ECE 4156/6156

Hardware-Oriented Security and Trust

Midterm I

March 1, 2023

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!

Name (Please print)___________________________________

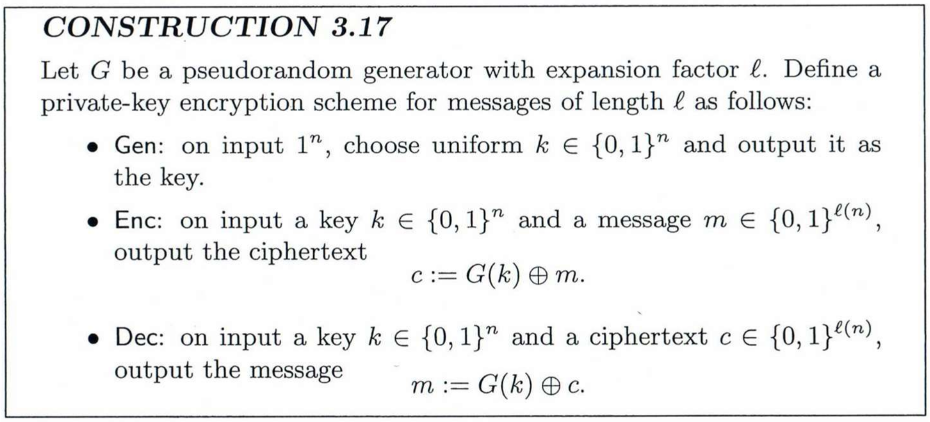
This test will be conducted according to the Georgia Tech Honor Code. I pledge to neither give nor receive unauthorized assistance on this exam and to abide by all provisions of the Honor Code.

Signed___________________________________

Question	Score	Max
1		**15**
2		**10**
3		**15**
4		**10**
5		**10**
6		**10**
Total		**60 or 70**

1. **(15 pts.) Eavesdropper secure versus CPA secure.**

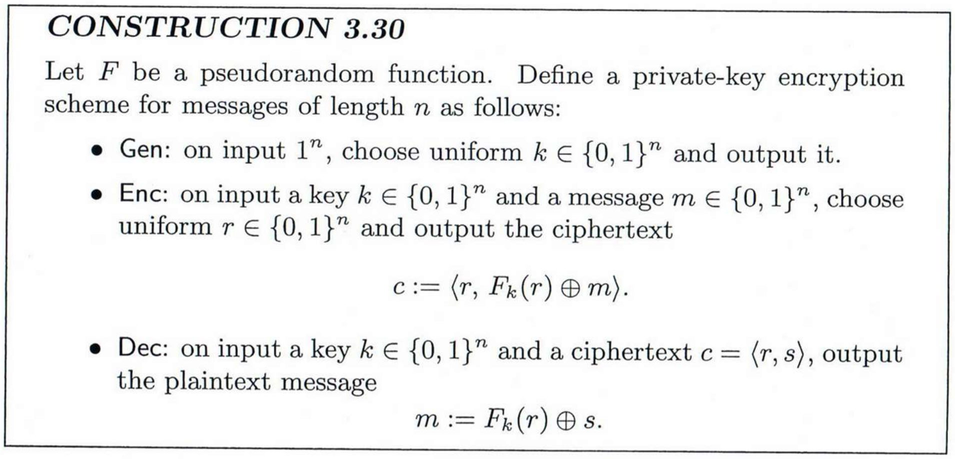
Two ways to classify an encryption scheme π_E = (Gen, Enc, Dec) is by (i) security against an adversary only with eavesdropped ciphertext (EAV-secure) and (ii) security against an adversary with the ability to obtain a polynomial number of arbitrary plaintext-ciphertext pairs (CPA-secure). The following two constructions were introduced in this context:



CONSTRUCTION 3.17

Let G be a pseudorandom generator with expansion factor ℓ. Define a private-key encryption scheme for messages of length ℓ as follows:

- Gen: on input 1^n, choose uniform $k \in \{0,1\}^n$ and output it as the key.
- Enc: on input a key $k \in \{0,1\}^n$ and a message $m \in \{0,1\}^{\ell(n)}$, output the ciphertext
$$c := G(k) \oplus m.$$
- Dec: on input a key $k \in \{0,1\}^n$ and a ciphertext $c \in \{0,1\}^{\ell(n)}$, output the message
$$m := G(k) \oplus c.$$



CONSTRUCTION 3.30

Let F be a pseudorandom function. Define a private-key encryption scheme for messages of length n as follows:

- Gen: on input 1^n, choose uniform $k \in \{0,1\}^n$ and output it.
- Enc: on input a key $k \in \{0,1\}^n$ and a message $m \in \{0,1\}^n$, choose uniform $r \in \{0,1\}^n$ and output the ciphertext
$$c := \langle r,\, F_k(r) \oplus m \rangle.$$
- Dec: on input a key $k \in \{0,1\}^n$ and a ciphertext $c = \langle r, s \rangle$, output the plaintext message
$$m := F_k(r) \oplus s.$$

(a) (2 pts.) Is Construction 3.17 CPA-secure? Please add one sentence explaining your answer, but a correct “yes” or “no” answer to this question (and one or more explanatory sentences) will earn full credit.

(b) (2 pts.) Is Construction 3.30 EAV-secure? Please add one sentence explaining your answer, but a correct “yes” or “no” answer to this question (and one or more explanatory sentences) will earn full credit.

(c) (11 pts.) In the PrivK experiment, the adversary A chooses m_0 and m_1 and receives back ciphertext; let us refer to this ciphertext as the *challenge ciphertext*. For the CPA-secure game $\mathrm{PrivK}^{\mathrm{cpa}}_{A,\pi}(n)$, the adversary A has oracle access to use Construction 3.30 to encrypt any messages, including m_0 and m_1. Therefore, suppose that A submits m_0 to the encryption oracle for Construction 3.30. Can A use the response to figure out if the challenge ciphertext is for m_0 versus m_1 with a greater than negligible chance of success? In other words, for Construction 3.30 and CPA security, it is given that the adversary A can use oracle access to Construction 3.30 to encrypt message m_0 and m_1. Therefore, can the adversary A use the response from submitting m_0 to Construction 3.30 to achieve a better than negligible probability of success in guessing whether or not the *challenge ciphertext* is from m_0 or m_1? Why or why not? Please explain your answer clearly and unambiguously. A correct "yes" or "no" answer without a valid explanation or reason will earn zero points. Please limit your answer to 10 sentences or less.

2. **(10 pts.) CBC-MAC.**

Let F be a pseudorandom function, and let Gen output a uniform $k \in \{0,1\}^n$. Consider usage of a CBC-MAC where the receiver only accepts 5-block messages (so $\mathrm{Vrfy}_{\mathrm{k}}(m, t) = 1$ only if m has length 5*n* and t = $\mathrm{Mac}_{\mathrm{k}}(m)$), but the sender authenticates messages of any length a multiple of 5*n* (i.e., 5*n*, 10*n*, 15*n*, etc., any multiple of 5*n*). Can the adversary forge a valid tag on a new message and fool the receiver? Please note that a correct “yes” or “no” answer without a clear and unambiguous explanation will earn zero points. Please limit your answer to 10 sentences or less.

3. **(15 pts.) One-time Pad.**

Alice wants to send Bob a message using a one-time pad, and so Alice and Bob meet in person and exchange a random bitstring of length *n*. Each message is of size *m* where *m* ≤ *n*.

(a) (5 pts.) Suppose Alice sends a message m_1 to Bob but then reuses the one-time pad from the beginning to send another message m_2. Show than an eavesdropper can easily obtain the XOR of the two messages.

(b) (5 pts.) Suppose Alice wants to use the one-time pad to send multiple messages to Bob. Can Alice use the same one-time pad for all of the messages? Explain why or why not. If any assumptions may be needed, please state any and all such assumptions clearly and unambiguously.

(c) (5 pts.) Suppose that Alice encrypts her message using the one-time pad, but she accidentally flips one bit of the ciphertext during transmission. What is the effect of this error on the decrypting of the message by Bob?

4. **(10 pts.) Message Authenticate Codes.**

Consider a MAC scheme based on a pseudorandom function *F* where the tag is computed for messages of length *n* as follows: $t := F_{\mathrm{k}}(m) \oplus k$. Assuming that the key k of length *n* is from a true random number generator and that only messages of length *n* are authenticated, is this MAC scheme secure? If so, please explain with at least one clear intuitive reason as to why. If not, provide an attack that breaks the security of the scheme. Please note that one counterexample is sufficient to show that a MAC scheme is insecure. For full credit, please limit your answer to 10 sentences or less (math equations do not count towards the 10-sentence limit!).

5. **(10 pts.) The S-Box in AES.**

Why is the S-Box critical to the success of AES? In other words, considering the SubBytes operation in AES which can be implemented by a look-up table called an S-Box, what does SubBytes (S-Box) provide that is unique when compared to the other AES operations of ShiftRows, MixColumns and AddRoundKey?

6. [ECE 6156 only!] (10 pts.) Adding an Initialization Vector to SHA-256.

Do you think that SHA-256 can be modified to use the concept of an initialization vector? If so, please propose a specific modification. If not, please explain why not with at least one intuitive reason which is clearly articulated and unambiguous. Please limit your answer to 10 sentences or less excluding math equations and drawings (i.e., there is no limit on the number of math equations or drawings you may provide in your answer!). If you write more than 10 sentences, please circle the sentences that you want graded.

THIS IS THE LAST PAGE OF THE EXAM!