Systems Security Exam

Bring calculator!

1. What threat do they pose?
   1. Daily carrier who drops packages and picks them up
      1. Access to servers, internal intruder
   2. Former employee who left because of downsizing
      1. Begrudged, might sell information or use information to harm the company
   3. Employee travelling on company business
      1. Loses laptop which can be hacked, and company data be stolen
   4. Building management company installs sprinkler system
      1. Access to servers and sprinkler might cause damage to hardware
2. Define notion of collision resistance in hash functions  
   h : X => Y is collision resistant => computationally infeasible to find 2 points x1,x2 € X such that h(x1) = h(x2)
3. A (has password) B (has key)  
   Send [conn] to B generate a random challenge R  
    Sends [R] to A  
   Compute key from password   
   compute X<=encrypt® with key   
   Send [X] to B  
    compute Y<=(x) with key, if Y equals R  
    A is authenticated  
     
   Breaking the algorithm:  
   repeat {   
    check candidate password cpw;  
    compute ckey password cpw;  
    compute cX;  
   }, until cX = X
4. Explain Bot Net, Easter Egg, Logic Bomb (One sentence is enough)
   1. Bot net is a peer to peer network of compromised computers
   2. Easter Egg is unspecified code hidden in the program
   3. Logic bomb is malicious code activated by trigger
5. Name ways hackers can compromise computers without code breaking
   1. Key catchers (sw, hw)
   2. Email executable files
   3. Boot CD
6. Firewall does not protect from:
   1. Malicious code in emails
   2. Human error or internal attacks. Compromised internal machines and VPN
   3. Malicious code injections
   4. Open ports
   5. Firewall itself
   6. DDoS attack against the firewall
7. Download email or web page with hidden content.
   1. TLS and SSL are encryption protocols => security and data protection on internet  
      => encrypt segments of communication at transport layer for end-to-end communication.
8. IP attacker inserts bogus packets into communication. Would this succeed on SSL and IPsec?
   1. IP sec would block the packages and not forward to TCP.
   2. SSL could break into TCP.

RSA! Vigenere! Playfair! Last year exam. Book mentioned in slides. Example problems on some website