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

Midterm 1
Fall 2017 – CSCE 522

Name: Csilla Farkas
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, ________Csilla Farkas________________, 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.	Developers of the cipher may miss serious vulnerabilities and weaknesses of the cipher, due to: • Lack of awareness • Lack of skills • Not understanding attackers' capabilities • Etc. 5 points	Cipher with non-obvious security flaw may be used to protect highly sensitive data. Attackers can exploit this weakness to access sensitive data. 5 points

(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, whose public key is KE-E. Assume that Eve tricks Bob into believing that KE-E is Alice's public key. Show the steps and messages Eve must generate to disclose **K_{AB}** and **M** without Bob or Alice detecting that Eve knows **K_{AB}.**

Message 1: Alice → Bob: E[(Id_A, K_{AB}, N_A), KE-B] 3 points

- Eve does nothing with this message
- Bob uses his own private key KD-B to decrypt Id_A, K_{AB}, N_A
- Bob generates the response message for Alice, and encrypting it with the incorrect KE-E

Message 2: Bob → Alice: E[(Id_B, K_{AB}, N_A, N_B), KE-E] INTERRUPTED! 8 points

- Eve interrupts this message before arriving to Alice
- Note, the message is encrypted by KE-E, therefore Alice can decrypt its content using her KD-E
- After decrypting, Eve knows Id_B, K_{AB}, N_A, and N_B
- Eve generates a new message and sends it to Alice, pretending to be Bob:

New message 2: Eve(masquerading as Bob) → Alice: E[(Id_B, K_{AB}, N_A, N_B), KE-A] 8 points

- Alice does not know that the message was sent by Eve
- Alice sees N_A and K_{AB} that she has sent to Bob, encrypted by Bob's public key. Noone else but Bob could have decrypted the first message from Alice to Bob.
- Alice believes that only she and Bob knows KAB

Message 3: Alice → Bob: E[N_B, K_{AB}] 3 points

- Eve can eavesdrop in the communication and decrypt the message since Eve knows K_{AB}

Message 4: Bob → Alice: E[M, K_{AB}] 3 points

- Eve can eavesdrop in the communication and decrypt the message M since Eve knows K_{AB}

2. 30 points Basic Security Concepts

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

Note, multiple answers are possible. Here are some examples:

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 2.5 points each	Students' grade must be correct (should be the grade they received in the class)	Attacker launches a SQL injection attack to change a grade	All use supplied input should be validated by the system
availability	Students' grade and transcript should be available whenever it is needed for the student or university.	Attacker has physical access to the registrar's computer and destroys the entire computer system.	Physical security and system back up stored at a different location.
authenticity	Only course instructors who teach a course should enter or modify students' grades.	Attacker guesses the password for the instructor who teaches the class, logs in as the instructor and submits grades.	Require multifactor authentication for login to the registrar's system.
non-repudiation	When a grade is modified by an instructor for the course, the instructor cannot deny that he/she modified the grade.	Attacker forges an email message to the registrar, requesting a grade modification. The attacker spoofs the instructor's IP address and pretend to be the instructor.	Require digital signature for all grade modifications.

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 1 points
  - Why? 3 points

  Multiple simple alphabetic substitution can be replaced with a single substitution. No additional security results from repeating it several times. E.g., A → i than i → k is equivalents with A → k

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

  When you "mix up" the plain text characters multiple times, it increases the diffusion. E.g., small patterns that remained after the first transposition are broken up.

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

  A plain text character is substitutes by more than a single cipher character. This removes patterns and letter frequencies that could be used by the cryptanalyst to break the encryption. E.g., the plain text character A is replaced by b in odd positions, and h in even positions.

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

  There is only one unbreakable cipher, that is the Vernon one-time pad. All others are computationally secure, that is, based on the current computing power, it is infeasible to brute-force break the encryption. Indeed, widely used symmetric key encryption algorithms, such as DES and AES, are based on combining substitution and transposition.

(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.

Note, multiple answers are possible. Here are some examples:

Motivation: 5 points

The attacker is working for the competition and wants to lower the trust in the automobiles manufactured by the competing manufacturer.

Opportunity:

The attacker has discovered a vulnerability of the in-vehicle communication of the automobile. For example, the authentication mechanism is insufficient. The attacker is in the physical vicinity of the targeted automobile that is stopped at a red light in an intersection.

Method:

The attacker logs into the in-vehicle communication, overrides the drivers commands and make the vehicle drive into the intersection while the traffic light is still red.

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

Policy determines what to protect. Often high-level description, independent from technologies.

Mechanism determines how to protect (i.e., what technologies to use)

4. 20 points GRADUATE AND HONORS COLLEGE STUDENTS ONLY!

(5) What is the main purpose of using hash functions?

Provides means for integrity verification. Any change in a message M will result in a different hash value.

(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.

- Eve intercepts E(M, KE-B) || Sign(h(M), KD-A) 1 point
- Eve verifies signature using Ann's public key KE-A on Sign(h(M), KD-A) . Eve knows h(M) 2 points
- Eve tries to find a message M' such that h(M') = h(M). If found, 2 points
- Eve send a message to Bob, pretending to be Ann:
  Eve (pretending to be Ann_ → Bob: E(M', KE-B) || Sign(h(M), KD-A) 2 points
- Bob get h(M) from Sign(h(M), KD-A) using Ann's public key KE-A 2 points
- Bob decrypts M' from E(M', KE-B) using his own private key KD-B 2 points
- Bob generates hash from M' and compares h(M') with h(M) 2 points
- If h(M') = h(M), Bob believes that the message originated from Ann and M' is the original, uncorrupted content. 2 points