute-Force-Angriff, wenn der Schlüssel um w Bit verlängert wird? (5 Pkt.)

Seit den 1970er Jahren wächst die Rechenleistung von Computern exponentiell an. Nach dem sogenannten Mooreschen Gesetz verdoppelt sich die Rechenleistung etwa all 18 Monate, wobei der Preis konstant bleibt. In den 1980ern und 1990er Jahren gab es vereinzelte Krypto-Anwendungen, für die ein 50 Bit Schlüssel verwendet wurde. Wir nehmen an, dass eine vollständige Schlüsselsuche 1992 ein halbes Jahr (183 Tage) dauerte.

e) In welchem Jahr wurde die Schlüsselsuche innerhalb einer Stunde möglich, wenn wir das Mooresche Gesetz für die Entwicklung der Computerrechenleistung zu Grunde legen? (5 Pkt.)