Q0 (5)	
Q1 (35)	
Q2 (30)	
Q3 (30)	
Bonus (5)	
Q4 (20)	
Total	
Grade	

Midterm 1
Fall 2018 – CSCE 522

Name:
Major:

Answer the following questions. Be brief and precise!
Undergraduate students need to answer questions 0 - 3. **Bonus** question is open for all students. **Graduate** and **Honors College** students need to answer all questions 0 - 4. **GOOD LUCK!**

0. 5 points
I, ____, pledge that my conduct in the course CSCE 522 adheres to the Honor Code of the University of South Carolina. I will not engage in any type of activity that is dishonest, fraudulent, or exhibit deceit of any type. Honor Code violations include: giving or receiving unauthorized assistance on test, accessing test before the scheduled time, revealing test questions to students who will take the test later, and plagiarism.

1. 35 points Cryptography
(10) Explain why triple-DES is still secure. Justify your answer based on complexity and effective key size.

(15) Consider the following message from Ann to Bob:
(**ID_Ann, ts) || E(M,K^{pub}_{Bob}) || S(h(M), K^{priv}_{Ann}) .** The message has 3 components: 1) (**ID_Ann, ts)** is plain text with Ann's identity and time stamp ts; 2) **|| E(M,K^{pub}_{Bob})** message M encrypted with Bob's public key; and 3) and **S(h(M), K^{priv}_{Ann})** the hash value of M signed with Ann's private key. Ann's identity and the time stamp are not confidential; M should be known by Ann and Bob only; and Bob should know that the message is coming from Ann and that it is not modified during transmission. Show whether the following attacks by Eve compromise any of these security requirements. Justify your answers.
a. Eavesdropping

b. Replay

(10) Extend the above message such that it is resilient against replay attack.

2. 30 points Basic Security Concepts

(15) Considering the MOM requirements of malicious attacks to succeed in the context of a hospital's surgical system. Assume that hospital have a program that allows a surgeon in one city to assist in an operation on a patient in another city via internet connection.

Describe a potential cyberattack against the system. Explain the attacker's motivation, opportunity, and methods (MOM principle)

Which security objective is violated and why?

(15) Which of the followings are true?

- Digital signature uses symmetric key technique. True \ False
  Why?

- Strong authentication requires that the users reveal their secret information. True \ False
  Why?

- DES is no longer secure because there is a major flow in the algorithm. True \ False
  Why?

- Timestamp is used to prevent against replay attacks. True \ False
  Why?

- Transposition techniques change letter frequency distribution. True \ False
  Why?

3. 30 points – Basic concepts

(15) Briefly explain the three methods of user authentication and give one advantage and disadvantage for each.

User authentication method:

Advantage:

Disadvantage:

User authentication method:

Advantage:

Disadvantage:

User authentication method:

Advantage:

Disadvantage:

(15) Consider the challenge-response-based user authentication. Describe how the security is changed if the system uses frequently asked personal information (e.g., date of birth, pet's name, school name, etc.) as the challenge. Justify your answer by explain the vulnerability of the protocol. Give details!

BONUS question 5 points
Explain the purpose of the Diffie-Hellman key exchange.

4. 20 points GRADUATE AND HONORS COLLEGE STUDENTS ONLY!

(10) Explain the use of nonces in the following protocol. Assume that Ann and Bob know each other's reliable public key. ID-A is Ann's identity, ID-B is Bob's identity. N_A and N_B are the nonces generated by Ann and Bob, respectively. E($N_{A,}$ K^{pub}_{Bob}) is the encryption of NA with Bob's public key, and E((N_A, N_B), K^{pub}_{Ann}) is the encryption of nonces N_A and N_B with Ann's public key. E(Message, $K_{session}$) is the encryption of a message "Message" with the symmetric key $K_{session}$.

Message1: Ann → Bob: ID-A || E($N_{A,}$ K^{pub}_{Bob})
Message 2: Bob → Ann: ID-B || E((N_A, N_B), K^{pub}_{Ann})
Message 3: Ann → Bob: ID-A || E(N_B, K^{pub}_{Bob})
Message 4: Bob → Ann: ID-B || E($K_{session}$, K^{pub}_{Ann})
Message 5: Ann → Bob: ID-A || E(Message, $K_{session}$)

(10) Show how the above protocol is vulnerable to men-in-the-middle attack and Eve can get the session key $K_{session}$ even if the public keys are reliable, i.e., K^{pub}_{Bob} is Bob's, and K^{pub}_{Ann} is Ann's true public keys, and Eve does not know Ann's and Bob's private keys.