**EE 4953/5453 Mid-Term - Fall 2022**
**Due: Oct 12 @ 11:59 PM, Points: 100**

**FULL NAME:**
**Submission Instructions:** Typeset your answers using a word processing software and upload as pdf to Blackboard by the stated deadline. Use software tools to draw the figure as well. Use the spaces I have provided as a guideline for the max amount of text I expect for each of your answers. This is an individual exam (i.e., not group work). Do not share solutions or search for answers on the Internet. I am looking for your approach to the problem not a repetition of someone else's approach who might have already solved the problem.

1. (2 points) How does CBC mode solve the security issue with ECB mode?

2. (2 points) What is Kerckhoff's principle?

3. (2 points) Suppose a key space of $2^{30}$. Alice decides to encrypt a plaintext block 6 times with 6 different keys. What is the *effective* key space for Trudy?

4. (2 points) Consider a computer that can conduct a brute force search with a speed of $2^{40}$ keys per second. In the worst case, how many seconds does it take to search through a key space of $2^{80}$?

5. (2 points) How does a public-key cryptosystem such as RSA address the limitation of symmetric key cryptosystem such as AES?

6. (5 points) DES numerology: 64 bit block length, 56 bit key length and 16 *rounds*. How many rounds in *total* are executed to encrypt the ASCII message "ABCDEFGHIJKLMNOPQRSTUVWX" (excluding quotes) in ECB mode? in CBC mode? Explain briefly.
   Hint: An ASCII character is of size 8 bits.

7. (5 points) Consider the one-time pad encryption/decryption scheme where "Attack location XYZ" is the message, K is the key and C is the corresponding ciphertext. Trudy, through her intelligence sources, finds out that Alice was sending the encrypted version of the message "Attack location XYZ". She intercepts the ciphertext C and replaces it with $C'$ such

that the recipient decrypts to get the message "Attack location PQR". What is the value of C′? Explain.

8. (10 points) Using a figure, explain how a MAC can be computed in 3DES.

9. (10 points) Suppose Alice and Bob live in a world that only has DES in CBC mode. Assume that Alice and Bob share a key $K_{AB}$. Using only $K_{AB}$ (i.e., without deriving any other additional key), can Alice send a message to Bob while simultaneously achieving confidentiality and integrity? If yes, explain how. If no, explain why not.

10. (10 points) Consider the following DEE variation of 3DES in which you decrypt with $K_1$, encrypt with $K_2$ and encrypt with $K_1$. What is the effective key space assuming a meet-in-the-middle attack? Does it offer the same two major benefits of the original 3DES? Explain.

11. (10 points) Give 2 advantages of symmetric key crypto such as AES over public key crypto such as DH. Give 2 advantages of public key crypto over symmetric key crypto.

12. (20 points) Diffie-Hellman works for two parties. Explain clearly using a figure how you can extend Diffie-Hellman to establish a symmetric key between `three` parties. Number the message exchanges in the figure and explain the contents of each message clearly. Next, extend it such that it works for `n` parties.

13. (20 points) Suppose currently files storage services such as Dropbox and Google Drive do not offer confidentiality and integrity of data that goes over the Internet. You launch a startup called RowdyBox. RowdyBox distinguishes itself from Dropbox by addressing confidentiality and integrity of their customers' files going over the public Internet. Explain using illustrations how you would design a security architecture for RowdyBox. Identify the various concerns and show how your security architecture addresses those security concerns. Remember, you start from scratch. We do not have any pre-agreed keys, etc. Draw a figure with various entities involved, label the messages and explain. You should use the notations used in this course. Do not use any technique we have not covered so far in this course.