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. What is the complexity, effective key size, and why?

*DES effective key size is 56 bits. If there are 3 keys K1, K2, and K3 are used for the encryption, and the attacker has pairs of (**P**laintext, **C**iphertext), to break the encryption, the attacker must perform at least: 2^56 x 2^56 = 2^112 computational steps from one direction, to generate all intermediate cypher and 2^56 computational steps from the other direction. Then, look for a match in the intermediate ciphers. 3DES is secure, because 112 bits key size is still computationally secure.*

(10) Consider the following message from Ann to Bob: **ID_Ann || E (M,$K_{session}$),** where **ID_Ann** is Ann's identity and it is concatenated with the encrypted plain text M using secret key $K_{session}$. Only Ann and Bob knows $K_{session}$. Ann's identity is not confidential; M should be known by Ann and Bob only; and Bob should know that the message is coming from Ann. Show whether the following attacks by Eve compromise any of these security requirements. Justify your answers.

a. Eavesdropping
No. The message M is encrypted by Ksession. Only Ann and Bob knows Ksession, so the eavesdropper will not be able to decrypt the message. M's confidentiality is still preserved. The attacker will know Ann's ID, but it is not confidential, so the security is not violated.

c. Replay
Yes. Eve can resend the message making Bob believe that Ann sent the message because it is encrypted by Ksession that is only known by Bob and Ann.

d. Modify
Yes. Eve can modify the ID_Ann component, and make Bob use the incorrect key or ignore the message, thus leading to denial of service attack. Also, Eve can modify the encrypted part. Depending on Eve's capability, the modification most likely makes the encrypted component not intelligent but Eve might be able to insert old messages encrypted by Ksession or delete parts without being noticed.
e. Delete

Yes. Encryption does not protect against deletion.

(15) Extend the above message such that it provides sender's authentication and verification of integrity. Show the activities at Ann's side and Bob's side as well.

Ann: : **ID_Ann || E [(M, ts)],$K_{session}$)|| S[h(M), K-privAnn]**

Ann

- *ads a timestamp, ts, to prevent replay attack. Ts is encrypted and protected against modification*
- *attaches the hash of message M and signs it with her private key*

Bob

- *decrypt second component and retrieve M and ts. Verifies ts so it is not a replay*
- *Creates a hash of the retrieved message M, call it h'(M).*
- *Uses Ann's public key to retrieve h(M) from the 3rd component.*
- *Compares h(M) and h'(M). if they are the same, Bob knows that*
    - *the message originated from Ann because no one else could have signed the hash in the 3rd component with Ann's private key.*
    - *M was not corrupted during transit.*

2. 30 points Basic Security Concepts and Authentication

(15) Considering the MOM requirements of malicious attacks to succeed in the context of a hospital's surgical system. Assume tht 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. Fill out the following table by describing the MOM requirements, give <u>an example/capability</u> of potential attacker for each requirement, and a defensive control to block attacker's actions.

Describe the requirement	Potential offensive action	Defensive control
M_ethod: have the skills and tools to carry out the offensive action	*Multiple good answers possible*	*Multiple good answers possible*
O_pportunity: have the opportunity (e.g., access to the resources, lack of surveillance, no authentication, etc.)	*Multiple good answers possible*	*Multiple good answers possible*
Motivation: why to carry out the offensive action. E.g., financial reward, ideology, disgruntlement, etc.	*Multiple good answers possible*	*Multiple good answers possible*

(15) Which of the followings are true?

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

Digital signatures require the use of private key, which is public-key encryption method

- AES is computational secure, so we can always use it in the future. True \ [✓ False]
  Why?

AES is computationally secure, meaning that based on current technology, the brute force attack to generate all possible keys of size 128, 256 is infeasible. In the future, with faster computers, the AES key size may not be secure any longer.

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

The problem is the effective key size of 56 bits (vulnerable to brute force attack). The algorithm is still secure.

- RSA is not stronger than DES if they both have the same key size. [✓ True] \ False
  Why?

Brute-force attack aims to generate all possible keys for decryption. The key size will determine the number of computational steps, i.e., 2^n if n is the key size.

- Substitution techniques cannot change letter frequency distribution. True \ [✓ False]
  Why?
  Substitution will change letter frequency because each plaintext character is replaced by a cipher text. Polyalphabetic substitution will break down letter frequency correlation.

3. 30 points – Basic concepts and Crypto

(15) Briefly explain the three methods of user authentication.

- ○ *What the user knows (see lecture notes for explanation)*
- ○ *What the user has (see lecture notes for explanation)*
- ○ *What the user is (see lecture notes for explanation)*

(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.

Challenge-response is based on the system sends a challenge to the user to be authenticated. If the user submits the correct response, the user is authenticated. If the answer for the challenge is known, a different user may be correctly answer the challenge, thus will be incorrectly authenticated.

BONUS question 5 points

Explain the steps of Diffie-Hellman key exchange.

See lecture notes for answer. Note, Diffie-Hellman Key exchange is used for agreeing on a shared symmetric key over insecure channel. It is NOT an encryption method.

4. 20 points GRADUATE AND HONORS COLLEGE STUDENTS ONLY!

(10) Explain the use of nonces in the following protocol. Assume that Alice and Bob know a previously agreed secret key K, N_A is the nonce generated by Alice, N_B is the nonce generated by Bob. E(M,K) represents the encryption of M with K.
Nonces are used for authentication. The idea is that the recipient of the nonce will return the nonce, proving that s/he knows a secret without revealing the secret. Nonces must be random and not-predictable.

Message1: Alice → Bob: N_A

Note: NAis not protected any malicious user can see and modify it. If Bob sees an nonce that he has received previously, he knows that it is replay.

Message 2: Bob →Alice: $N_B || E(N_A, K)$

Bob returns NA encrypted by a symmetric key K, that is known by Alice and Bob only. Alice knows that the message is coming from Bob because noone else can generate E(NA, K) also, that message2 is the response for message1 from Alice. Bob also sends a new nonce to Alice, to verify Alice's identity.

Message 3: Alice → Bob: $E(N_B, K)$

Alice returns NB encrypted by a symmetric key K, that is known by Alice and Bob only. Bob knows that the message is coming from Alice because noone else can generate E(NB, K) also, that message3 is the response for message2.

(10) Show how the above protocol is vulnerable to men-in-the-middle attack even if the attacker does not know the shared secret key K.

Message1: Alice → Bob: N_A

Eve intercepts the message

Message1': Eve → Bob: N_A

Message 2: Bob →Eve~~Alice~~: $N_B || E(N_A, K)$

Eve forwards the message to Alice.

Message 3: Alice → Bob: $E(N_B, K)$
Eve intercepts the message
Message 3: Eve~~Alice~~ → Bob: $E(N_B, K)$

Eve forwards the message to Bob for verification of NB.