**Problem 1 (9 pts)** Classify each of the following as a violation of confidentiality, integrity, or some combination thereof.

* Paul makes a copy of Linda’s data.
  + Confidentiality
* Gina forges Roger’s signature on a deed.
  + Integrity
* Henry spoofs Julie’s IP address to send a message to a computer
  + Confidentiality, Integrity

**Problem 2 (6 pts)** Why can’t a block cipher have a smaller output (i.e., ciphertext block) size than the input (i.e., plaintext block) size?

* Because you would be losing data and with a smaller block there would be less security

**Problem 3 (9 pts)** For block cipher modes, under the ECB mode, if ten consecutive message blocks of the same message are the same, will their ciphertext blocks also be the same? How about in the CBC mode? How about in the Counter mode?

* In EBC mode, repeated plaintext blocks yields repeated ciphertext blocks which results in a pattern that hackers can follow. In CBC mode there is no apparent pattern left to follow. In Counter mode, you will not see any repeating blocks

**Problem 4 (10 pts)** Suppose a message has been encrypted using an old system with the basic DES algorithm under key k. (i) If the receiver of the message is running a new system with 3DES implemented. Can the receiver decrypt the ciphertext by setting k1=k2=k3=k and why? (ii) If the encryption of 3DES used the EEE mode instead of EDE and the decryption used the DDD mode instead of DED, can the receiver decrypt the ciphertext by setting k1=k2=k3=k and why?

* (i): yes they can since 3DES uses three keys of different values when they are all set equal to each other then it results in just 1 key like in DES.

P = D(K1 | K2 | K3,C) = D(K1,E(K2,D(K3,C)))

* (ii) Yes, an encryption in EEE mode can be decrypted in DDD mode since in EEE mode all keys are equal to each other it would only make sense to decrypt with all the same key too.

**Problem 5 (12 pts)** In EDE mode of 3DES, encryption of message m with keys k1, k2 and k3 works as follows: C=Ek1(Dk2(Ek3(m))), where E and D denote the encryption and decryption operation respectively. Given some pairs, how can an attacker find the three keys with effort in the order of 2112? Describe in details. (hint: meet in the middle attack)

* 3DES encryption in EDE mode makes the keys K1 = K3 with K2 being a seperate value. If a hacker were to attack after the first encryption they would be able to find the keys K2 and K3 and since K3 = K1 then the hacker has all three keys.

**Problem 6 (15 pts)** **a.** Suppose Alice shares a secret block cipher key, K with Bob, and a different secret block cipher key, KAC with Charlie. Describe a method for Alice to encrypt an m-block message such that it can only be decrypted with the cooperation of both Bob and Charlie. The ciphertext should only be a constant size greater than m blocks. You may assume that Bob and Charlie have a pre-established secret channel on which to communicate.

* You could try double encrypting the message with both Bob’s and Charlie’s keys

**b.** Now, suppose Alice shares a block cipher key, KAB with Bob, a block cipher key KAC with Charlie, and a block cipher key K with David. Describe a method for Alice to encrypt an m-block message such that any two of Bob, Charlie, and David can decrypt (for example, Bob and Charlie can decrypt), but none of them can decrypt the message themselves. Again, the ciphertext should only be a constant size greater than m blocks. (Hint: Pick a random message encryption key to encrypt the message with. Then add three ciphertext blocks to the ciphertext header.)

* You could OR every key pair together

**c.** How does your solution from part (b) scale as we increase the number of recipients? In other words, suppose Alice has a secret key with each of n recipients and wants to encrypt so that any k out of n recipients can decrypt, but any k-1 cannot. What would be the length of the header as a function of n and k?

**Problem 7 (6 pts)** It is common, for performance reasons, to sign the hash of a message rather than the message itself. Why is it so important that it be difficult to find two messages with the same message digest?

* It would be possible to forge the message without any knowledge that it was forged when two messages have the same message digest

**Problem 8 (7 pts)** Generating a signature with RSA alone on a long message would be too slow (presumably using cipher block chaining). Suppose we could do division quickly. Would it be reasonable to compute an RSA signature on a long message by first finding what the message equals (taking the message as a big integer), mod n, and signing that?

* RSA operation cannot handle anything longer than the modulo’s size and you cannot directly sign anything larger than 256 bytes

**Problem 9 (8 pts)** Prove that if H is collision resistant then so is HMAC**k(m)**=H(k|H(k|m)).

**Problem 10 (8 pts)** Suppose only public-key cryptography can be used to encrypt the communications between Alice and Bob. Alice’s public key is eA, private key is dA; Bob’s public key is eB, private key is dB. Now Bob wants to send a message m to Alice. Describe which keys should be used to encrypt the message and decrypt the ciphertext.

* Bob would grab Alice’s public key and encrypt a message with and Alice would use her private key to decrypt

**Problem 11 (8 pts)** Suppose only secret-key cryptography can be used to protect the communications between Alice and Bob. Suppose Alice and Bob already have a shared secret key k. Now Bob wants to send a message m to Alice. Which components should be included in the message to protect the integrity of the message?

**Problem 12 (6 pts)** If public key certificates do not have the CA’s signature, what will be the problem?

* Without a CA there is a greater risk of both parties getting info stolen

**Problem 13 (6 pts)** Find and list three trusted CAs in your web browser.

* Amazon Trust Service
* Atos
* Buypass

**Problem 14 (10 pts – Extra Credit)** Suppose a system is encrypting English messages. It divides each message into blocks, with 26 characters in each block, and then encrypts each block using Substitution Cipher. Design an Enhanced Substitution Cipher that can provide better security than the basic substitution cipher in the system. Analyze why your cipher is more resistant to frequency analysis than the basic version.