ECE 4156/6156

Hardware-Oriented Security and Trust

Midterm I

February 29, 2024

This test is open book for the required as well as 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 open books, open notes and the course website 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!

Question	Score	Max
1		**10**
2		**10**
3		**5**
4		**5**
5		**10**
6		**10**
7		**10**
Total		**50 or 60**

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_____

1. **(10 pts.) Diffie-Hellman.**

Consider the first step in Diffie-Hellman key exchange: the choice of an appropriate prime number p and generator α of $\mathbf{Z}_p^*$.

(a) (5 pts.) Regarding α, what does it mean for α to be generator of $\mathbf{Z}_p^*$? Please do not refer to any specific proposed value of p, α or $\mathbf{Z}_p^*$; instead, please give a high-level, general explanation valid for any specified proposed values of p, α or $\mathbf{Z}_p^*$. Also, explain your answer using words and concepts and do not explain exclusively or even primarily using mathematical equations. To help, you could consider that you are talking to a friend on the phone who has the same overall ECE background at the same level as you but is not taking this class. Please limit your answer to 10 sentences or less.

(b) (5 pts.) Now consider $p = 21$, i.e., consider $\mathbf{Z}_{21}^*$. Is $\alpha = 6$ a generator for $\mathbf{Z}_{21}^*$? Why or why not?

2. **(10 pts.) CPA Security.**

Let F be a pseudorandom function. To encrypt $m \in \{0,1\}^{4n}$, parse m as $\langle m_1, m_2, m_3, m_4 \rangle$ with $|m_1| = |m_2| = |m_3| = |m_4|$, then choose uniform $r \in \{0,1\}^n$ and output the ciphertext $\langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r+1), m_3 \oplus F_k(r+2), m_4 \oplus F_k(r+3) \rangle$.

Is this encryption scheme CPA-secure? If so, give at least one intuitive reason why. If not, provide one valid reason why not. (Please do not write more than 10 sentences or give multiple reasons; if you do write a long answer please indicate which part of the answer you want graded, otherwise answers longer than 10 sentences will receive zero points.)

3. **(5 pts.) CBC versus Counter Mode.**

You are an engineer at a company performing consultations for security implementations. Two clients have the following applications:

(i) Encrypted messages between a bank and a client are periodically sent. The messages are large (i.e., much greater than 128 bits) and comprise banking transactions.

(ii) An online video streaming service streams encrypted audio to clients on a busy network. Some errors in the unencrypted audio files or dropped message blocks are acceptable, but delays in service are not.

For each application (i) and (ii) above, state whether you would recommend the usage of either Cipher Block Chaining (CBC) or Counter (CTR) mode of operation. For full credit, state any assumptions you have about the application scenarios (i) and (ii); furthermore, make sure to state the reasoning for choosing the mode of operation for each application scenario.

4. (10 pts.) Secret Sharing.

Consider a secret sharing scenario where $N = 4$ and $t = 2$. There are four company executives where 2 out of the 4 must be present in order to enter their password information and open the safe. Now consider the case of a 10-bit key. This key will be calculated from the inputs provided by any two of the executives.

The computer system generating the keys has provided the first key share to one executive as follows:

Executive 1: (100, 450)

(a) (5 pts.) Given the key share above assigned to Executive 1, assign three more key shares to Executives 2 through 4 such that any two shares will combine to give a consistent and valid (i.e., 10-bit) key. For full credit please provide the **key**, the **four secret shares** and the mathematical **equation** from which the shares were derived.

(b) (5 pts.) The company suspects foul play and believes an additional secret share has been produced which will create the correct (valid) key when paired with another secret share. Are there any mechanisms inherent to secret sharing that the company can utilize to detect which secret share may be the forged secret share? For full credit state all assumptions for why you can or cannot detect the forged secret share.

5. **(5 pts.) (i) Encrypt-and-Authenticate.**

One method to utilize a tag with encryption is known as (i) encrypt-and-authenticate. Assuming that the tag is being calculated with SHA256, please provide one reason why (i) encrypt-and-authenticate is generally not preferred. Please give the best reason you can think of; any valid reason will receive partial credit, but for full credit there is one reason which is particularly impactful.

6. **(10 pts.) (ii) Authenticate-then-Encrypt versus (iii) Encrypt-then-Authenticate.**

In addition to (i) encrypt-and-authenticate, two additional methods to utilize tags with encryption are (ii) authenticate-then-encrypt and (iii) encrypt-then-authenticate. Assuming that the tag is being calculated with SHA256, which of these two methods is better and why? Please note that the correct answer without a valid reason will lose most of the points for this problem; furthermore, even if the reason given is valid, only partial credit will be earned if the reason is not a high impact reason. In summary, please clearly explain the reason for your choice of (ii) authenticate-then-encrypt versus (iii) encrypt-then-authenticate when the tag is being calculated with SHA256. If you give multiple reasons, you are required to indicate which reason you believe to be the most important (i.e., the highest impact).

7. **[ECE 6156 only!] (10 pts.) New MAC for messages of length 2n-2.**

Let F be a pseudorandom function. As usual, assume that the MAC has access to a key generation function Gen which outputs a uniform $k \in \{0,1\}^n$. Consider the following construction for messages of length $2n$-2:

To authenticate a message $m = m_1, m_2$ where $m_i \in \{0,1\}^{n-1}$, compute $t := F_k(0 \parallel m_1) \parallel F_k(1 \parallel m_2)$.

Is this MAC construction secure? Keep in mind that the length is fixed to only and always be $2n$-2 (any length other than $2n$-2 is not allowed; neither the sender nor receiver accepts any messages of invalid length, including the oracle). Please note that the correct answer (secure versus insecure) will earn at most half of the points for this problem; for full credit you must explain at least one clear and valid reason for your answer – vague and/or unclear reasons will not be accepted for credit.

THIS IS THE LAST PAGE OF THE EXAM!