

ECE 3170

Cryptographic Hardware for Embedded Systems

Midterm I

October 9, 2025

*This test is open book for the Schneier textbook and the optional textbooks. This test is also open note. Calculators are permitted but no programs may be used. Open notes include electronic notes with any handwritten or typed information you may have added. For electronic notes, all wireless connectivity must be turned off, and cell phones are not allowed; in other words, no connection to any information source outside of the classroom is allowed during the exam. Open notes also include all course assignments (homeworks or labs) as well as solutions (including both your solution as well as official solutions posted on the course website). All aspects of the Georgia Tech Honor Code apply. Please follow the instructions precisely. If you need to continue a problem, please use the back of the **previous** page. The meaning of each question should be clear, but please state any assumptions and ask for clarification if necessary.*

You can do it!

Name (Please print)_____

This test will be conducted according to the Georgia Tech Honor Code. I pledge to neither give nor receive unauthorized assistance on this exam and to abide by all provisions of the Honor Code.

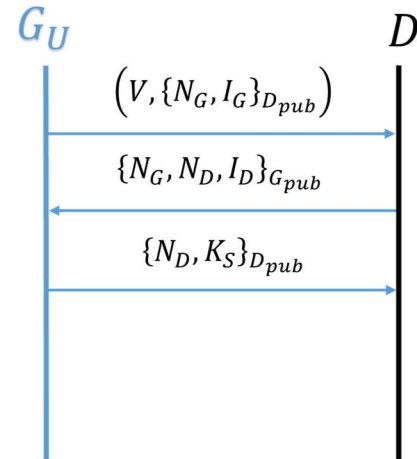
Signed_____

Question	Score	Max
1		15
2		10
3		15
4		15
5		10
6		10
Total		75

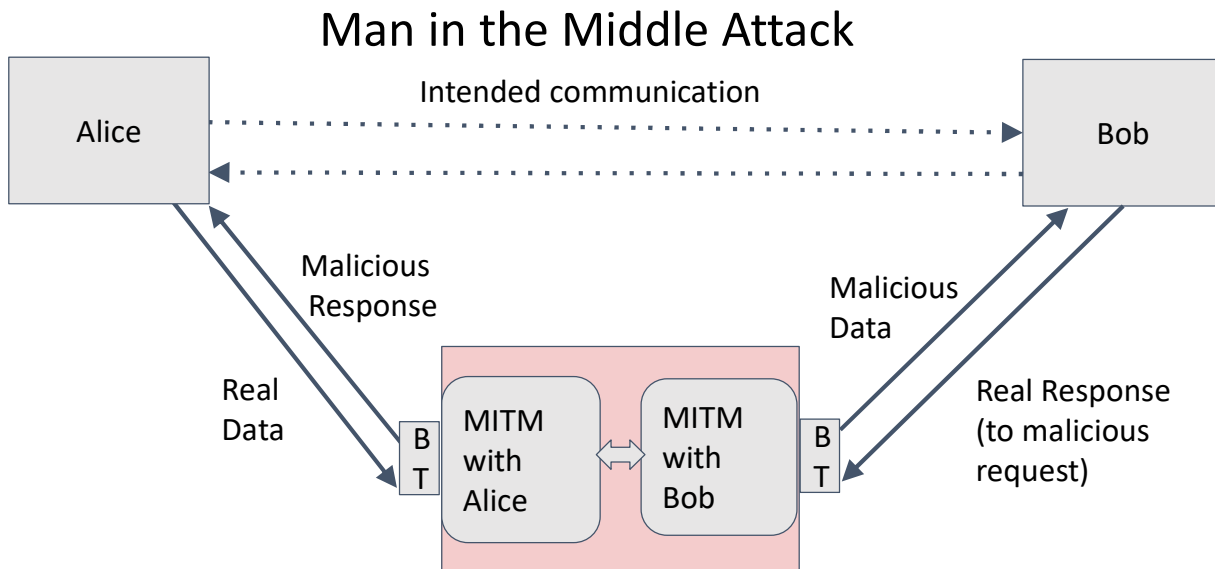
1. (15 pts.) Man in the Middle Attack.

Consider authentication using public key cryptography in the following diagram from lecture:

1. Organization nonce N_G and identifier I_G sent to device
2. Device retrieves N_G , then appends its own nonce N_D and identifier I_D
3. Finally, organization responds with N_D and symmetric key K_S



Furthermore, assume that public keys have not yet been exchanged and that a Trusted Third Party (TTP) or Certificate Authority (CA) exists but can be spoofed; in other words, Mallory can intercept requests for public keys. Finally, please consider the following diagram from Lecture 14 Authentication II. Please note that “BT” stands for BlueTooth, but any form of communication can be used (e.g., wired Ethernet, 802.11 or radio).



Part (b) on the next page asks you to describe the first 5 or 6 steps of the classic Man-in-the-Middle (MITM) attack, while part (a) asks for any assumptions that you believe need to be stated to help explain the steps.

(Please turn to the next page!)

(a) (5 pts.) Please state any assumptions which you believe to be necessary to properly understand your answer to part (b) below (hint: you may wish to start to answer the next question below first, and then you may return here to write down your assumptions as necessary). If you believe that no additional assumptions are needed, please state that no additional assumptions are necessary.

(NOTE: Because this is a test, Prof. Mooney cannot during the exam answer questions about whether or not your stated assumptions are correct or not – part of this test question is your ability to properly state correct assumptions!!)

(b) (10 pts.) What are the first 5-6 steps of the MITM attack? Focus on the standard authentication protocol shown on the previous page utilizing public-key cryptography together with symmetric-key crypto (for the session). Please include sufficient detail to explain how Mallory is able to decrypt both Alice's and Bob's messages. The assumptions stated above in part (a) will guide the interpretation of your answer. Please note that the specific steps may vary with many correct answers to this question; minor variations in steps will not lose points as long as there is clarity regarding Mallory's ability to decrypt.

Please do not give more than 10 steps or you will lose points. Obviously, giving less than five steps will also lose points. Is it OK if some of the steps are not fully described as long as how Mallory can encrypt and decrypt messages is clearly explained.

2. (10 pts.) Padding Technique.

Someone on your team proposes a new padding technique. The idea is to count upwards from the least significant byte. Let us consider 64 bits only (eight bytes), and the minimum padding length is one while the maximum is eight.

For example, consider the following message m_2 consisting of six bytes (one per letter):

ATTACK

For simplicity, assume that an eight-byte padded ciphertext c_2 encoding of the above is representative of our scenario. Given the new padding technique, the message results in the following:

0xFE3838FEC21B0201

For another example, consider the following message m_2 consisting of four bytes (one per letter):

TACK

For simplicity, assume that an eight-byte padded ciphertext c_2 encoding of the above is representative of our scenario. Given the new padding technique, the message results in the following:

0x38FEC21B04030201

Do you anticipate any problems with this new padding approach? If so, please clearly state at least one problem which is significant. If you do not see any problems, please state that the new padding approach has no problems and write at least two sentences explaining why you think that the new padding approach will work just fine. Please limit your answer to 10 sentences or less (math equations do not count towards the number of sentences).

3. (15 pts.) Position Attack on Encryption with a One-Time Pad.

Consider the use of a one-time pad (OTP) to encrypt a bank deposit with the following format:

Routing Number	Check Number	Amount
----------------	--------------	--------

The adversary knows this format, and for simplicity let us assume each field is an 8-bit value unsigned (i.e., no negative numbers, so each field may contain zero through 255). For example, a deposit with routing number 254, check number 128 and amount \$1 would have the following plaintext:

11111110	10000000	00000001
----------	----------	----------

Now for the scenario. Given the above example, i.e., suppose the adversary knows that a check deposit of \$1 has been initiated but has not been processed, e.g., the adversary intercepts the following encrypted deposit and can alter it:

11101100	01110000	10010111
----------	----------	----------

In summary, through other means the adversary observed the bank deposit above and knows that a deposit of \$1 is encrypted with OTP which the adversary does not know (the adversary does not possess the bit values of the one-time pad).

(a) (5) Suppose a deterministic hash is used without a key (i.e., the hash is keyless). Furthermore, assume that the hash is calculated on the encrypted value. Can the adversary recalculate the hash after altering the encrypted bank deposit, and will this recalculated hash value be accepted by the bank? Why or why not? For full credit, you must clearly explain your answer and state any and all assumptions you believe to be necessary to support your answer; a vague or unclear answer – or an answer depending on unstated and unexplained assumptions which are necessary and non-obvious – will lose points.

(b) (10) Regardless of your answer to part (a), suppose that the adversary can alter the encrypted deposit and can do so undetected; in other words, the adversary has intercepted the packet in transit and can alter any of the following bits undetected by the bank:

11101100	01110000	10010111
----------	----------	----------

Can the adversary flip a single bit and guarantee that the deposit amount has increased? If not, why not? If so, what is the maximum amount of increase in deposit amount that the adversary can cause by flipping one and only one bit? For full credit in case of a correct answer, and for partial credit in case of an incorrect answer, please explain your answer in detail but with 10 sentences or less; any lack of clarity in your answer will result in lost points.

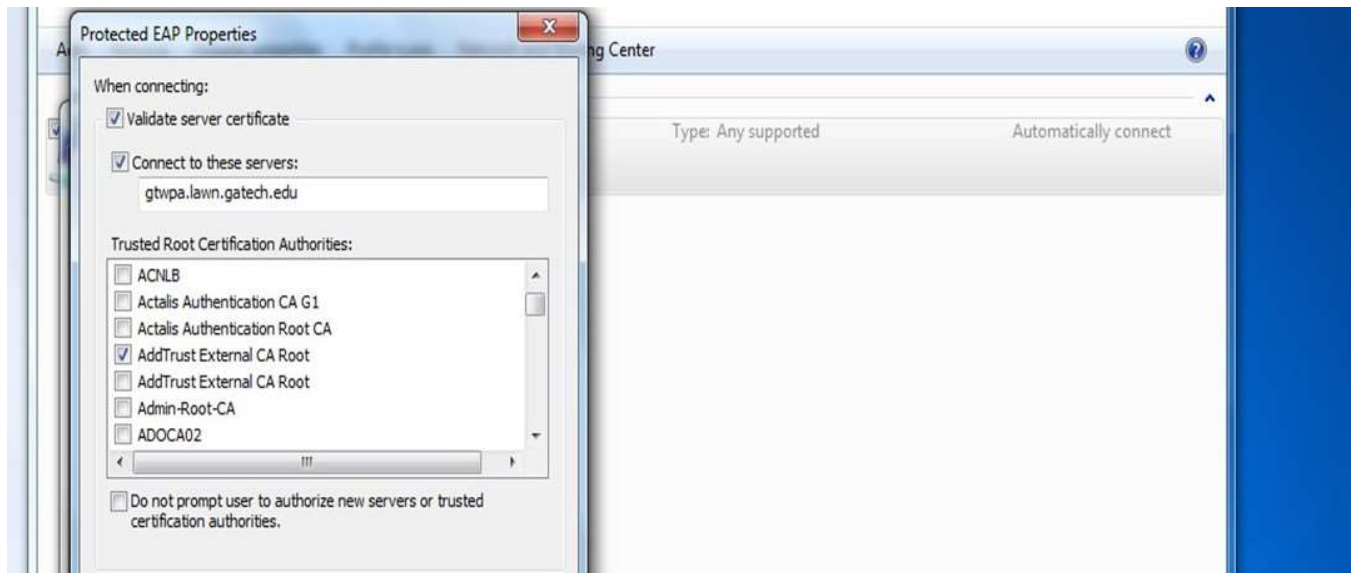
4. (15 pts.) The Interlock Protocol.

Consider the interlock protocol where the first message sent always has the following format: `NameMonthDayYearHourMinutes` using two-digit numbers for all fields except for `Name`. For example, at the beginning of this exam Bob would have sent the message `Bob0925251400` (note that the two digits for `Hour` are in 24-hour format) and Alice would have sent the message `Alice0925251400`.

Assuming that Mallory knows the message format (as described in the previous paragraph) that Alice and Bob will use to initiate encrypted communication using the Interlock Protocol, but that Mallory does **not** have any reset capability (i.e., Mallory **cannot** reset the connection in the middle of the Interlock Protocol), is it possible for Mallory to successfully carry out a Man-in-the-Middle (MitM) attack? If so, clearly explain how and show some of the key (i.e., most important) steps to do so. If not, clearly explain why not and show some of the key steps where Mallory fails to succeed. (Please note that a correct “yes” or “no” answer without a valid explanation and clearly explained steps will earn zero points.)

5. (10 pts.) Class Discussion.

Consider the following screenshot:



As discussed in class, what is worrisome about this screenshot and why? Please explain your answer in detail, including all concepts used in your answer.

6. (10 pts.) Combining Encryption with Message Integrity.

The three main methods to combine message integrity with encryption are (i) encrypt and authenticate, (ii) authenticate then encrypt and (iii) encrypt then authenticate. Of the three possible methods, if only a keyless hash such as MD5 (or SHA2) is available, which method is the most suitable and why? You do not have to “prove” beyond a doubt that your answer is the best; you only need to explain intuitively why it is likely to be better than the other two options. For full credit you are required to give at least one plausible reason why the option you choose for your answer is more suitable, and the correct choice without any valid reason given at all will earn zero points. Finally, you must limit your answer to 10 sentences or less.

THIS IS THE LAST PAGE OF THE EXAM!