Gesamtpunkte:

DatKom	Übungsblatt 8	Kaan Giray Buzluk	405099
SS 2021		Su Ada Yıldırım	410949
12. Juli 2021		Ozan Ege Şap	411851

Aufgabe 8.1 0.5/2.5

(a) Weil TCP ein bi-direktionales Protokoll ist, braucht man noch eine dritte Nachricht um die Verbindung zu anschließen, sonst könnte nur eine Seite Daten versenden. Der Server muss auch feststellen, dass der Client auch Pakete bekommen kann.

Nein, es geht darum dass der Server weiß, dass der Client den Verbindungsaufbau als abgeschlossen sieht. -0.5

(b) TCP Protokoll bietet mehr als ein zuverlässiger Datenübertragungsdienst. Das ist ein Standard, sonst müsste man immer Mühe geben, um unterschiedliche Datenübertragungsdienste miteinander zu verbinden. Man könnte auch Probleme erfahren, da es dabei auch um unterschiedliche Protokolle umgehen kann, dabei können Synchronisationsfehlern entstehen.

Staukontrolle wird trotz zuverlässiger Leitung benötigt -0.5

(c) -0.5

(d) Mit der UDP wartet man nicht für eine erfolgreiche Verbindung, man kann jeder Zeit Paketen senden. Damit kann man dies für Zeitkritische Fälle anwenden, da die Prozesse schneller laufen.

Welche wesentliche Funktion (von TCP) hat UDP auch? → Ports -0.5

(e) Ja, das ist möglich. Man muss aber neben UDP noch eine Methode implementieren, welche die Pakete nummeriert und danach überprüft ob es fehlende Pakete gibt und bietet es diese nochmal. UDP allein bietet aber kein zuverlässiger Datentransfer. ✓

8.2 0/6

Aufgabe 8.3 2.5/2.5

(a) Angenommen betrachten wir den Caesar Cipher nur für eine einzige Buchstabe. Dann ist offensichtlich $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}| = 26$. Dabei wählt man zufällig eine Buchstabe aus Σ für $P \in \mathcal{P}$. Dabei ist erstmal $Pr(P) > 0$ für alle Klartexte P (was hier nur eine Buchstabe ist). Dabei hat man den Ciphertext C und man beobachtet, dass jedes K gleich wahrscheinlich ist, da man von dem Ciphertext nichts über den Klartext sagen kannst. Damit kann der Plaintext jede Buchstabe sein. Man weiss nichts und kann nichts darüber sagen. Aber es gibt nur K, sodass diese angewandt auf P den Ciphertext C gibt. Dabei hat man Perfect Secrecy. ✓

1.5/1.5

Wenn man aber nicht Buchstaben sondern Wörter betrachten kriegt man kein Perfect Secrecy. Sei $\Sigma = \{A, B, \cdots, Z\}$. Man hat als plaintext $P \in \Sigma^*$ ein Wort aus dieser Sprache mit einer beliebigen Länge. Aber man hat zur Auswahl eines Schlüssels nur 26 unterschiedliche Möglichkeiten. Dabei ist die Plaintext space nicht gleichmächtig mit dem Key space. ✓ Man kann hier alle Schlüssel probieren um den Text zu decodieren, wenn der plaintext ein Wort aus einer bekannten Sprache ist (Deutsch, Englisch, usw.), dann kann man überprüfen ob das dekodierte Wort Sinn macht. Damit kann man fest schließen, dass vielleicht ein Schlüssel wahrscheinlicher als die anderen Schlüsseln ist. Dabei wird es mit dem Perfect Secrecy widersprechen. ✓

Also $|K| \neq |P|$

(b) Hier ist der Key Space gleichmächtig wie der plaintext Space. ✓ Wenn man die Schlüssel echt random wählt, dann hat man für ein plaintext der Länge $n \in \mathbb{N}$ insgesamt 26^n

1/1

mögliche Schlüsseln. Dabei kann man aus einem Ciphertext mit einem beliebigen Scchlüssel jeder Plaintext der Länge $n \in \mathbb{N}$ konstruieren (dekodieren). Dabei ist es uns unbekannt, wie der plaintext sein sollte, wenn wir nur den Ciphertext kennen. Also ist jeder Schlüssel K gleich wahrscheinlich. Damit hat man in diesem Fall Perfect Secrecy.

Aufgabe 8.4 2/4

(a) i. Wenn man den Schlüssel beim Plaintext oft wiederholt, dann kann man merken, dass in manchen Stellen es kleinere Teilwörter gibt, die gleich sind. 2/2

ii. Man findet diese wiederholte kleinere Teilwörter im Ciphertext. Danach zählt man die Distanz zwischen dieser beiden Wiederholungen. Sei $n \in \mathbb{N}$ die Distanz. Dann kann man die Teiler von n listen und gucken ob sie als Schlüsselänge Sinn machen. z.B. würde es sehr absurd sein, dass die Schlüssellänge 1 oder 2 ist.

iii. Wir suchen wiederholte Wörter. Hier hat man z.B. das Wort "TENX", wiederholt in zwei Stellen. Auch haben wir "VQOKMïn zwei Stellen. Die anderen Wörter sind wie folgt mit ihrer Distanzen gegeben:
"TENX"16
"CJVQOKM"8
"GL"16
ÏWNRWX"16
ÏTLFCM"264

Daher hat man die Möglichkeiten: $16, 8, 4, 2, 1$
1 und 2 sind sehr kurz. Dann haben wir 16,8 und 4. Man führt Schnittmenge mit 264 und dann kriegt eine Möglichkeit, welche 8 ist.

Also ist die Schlüssellänge 8.

(b) 0/2