

1. Chapter - 1 (1 Question 10 points)
 - (a) Please classify each of the following as a violation of *confidentiality*, of *integrity*, of *availability* or of some combination of those:
 - i. John copies Mary's homework.
 - ii. Paul crashes Linda's system.
 - iii. Carol changes the amount of Angelo's check from 100to1000.
 - iv. Gina forges Roger's signature on a deed.
 - v. Rhonda registers the domain name *AddisonWesley.com* and refuses to let the publishing house buy or use the domain use the name.
 - vi. Henry spoofs Julie's IP address to gain access to her computer.
2. Chapter - 9 (2 Questions 30 points)
 - (a) Please describe the following keywords (include diagrams if necessary)
 - i. One-time pad
 - ii. Confusion
 - iii. Diffusion
 - iv. Triple DES
 - (b) Suppose Alice and Bob have RSA public keys in a file on a server. They communicate regularly using authenticated, confidential messages. Eve wants to read the messages but is unable to crack the RSA private keys of Alice and Bob. However, she is able to break into the server and alter the file containing Alice's and Bob's public keys.
 - i. How should Eve alter that file so that she can read confidential messages sent between Alice and Bob, and forge messages from either?
 - ii. How might Alice and/or Bob detect Eve's subversion of the public keys?
3. Chapter - 10 (2 Questions 20 points)
 - (a) Consider the following authentication protocol, which uses a classical cryptosystem. Alice generates a random message r , enciphers it with key k she shares with Bob, and send the enciphered message rk to Bob. Bob decipheres it, adds 1 to r , and sends $r + 1k$ back to Alice. Alice decipheres the message and compares it to r . If the difference is 1, she knows her correspondent shares the same key k and is therefore Bob. If not, she assumes he correspondent not to share the same key k and so is not Bob. Does this protocol authenticate Bob to Alice? Why or why not?
 - (b) Consider an RSA digital signature scheme. Alice tricks Bob into signing messages m_1 and m_2 such that $m = m_1m_2 \bmod n_{Bob}$. Show that Alice can now forge Bob's signature on the message m .

4. Chapter - 12 (2 Questions - 20 points)

- (a) Explain how one-time password schemes work. Assuming a one-time password scheme uses Lamport's technique to generate passwords: comment on the following.
 - i. Explain whether the scheme is compromised if an attacker sniffed a password?
 - ii. How should the attacker proceed to attack this scheme?
 - iii. Where does security of this scheme come from?
- (b) On Unix systems why are *salts* used for? Does using passwords with a salt make attacking a specific account more difficult than using passwords without a salt? Please explain why or why not?

5. Chapter - 13 (1 Question 10 points)

- (a) A common technique to inhibit password guessing is to disable an account after three consecutive failed login attempts.
 - i. Please discuss how this might cause a denial of service attack. Why is this action a violation of the principle of least common mechanism?
 - ii. One can argue that this is an example of fail-safe defaults, because by blocking access to an account under attack, the system is defaulting to a known, safe state. Do you agree or disagree with this argument? Please justify your answer.

6. Chapter - 14 (1 Question 10 points)

- (a) What is a *persona* certificate? Why would anyone use a persona certificate? Give an example.