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

Midterm 1
Fall 2017 – 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) A good cipher must have been carefully examined by experts. Explain the rationale for this requirement. Give a brief example of security risk if this requirement is not satisfied.

Characteristics	**Rationale**	**Example**
The cipher must have been carefully examined by experts.		

(25) Consider the following cryptographic protocol that allows Alice and Bob to establish a secret session key (K_{AB}). Alice and Bob use the following protocol, where E[M, K] denotes the encryption of message M with key K, Id_A, Id_B, are the identities of Alice and Bob, KE-A, KE-B are the public keys of Alice and Bob, and N_A, N_B are nonces generated by Alice and Bob, respectively.

Message 1: Alice → Bob: **E[(Id_A, K_{AB}, N_A), KE-B]**
Message 2: Bob →Alice: **E[(Id_B, K_{AB}, N_A, N_B), KE-A]**
Message 3: Alice →Bob: **E[N_B, K_{AB}]**
Message 4: Bob →Alice: **E[M, K_{AB}]**

Eve is a malicious user. Eve's public key is KE-E. Assume that Eve can trick Bob into believing that KE-E is Alice's public key. Show and explain the steps and messages Eve must do to disclose **K_{AB}, M** such that Bob or Alice won't know that Eve knows **K_{AB}.**

2. 30 points Basic Security Concepts

Complete the following table. I have gave a sample answer for confidentiality.

A	B	C	D
	Give an **example of the objective** in column A, using the context of university	Describe an **attack** that would violate the objective of your example described in column B	Describe a **security control** that would prevent the security violation of column C
confidentiality	Students' grades must remain confidential at all time. Only the student and the professor should know a student's grade.	A laptop containing student grades is stolen. The attacker logs in to the laptop and accesses the grade info.	Store grades in encrypted file and require biometrics-based authentication for login. Use physical security.
integrity			
availability			
authenticity			
non-repudiation			

3. 30 points – Basic concepts and Crypto

(15) Which of the followings are true?

- Multiple simple alphabetic substitutions increase security over a single simple alphabetic substitution.
  - True \ False
  - Why?

- Multiple transpositions increase security over a single transposition.
  - True \ False
  - Why?

- Polyalphabetic substitution increases security over multiple simple alphabetic substitutions.
  - True \ False
  - Why?

- Combination of a transposition and a substitution result in unbreakable cypher.
  - True \ False
  - Why?

(15) Malicious users must have three things to succeed: motivation, opportunity, method. Consider the previous threat of cyber attacks against automobiles causing accidents. Give a brief example (1-2 sentences) for each MOM aspect.

Motivation:

Opportunity:

Method:

BONUS question 5 points
What is the difference between security policy and security mechanism?

4. 20 points GRADUATE AND HONORS COLLEGE STUDENTS ONLY!
(5) What is the main purpose of using hash functions?

(15) A hash function is second-preimage resistant (weak collision resistant) if it is computationally infeasible to find any second input which has the same output as any specified input. Consider the message: **Ann → Bob: E(M, KE-B) || Sign(h(M), KD-A)**, where KE-B is Bob's public key, KD-A is Ann's private key, h(M) is the hash value of plain text M. Show how Eve can attack this message if the function h is not second-preimage resistant.