433/533 HW1 Answer Key

1.
    a. Confidentiality -> Interception
    b. Integrity -> Modification
    c. Availability -> Interruption
2. Activists, terrorists, opposing factions, and outside forces can meddle with the system in various ways to change the results, delay the results, or disrupt it to induce chaos and uncertainty.
3. Q3:
    a. Some pieces of knowledge
    b. Some physical item
    c. A part of the user's body
4. It is fine as long as it learns more about the user as time goes by, through various dubious means, and uses them later on to verify them after they have done something to require authentication.
5. A good solution must address at least:
    a. The increasing gap by synching on a need basis
    b. The small discrepancies by having a window of accepted tokens from before and after

    I also accepted creative solutions.
6. Refer to the book for exact answers for different cases. It is probably good enough as long as you provide a good rationale for your answer. The "ease of use" changes depending on the size and scale of what you want to do, which isn't given here.
7.
    a. If the access control is to be enforced by the machine of Alice, the access control is **per object**, where the object can list which subjects can access it (i.e., send traffic to it). This is an ACL.
    b. If the access control is to be enforced by a firewall machine right in front of each sender, the access control is **per subject**, where the subject can list which objects it can access. More specifically, the firewall will specify which machines the sender can send traffic to, including whether it can send traffic to Alice's machine. This is a directory.
    c. If the access control is to be enforced by routers en route from each sender to the machine of Alice, which inspects the traffic to either block or pass it, the traffic must carry some kind of token to indicate whether the traffic from its sender can reach Alice's machine. This kind of token is a capability.
8. Quite a long while, but who can say, points off only if you haven't tried.
9. The answer is in the slides, or chatgpt
10. Answer in slides again, but roughly:
    a. Both sides choose a public mod m and a public base b
    b. Both sides choose their own private key k, l
    c. side1 does b^k mod m
    d. side2 does b^l mod m
    e. they give each other their calculated value

f. they repeat steps c and d, but now using the result of the other side as their base.
g. Now they have a shared secret key

11. She could choose a symmetric key to encrypt the message, and then encrypt this symmetric key with the public keys of her friends, and send the encrypted message and encrypted key to all the friends. Then the friends can decrypt the key with their private keys, then use the symmetric key to decrypt the message.