12.5/15P

DatKom	Übungsblatt 8	Mert Saglam	406572
SS 2021		Parsa Bahadori	407004
12. Juli 2021		Thilo Metzlaff	406247

Aufgabe 8.1 1.5/2.5P

0.5/0.5P a) Die ersten beiden Nachrichten würden ausreichen, wenn man davon ausgeht, dass die Pakete sicher ankommen würden. Es können alle Pakete bei Verwendung von IP verloren gehen, also ist es nicht gewährleistet, dass der Connection Request beim Empfänger ankommt. Also ist eine Quittierung vom Verbindungsaufbau nicht nur notwendig um Parameter mitzuteilen und ein ACK zu senden, sondern auch, damit der Sender weiß, dass sein Connection Request nicht verloren gegangen ist. Da die Quittierung, dass der Empfänger bereit ist, aber auch verloren gehen könnte, ist eine dritte Nachricht von nöten, wo der Sender die Nachricht vom Empfänger quittiert.

0.5/0.5P b) Nein, da TCP auch weitere nützliche Funktionalitäten wie z.B. Verfahren zur prevention von Netzüberlastung bietet.

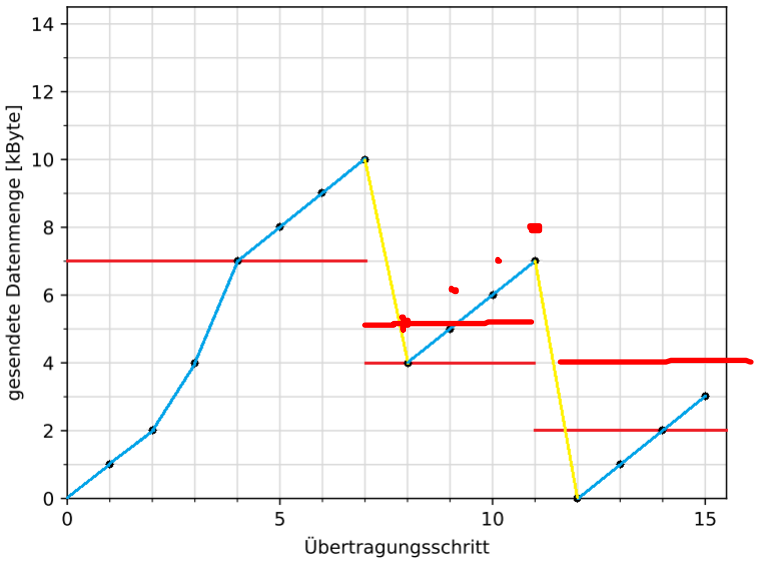
0/0.5P c) Falls TCP *Go-Back-N* benutzt, so findet eine Übertragungswiederholung ab dem verloren gegangenen ACK statt. -0.5P: Nein. ACKs sind kumulativ. Geht eins verloren, wird es durch das nächste ACK ersetzt
Falls TCP *Selective Repeat* benutzt, so wird nur das fehlerhafte ACK explizit angefordert. Es kommt also auf das Verfahren an, welches TCP benutzt.

0/0.5P d) Die wesentliche Funktion von UDP ist die Cheksum-Prüfung. -0.5P: Addressierung einer Anwendung durch Ports

0.5/0.5Pe) Ja, falls sich die Anwendung um das Quittieren und die Neuübertragung kümmert, da UDP dies nicht macht.

Aufgabe 8.2 4.5/6P

a) 1.5/3P



-1.5P:
- zweiter Threshold bei 5.5 und nicht 4
- dritter euer Threshold bei 4 und nicht 2
- Runterfall auf 1MSS und nicht 0MSS bei Schritt 12

2.5/2.5P b) i) 1/1P
Wir haben einen Slow-Start bis wir sstresh von 8 kByte erreichen, ab da erhöhen wir unsere MMS in jedem Übertragungsschritt um 1 kByte. SStresh erreichen wir nach dem 4. Übertragungsschrit mit einer MMS von 8 kByte.
Das Sendefenster im 8. Übertragungsschritt beträgt dann 12 kByte, also haben wir im neunten Übertragungsschrit eine Datenrate von 13 Kbyte.

ii) 0.5/0.5P
Bis zum 8. Übertragungsschritt hat der Sender schon $(1+2+4+8+9+10+11+12)kByte = 57kByte$ an Daten gesendet.

iii) 1/1P
Die maximal mögliche Datenrate beträgt 30 kByte, da der Empfänger nicht mehr als 30 kByte puffern kann. Wenn der Sender 31 KByte senden würde, so würde 1 kByte verloren gehen.

0.5/0.5P c) Dies kann passieren, wenn wir vorher eine eventuelle Stausituation hatten, wo z.B. 10 PCs Daten gleichzeitig über die gleichen Router senden, und nun 9 dieser PCs ausfallen. Dann kann man das vorherige lokale Maxima überholen, da keine Stausituation mehr eintritt und wir problemlos unsere cwnd in jedem Schritt um 1 erhöhen können.

Aufgabe 8.3 2.5/2.5P

1.5/1.5P a) Sei $P = ABC$ und $C = AAA$.
Dann gilt $Pr(P|C) = 0$, da der Plaintext nur gleiche Buchstaben haben dürfte.
Es gilt jedoch $Pr(P) > 0$, da P ein zulässiges Wort ist.
Somit bietet die Caesar Cipher keine perfekte Verschlüsselung.

1/1P b) Die so modifizierte Cipher bietet eine perfekte Verschlüsselung.
Sei $P = m_0m_1 \dots m_n, c = c_0c_1 \dots c_n$ und $k = K_0k_1 \dots k_n$ mit $m_i, c_i, k_i \in \{A, B, \dots, Z\}$ und $i \in \{0, 1, \dots, n\} \subseteq \mathbb{N}$.
Dann gilt $|P| = |C| = |K|$ und $Pr(P) > 0$, da jedes P ein zulässiges Wort über das Alphabet ist. Da jedes k_i (nach Aufgabenstellung) gleich-verteilt zufällig gewählt ist, ist somit jedes k gleich wahrscheinlich. Für jedes P der Form $P = m_0m_1 \dots m_n$, und C der Form $c = c_0c_1 \dots c_n$ gibt es nun genau ein K der Form $k = K_0k_1 \dots k_n$ mit $k_i = c_i - m_i \mod 26$, sodass $E_k(P) = C$.
Nach Shannon's Theorem bietet dieser modifizierte Cipher also perfekte Verschlüsselung.

Aufgabe 8.4 4/4P

a) 2/2P

0.5/0.5P (i) Wenn sich der Schlüssel wiederholt, treten wahrscheinlich irgendwo im Ciphertext Buchstabenfolgen auf, die doppelt Vorkommen.

0.5/0.5P (ii) Falls sich im Ciphertext Buchstabenfolgen wiederholen, ist dies sehr wahrscheinlich ein Zeichen dafür, dass sich der Schlüssel wiederholt hat und im Plaintext diese Buchstabenfolge mit dem gleichen Schlüsselteil verrschlüsselt wurde. Der Abstand dieser Buchstabenfolgen gibt dann Auskunft über die Schlüssellänge, da die Schlüssellänge sehr wahrscheinlich ein Teiler aller Abstände von den wiederholten Buchstabenfolgen ist.

1/1P (iii) Suche dafür Buchstaben, die sich wiederholen:

OIT LFCMCL WQ MGIXR VYTWY VTAZX WHU EBLV?
IU CJB WCJ VQOKMK, CJ VQOKMM EWWEBNQGB!
TENX IWNRWX GL YQXP, TENX IWNRWX GL UWKR
BIFITP WGW TCEVBX, QAI MIDUXL FMEBK NHPL.
WKY JIFKWPP OEL WPSIPAVTG QAGJ, QRZMCF VGWYB EYFKG
CE MBLWV BO EQXBJMI JIQHPAWKYIBXL KGJFRVZC.

VMG MTPEYFKGH JQGB NSNF, UMK PGYVYI QF QLVGMJ,
LT KWPFYK ABAZ ZQLCINR VIT LFCMGFKRLFHXQK
YPX ICYR "SPN CYZ IYWGMWYMG, GZV UIIOM CMGJ TL DBCD,
RKWYB WCJ MR-BFAM, LWMP, XVZ PCY MUN UIL XAIN!"
YJ SHKEI IUI JTJV IKHVU CCVIP TL ONRW
IKHV AHPYWCG XMIJSRVY LVW JGSRZIMBC JSWNV.

Abstand zwischen CJVQOKM: 8
Abstand zwischen TENXIWNRWXGL: 16
$ggT(8, 16) = 8 \Rightarrow$ Schlüssellänge 8

2/2P b) 1. Teile den Ciphertext in Blöcke.

GEL XSFCEL FSDVCAVIZJEGO HASOEYUUH
EGDKUUR' BMV YLT WSXWVTKKG LHRXWCZLE.
WOF XRHG, OWZH HXBFXLCAO FAXTBXUFDBXVZQ,
GOKD GFHH'G CCSDR KYIFHN SE VUPMXV IZG HHOZXH.
VXBUUITXD RQU RNOQWZEZ, NUE ELBMYRHLW QSESAEDSZ,
PIM BWB ZIKN RUH WXVH ZXR SEA ZDRKOB SHHTVHQQ.

2. Führe Häufigkeitsanalyse für den ersten Buchstaben von jedem Block durch.
$\Rightarrow$ H kommt am häufigsten vor, insgesammt 9 mal.
$\frac{9}{36} = 25\%$ relative Häufigkeit.
3. Nehme an, dass das H im Klartext E ist. Dann ist der erste Schlüsselbuchstabe $H - E = D$.

Häufigkeitsanalyse zweiter Buchstabe von jedem Block:
E und R kommen am häufigsten vor.
Nehme an, dass E im Klartext E ist, dann ist der zweite Schlüsselbuchstabe $E - E = A$.

Dritter Buchstabe:
X kommt am häufigsten vor.
Nehme an, dass X im Klartext E ist, dann ist der dritte Schlüsselbuchstabe $X - E \mod 26 = T$.

Vierter Buchstabe: O kommt am häufigsten vor.
Nehme an, dass O im Klartext E ist, dann ist der vierte Schlüsselbuchstabe $O - E = K$.

Fünfter Buchstabe:
S kommt am häufigsten vor.
Nehme an, dass S im Klartext E ist, dann ist der fünfte Schlüsselbuchstabe $S - E = K$.

Sechster Buchstabe:
Rate Schlüsselbuchstabe M, d das Schlüsselwort dann DATKOM ist.

Entschlüsselte Nachricht: Des Netzes verschlungene Topologie
entwirr' ich mit Dijkstras Zeremonie.
Der Lahn, eine herrliche Routingtabelle,
dort steh'n sogar Routen zu Himmel und Hoelle.
Vergiftet der Rueckweg, das Blickfeld gespalten,
mit RIP wird die Welt nur zum Narren gehalten.

Gut gemacht. :)