1. **Hashing**
   1.1. [3/30] Give your statement, and justify it, about the number of collisions generated by a cryptographic hashing function. In particular, are they less with respect to a non-cryptographic hashing function? And in what sense? Extensive discussion required.
   1.2. [2/30] What is the Merkle–Damgård construction and what is its use? Why do we use it and when?
   1.3. [2/30] Let f and g be two cryptographic hashing functions and let $F(x) = f(g(x))$ the function obtained by combining f and g (g first). Does F behave (to the purpose of having another cryptographic hashing function) better than f or g? Explain.

2. **Encryption**
   2.1. [3/30] Alice loves stream ciphers and she prefers them to block ciphers. Bob replies they are old and that the most used cipher is a block cipher, namely AES. Alice says this does not contradict her preference and the two ingredients - a block cipher and the stream cipher approach - can coexist. Why? Explain.
   2.2. [3/30] Can encryption be authenticated? What approaches do you know? Illustrate.
   2.3. [3/30] What is "ciphertext stealing"? (you can use a drawing). Discuss how it works and its benefits.

3. **Access control**
   3.1. [2/30] Discuss how a method of access control can help the requirement of confidentiality.
   3.2. [2/30] Can access control and encryption coexist? Elaborate.

4. **Firewalls**
   Assume that the iptables software is running on host H, having a network interface eth0 (IP: 192.168.0.2) connected to a LAN (IP: 192.168.0.0/24; the LAN is protected by H) and a network interface eth1 (IP: 151.100.4.3) connected to the Internet. Assume that the default policy for all built-in chains is DROP.
   4.1. [3/30] Allow hosts in the LAN to connect to H by ssh.
   4.2. [3/30] Allow hosts in the LAN to connect to the web but block Facebook (IP: 157.240.231.35) connections.

5. **Digital signatures**
   5.1. [3/30] Illustrate at a high level the procedure to produce a valid digital signature. (No confidentiality required, only non-repudiation).
   5.2. [3/30] Illustrate the algorithm used by Bob for verifying the digital signature upon receival of a pair (D, S), where D is a document and S is the digital signature of Alice on D.

student