Bei uns war ursprünglich noch ein Dritter in unserer Abgabegruppe eingeteilt. Wir haben ihn vor über einer Woche versucht per E-Mail zu erreichen, leider erfolglos.
Nach Ablauf der Anmeldefrist zu den Abgabegruppen haben wir gesehen, dass diese Person leider unsere Abgabegruppe verlassen hat.
Bisher konnten wir noch keinen Dritten für unsere Abgabegruppe finden.
Uns wurde auch seit dem letzten Blatt keine weitere Person zugeteilt.

Aufgabe 8.1

a) Mit dem ersten Paket teilt Host 1 Host 2 seine Initialparameter aus. Mit dem zweiten Paket bestätigt Host 2 diese und teilt Host 1 seine Initialparameter aus. Mit dem dritten Paket bestätigt Host 1 diese. Würde man diese Bestätigung wegfallen lassen, so könnte es Vorkommen, dass beispielsweise die Sequenznummer von Host 2 nicht mit Host 1 synchronisiert ist. Dadurch wäre die Kommunikation gestört.

b) Nein, wäre noch sinnvoll: Router verwerfen Pakete absichtlich bei Stau. Dann würde ja ein solches Paket nicht zuverlässig übertragen werden.

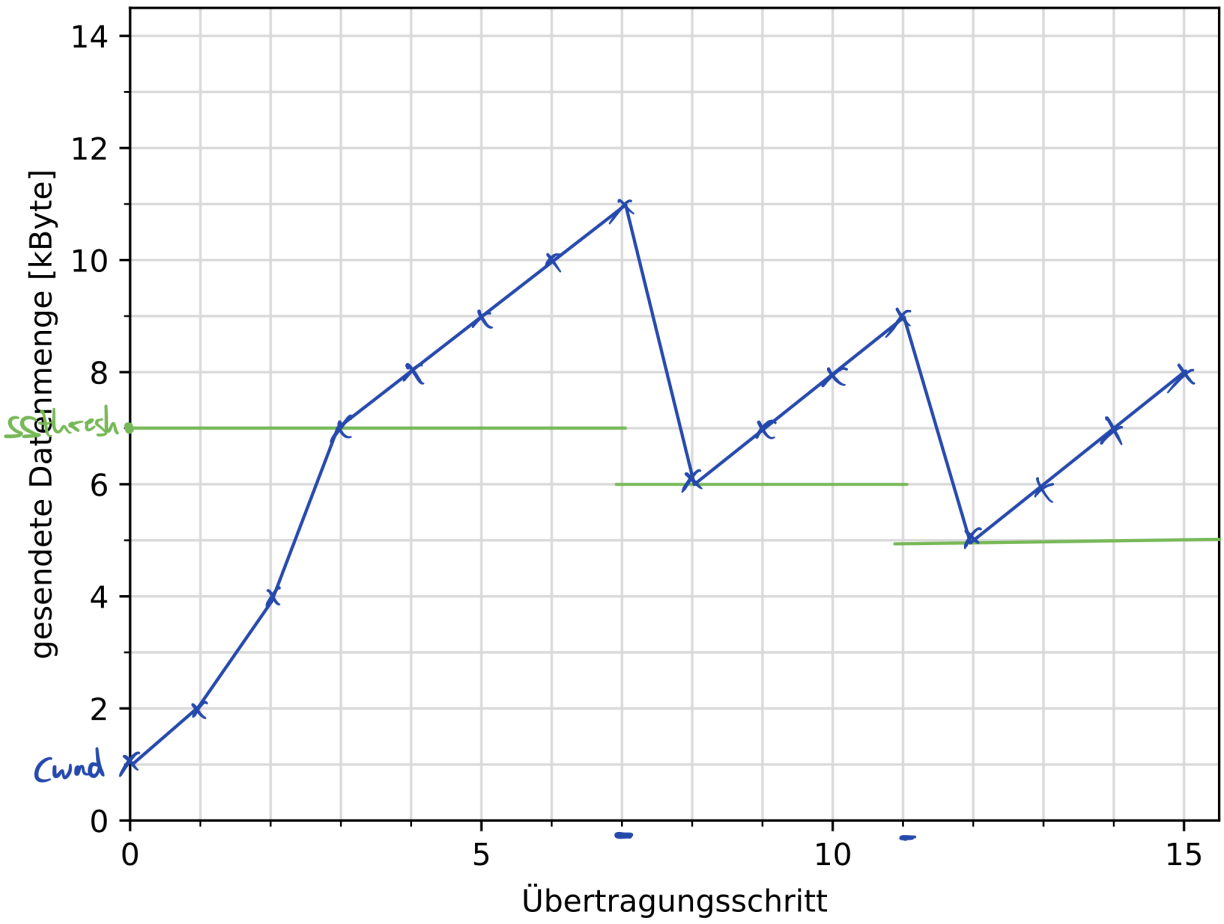
c) Ja. Das Paket wird als verloren anerkannt, wenn es nach RTT immer noch nicht bestätigt wurde, oder wenn nach dem verlorenen ACK noch ein weiteres / weitere ACKs eintreten, sodass das Paket wegen 3-ACKs retransmittet wird.

d) Schnelligkeit und Effizienz.

e) Ja. Man kann einen weiteren Dienst / Protokoll basierend auf UDP entwickeln, welche dann zuverlässig ist (genauso wie TCP auf IP ist).

Aufgabe 8.2

a)



b) i) Nach 4 Übertragungsschritten ist `cwnd = ssthresh`. Nach 4 weiteren Schritten ist also `cwnd = ssthresh + 4 kB = 12 kB`.

ii) `(1+2+4+8+9+10+11+12) kB = 57 kB`

iii) `30 kB`, da sonst würde der Empfangspuffer überlaufen und es würden Pakete verworfen werden müssen, was zu einer Erniedrigung von `cwnd` führt.

c) Angenommen im Netzwerk kommunizieren noch andere Geräte und jeder Datenaustausch läuft durch einen Router. Dann kann es sein, dass andere Rechner vorher mehr kommuniziert haben, weshalb der Router aufgrund von Stau ein Paket verwerfen musste (voriges lokales Maximum). Wenn jetzt sonst niemand mehr im Netzwerk kommuniziert, können wir offensichtlich mit einer höheren `cwnd` senden.

Aufgabe 8.3

a) Es gilt $\mathcal{P} = \mathcal{C} = \{A, \ldots, Z\}^*$ und $\mathcal{K} = \{A, \ldots, Z\}$. Es gilt offensichtlich $|\mathcal{K}| < |\mathcal{P}|$. Nach Claude Shannon ist der Caesar-Cipher nicht perfekt.

b) Jetzt gilt nun dass $|\mathcal{K}| = |\mathcal{C}| = |\mathcal{P}|$. Zudem gibt es für alle m_i und c_i aufgrund von Modulo nur ein κ_i, sodass $c_i = m_i + \kappa_i \mod 26$. Da dies für alle $i \in \mathbb{N}$ gilt, gibt es für jedes $c \in \mathcal{C}, m \in \mathcal{P}$ genau ein $\kappa \in \mathcal{K}$, sodass $c = m + \kappa \mod 26$.
Nach Shannon's Theorem ist diese Variante des Caesar Cipher perfekt.

Aufgabe 8.4

a) i. Wiederholungen des Schlüssels äußern sich, wenn im verschlüsselten Text an unterschiedlichen Stellen dieselben Zeichenfolgen vorkommen. Dies kann indizieren, dass der Schlüssel wiederholt and derselben Stelle/Index denselben Klartext verschlüsselt hat.

ii. Ist dies der Fall, so kann man anhand der Zeichenlänge die minimale Schlüssellänge bestimmen. Weiterhin kann man damit noch die Zeichen bis an den Start des Ciphertexts zurückzählen, und so somit die minimale Schlüssellänge womöglich genauer bestimmen:
Angenommen man findet eine sich wiederholende Zeichenfolge der Länge m im Ciphertext und man geht davon aus, dass der Schlüssel sich hier wiederholte. Dann beträgt die minimale Schlüssellänge m. Beginnt die Zeichenfolge im i-ten Zeichen im Ciphertext, so ist die minimale Schlüssellänge m', sodass $\lfloor \frac{i}{m} \rfloor = \frac{i}{m'} \in \mathbb{N}$.

iii. In Zeile 2 und Zeile 3 sind solche Zeichenfolgenwiederholungen. Die längere Zeichenfolge beträgt 12 Zeichen. Der Schlüssel beträgt 16 Zeichen (Vorgehensweise oben).

b) Key: `DATKOM` - wie zu erwarten.