These are the questions I remembered:

Q1. Given 5 statements, you need to say if they are related to Confidentiality, Integrity, or availability (I don’t remember all of them):

* Student A copied Student B’s homework
* A crashes B’s operating system
* A changed a message (this is integrity)

Q2. Define each of the following terms:

* Threat
* Attack
* Attacker
* Vulnerabilities
* Risk

Q3. Gave you an image and ask you which security model it represents. The image briefly says “No write Down” and “no read up”.

* This represents Bell-LaPadula model (lecture #3).
* Then asked why this model have “No Write Down”?

Q4. What is the difference between attack and risk, who becomes first?

Question about SHA-1 (this is not in the slides).

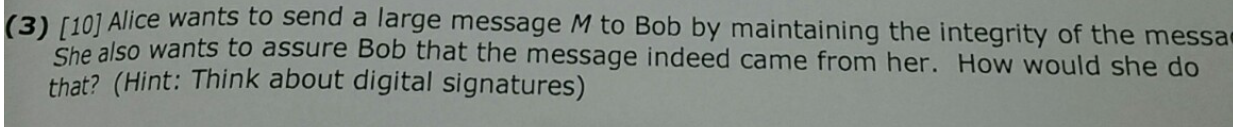
* What is SHA-1
* What is the collision that Google detected in SHA-1? ( Not 100% it the question was like this)
* Is the collision avoidable?

Question about: Botnet, DOS, and DDOS (also not in the course material)

* What is Botnet
* What is DOS (Denial Of Service) attack, what is the DDOS (Distributed Of Service) attack. What is the difference between both

Question about CAPTCHA (also not in the course material). I don’t remember the exact question

Question about digital signatures (same as previous years):



SCI:

Relate a security principles to a SCI principles that we’ve studied