Jo, also die Sachen die er mich gefragt hat, waren (Fragen/Aufgabenstellungen sind fett, "Antworten" kursiv):

- **Zertifikate** (hab mich bissl vertan und hab angefangen Needham-Schröder zu erklären, hab dann aber doch gemerkt, dass was schief läuft und ne umständliche Art von Zertifikat erklärt, ne Art Zwitter aus Needham-Schröder und Zertifikat... weshalb er dann auch gewechselt hat zu...)
- **Needham-Schröder** (so grob erklären wer wem schickt und wer die Arbeit dabei hat, nämlich vor allem *A* und nicht die *TTP*, damit kein Denial-of-Service und so...)
- **dann wollt er wissen, was ich nehm um ne Nachricht *m* die *A* an *B* schickt zu authentifizieren und die Nachrichten-Integrität zu sichern** (sprich dass nix dran geändert wurde und das immer noch die original Nachricht is.) Ich meinte zum authentifizieren kann ich z.B. *DES* oder *RSA* benutzen, weil das den Vorteil hat, dass es auch gleichzeitig ordentlich verschlüsselt. Is ja dann sichergestellt, dass das von mir kommt, weil ja ich nen Schlüssel benutz, den nur ich kennen kann... Und für die Integrität hab ich halt *MD5* gesagt. Dann hat er gemeint, dass ja nach *DES m* verschlüsselt is, also *E(k, m)* und was jetzt durch *MD5* betroffen is. Ich meinte, dass das wohl *m* selbst wäre, und nicht *m' = E(k, m)*, weil das ja auf nem anderen Layer stattfinden kann als MD5. Hat ihm wohl getaugt.
- dann sollte ich **grob MD5 erklären**; hab ungefähr die *Grafik mit |A|B|C|D|* hingemalt, wo dann eben *A* mit meinem Messageblock ver-XOR-t wird und so... und gesagt dass halt *Hashfunktionen* benutzt werden, die eben immer einen Wert einer bestimmten größe erzeugen.
- als nächstes wollte er zu was praktischem kommen: **IPSec**; da hat er gemeint, dass das ja so ungefähr alles kann und **wollte wissen, was ich für Einstellungen bei IPSec nehmen würd um Verschlüsselung, Datenintegrität, Authentifizierung sicherzustellen**. Ich hab erstmal *erklärt, was bei IPSec passiert*, also eben *SA*, *Tunnel- vs. Transaction-Mode*, *AH* und *ESP* (also überall kurz gesagt, was passiert...); **Er malte dann so einen IPSec Block hin: |IP| AH|ESP|Data|ESP-T| und fragte, was daran authentifiziert und was verschlüsselt is**. *Data is verschlüsselt*, evtl. durch ESP auch authentifiziert, aber unnötig, weil *AH* ja den *ganzen Block (inkl. IP!) authentifiziert*. Die Antwort auf seine Frage is halt, ne *Kombo aus AH und ESP*.

Außerdem hab ich dann noch kurz mit ihnen darüber geredet, dass MAC auch zur Sicherstellung der Datenintegrität taugt (weil, wenn man was an der orig. Nachricht verändert, auch die MAC anders wird), warum man AH braucht, wenn doch auch ESP authentifiziert (AH nimmt den IP-Header am Anfang mit, ESP nicht) und dass ja das Interlock-Protokoll ziemlich schwierig anzuwenden is, weil A und B ja schon vor dem Anwenden was wissen müssen und was das sein könnte (z.B. aus ner alten Session nen Key oder eben eine bestimmte Protokollspezifikation, die durchgewechselt wird oder sowas; kam halt dann im Grunde drauf raus, dass das Protokoll nix bringt, wenn A und B sich absolut nich kennen.
Die letzten Sachen gingen aber ned in die Bewertung wirklich ein, denk ich.

Insgesamt hab ich mich halt anfangs voll vertan, was dazu führte, dass ich die ganze Prüfung über sehr unsicher war und dumme kleine Fehler gemacht haben. Das hat sie aber glücklicherweise ned gestört und sie ham nirgends auf Details oder sowas rumgehackt, waren sehr freundlich und es war ne lockere Atmosphäre. Sie helfen dir zwar ned raus, wenn du dich wo vertan hast, indem Sinn, dass sie dir die Lösung sagen, aber sie geben dir die Chance, es später nochmal selbst zu verbessern, indem Sie dich zwischendrin was anderes machen lassen oder halt auf deinen Fehler stoßen.
Insgesamt hat meine Prüfung wohl effektiv ca. 20 Minuten gedauert, wenn man bissl Smalltalk und Überprüfung der Daten am Anfang und das Gespräch am Ende abzieht.