ECE 4156/6156

Hardware-Oriented Security and Trust

Final Exam

April 25, 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 no cell phone is allowed; in other words, no connection to any information source outside of the open books, notes and items downloaded from 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 or passed out for previous exams). 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		**5**
2		**10**
3		**10**
4		**15 or 30**
5		**10**
6		**30**
7		**15**
8		**15**
9		**10**
10		**10**
Total		**120 or 145**

1. **(5 pts.) NIST Test Suite for Random and Pseudorandom Number Generators.**

   Why might some NIST random number tests pass while others fail when evaluating number sequences for randomness? For full credit include an explanation of at least two different tests performed by the NIST statistical test suite, with clear reasoning of why one test would pass while the other test would not pass. Do not base your answer on whether or not the number sequence was in fact generated by a TRNG versus a PRNG; instead, please base your answer on specific bit patterns in the sequence under test.

   Please limit your answer to 10 sentences or less. If you write more than 10 sentences, please circle or otherwise clearly indicate which 10 sentences you want graded.

2. **(10 pts.) SRAM PUFs.**

(a) (5 pts.) You would like to utilize an SRAM PUF to generate a key of length 256 bits. In order to be space efficient, it would be beneficial to only dedicate enough silicon to the PUF to create no more than 256 SRAM cells; therefore, the decision is taken to use only 256 bits to implement an SRAM PUF. Do you expect this SRAM PUF to generate a sufficiently random 256-bit key from only 256 SRAM cells? Clearly explain why or why not you could expect to receive a random 256-bit key sufficient for use in cryptographic applications.

Please limit your answer to 10 sentences or less. If you write more than 10 sentences, please circle or otherwise clearly indicate which 10 sentences you want graded.

(b) (5 pts.) For this question – part (b) of the second question on this final exam – assume that you have an SRAM PUF which generates a truly random 256-bit value. For this SRAM PUF which generates a value that passes all relevant tests and therefore appears to be truly random, is the usage of said SRAM PUF better suited for entity authentication or encryption? For full credit for this answer, please provide a minimum of one clear reason why you believe the SRAM PUF is better suited for authentication or encryption. In your explanation, provide a clear example of how the 256-bit value could be utilized.

Please limit your answer to 10 sentences or less. If you write more than 10 sentences, please circle or otherwise clearly indicate which 10 sentences you want graded.

3. **(10 pts.) Shift Cipher.**

Consider the following message encoded with a shift cipher:

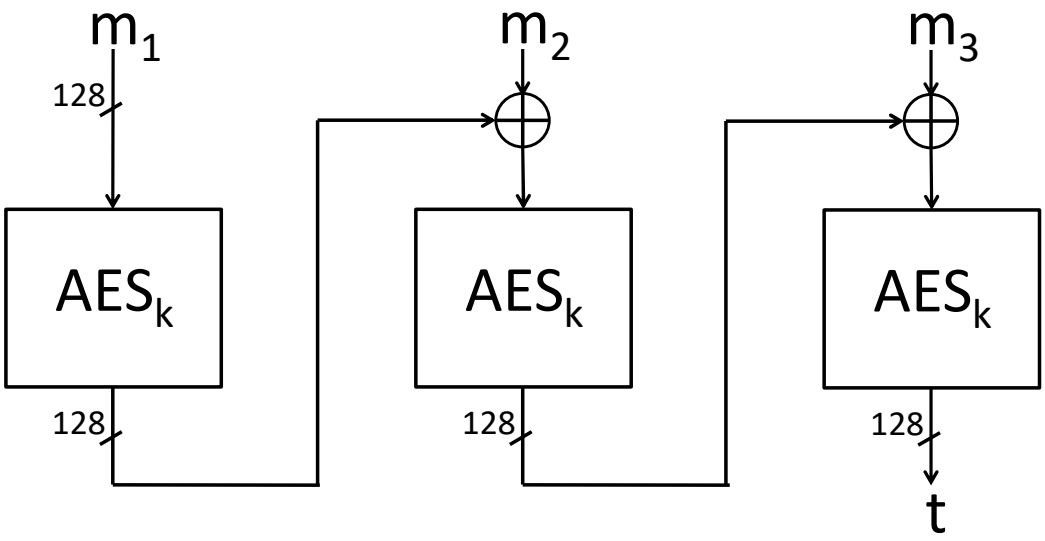
```
EHJLQWKHDWWDFNQRZ
```

Write the message in plaintext. HINT1: you may want to utilize the matrix below. HINT2: you should be able to solve this cipher in 26 tries or less.

A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B
B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C
C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D
D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E
E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F
F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G
G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H
H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I
I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J
J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K
K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L
L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M
M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N
N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O
O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P
P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q
Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R
R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S
S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T
T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U
U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V
V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W
W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X
X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y
Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

4. **[ECE 4156] (15 pts.) [ECE 6156] (30 pts.) Message Integrity using Cipher Block Chaining.**

Consider using AES with key k to generate a tag on any message of any length a multiple of 384 bits (i.e., lengths 384 bits, 768 bits, 1152 bits, 1536 bits, etc.). Consider the following example for a message $m = \{m_1, m_2, m_3\}$ where $m_i \in \{0,1\}^{128}$:



Suppose the adversary has access to a MAC oracle which only outputs tags for messages of length 384 bits; i.e., messages of any other length are not provided with a tag.

(a) (15 pts.) Show how to forge a valid tag for a new message of length 768 bits. As defined in the adaptive chosen message attack, the adversary may choose any message desired; only one message of length 768 bits with a valid tag suffices to answer this question, but keep in mind that the MAC oracle only answers requests for tags for messages of length 384 bits.

(b) **[ECE 6156 only]** (15 pts.) This question – part (b) of the fourth problem on the final exam – is nearly identical to the previous question – part (a) of the fourth problem on the final exam – except that only one oracle query is allowed. Here is the question:

Show how to forge a valid tag for a new message of length 768 bits with only one oracle query. As defined in the adaptive chosen message attack, the adversary may choose any message desired as the forged message which is verified; only one message of length 768 bits with a valid tag suffices to answer this question, but keep in mind that **only one MAC oracle query is allowed** and the MAC oracle only answers a request for a tag for a message of length 384 bits and not any other length.

HINT: If you only used only one MAC oracle query to answer the previous question – part (a) of the fourth problem on the final exam – you may simply repeat the same answer here. In other words, it is perfectly fine – but is not required! – to give the identical answer to parts (a) and (b) of this problem, i.e., the fourth problem on the final exam.

5. **(10 pts.) The Needham-Schroeder Protocol.**

Consider the Needham-Schroeder protocol as presented in the course textbook where A is an identifier for Alice, B is an identifier for Bob, $E_A()$ is encryption with a symmetric key held by Alice, $E_B()$ is encryption with a symmetric key held by Bob, K is a symmetric key, and both R_A and R_B are nonces:

1) Alice to Trent: A, B, R_A
2) Trent to Alice: $E_A(R_A, B, K, E_B(K, A))$
3) Alice to Bob: $E_B(K, A)$
4) Bob to Alice: $E_K(R_B)$
5) Alice to Bob: $E_K(R_B - 1)$

Now suppose that Trent is hacked by Mallory, a malicious third party. In this case is it possible for Mallory to carry out a Man-in-the-Middle (MitM) attack on the Needham-Schroeder protocol as shown above, or are Alice and Bob able to avoid a MitM attack from Mallory under these conditions?

If a MitM attack is not possible, give at least one clear reason why any MitM attack will fail and also show some of the steps to demonstrate how Mallory might try to carry out a MitM attack against Bob and Alice but nonetheless fail.

If a MitM attack is possible, give at least one clear reason why a MitM attack might succeed and show some of the steps to demonstrate how Mallory might be able to successfully carry out a MitM attack against Bob and Alice.

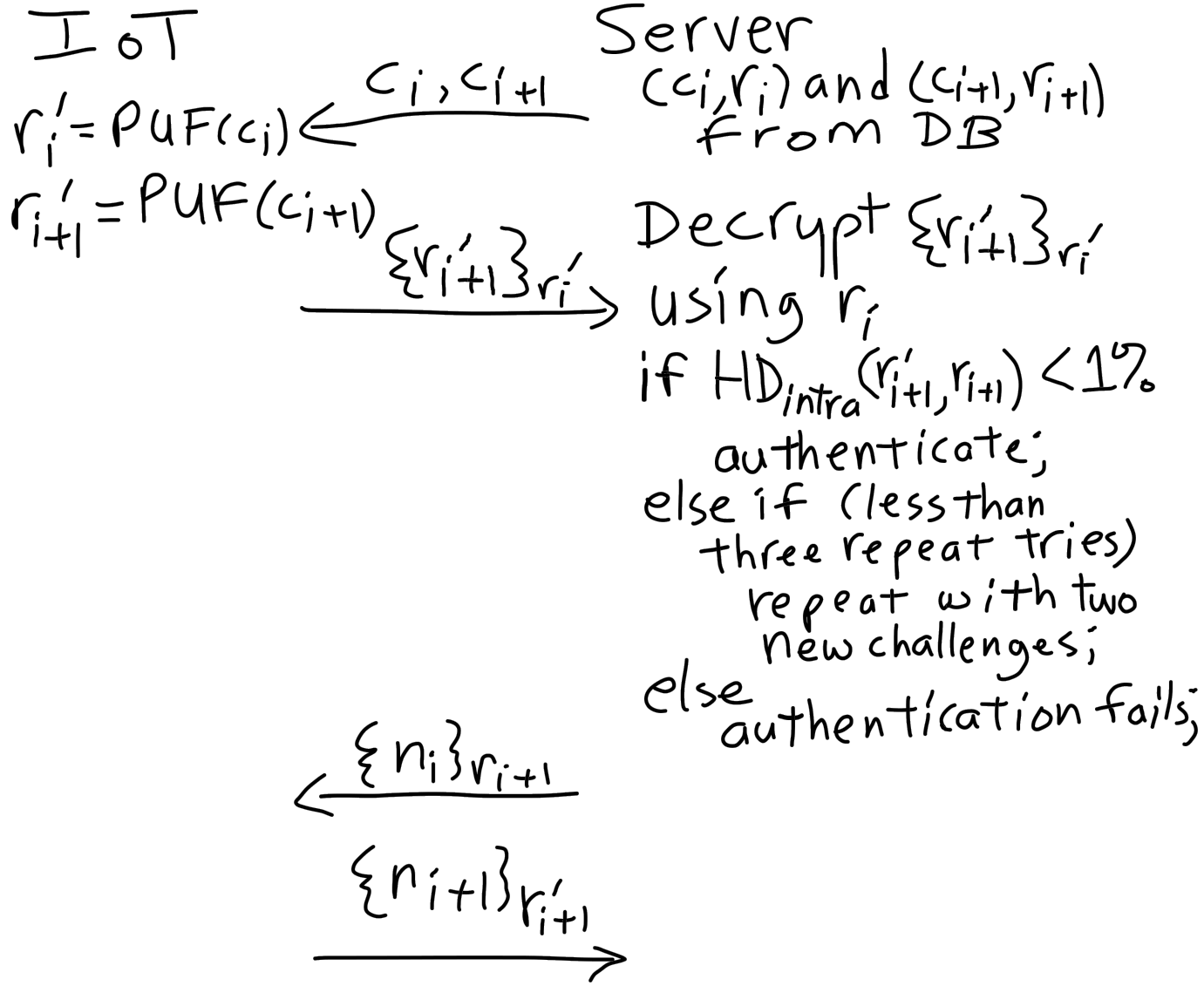
Please note that you will be graded both based on the reason given as well as the specific steps; if you give a valid and clear reason but you have a few mistakes in your specific steps shown, you can still earn full credit, but if your reason given is faulty you will not earn full credit even if your steps as given are correct. Some assumptions are likely to be needed for your answer; if so, please clearly state any assumption(s) you may require. Please note that different assumptions may lead to different answers; all reasonable assumptions will be granted for full credit.

6. **(30 pts.) Controlled PUF.**

Consider an Internet-of-Things (IoT) device which is resource constrained with barely enough memory for computation and message protocol processing (i.e., IoT has essentially zero free memory for storage). Furthermore, IoT has only one cryptographic algorithm available, AES, and also has a weak PUF; otherwise, IoT has no further abilities with regard to authentication and encryption. In particular, IoT does not have any random number generation capability at all.

You are part of a team that proposes the following protocol for two-way authentication between IoT and Server (i.e., the home base which controls a fleet of resource constrained devices). The notation in the protocol below has c_i representing a challenge, r_i representing a response from enrollment, r'_i representing a response from an IoT in operating its PUF live in the field, $\{message\}_{key}$ denoting AES encryption of *message* using *key* for the AES encryption key, and n_i representing a nonce from a true random number generator on the Server.

Please assume enrollment is properly carried out with enough database (DB) entries for the protocol to succeed; enrollment is not shown and is not a part of this problem.



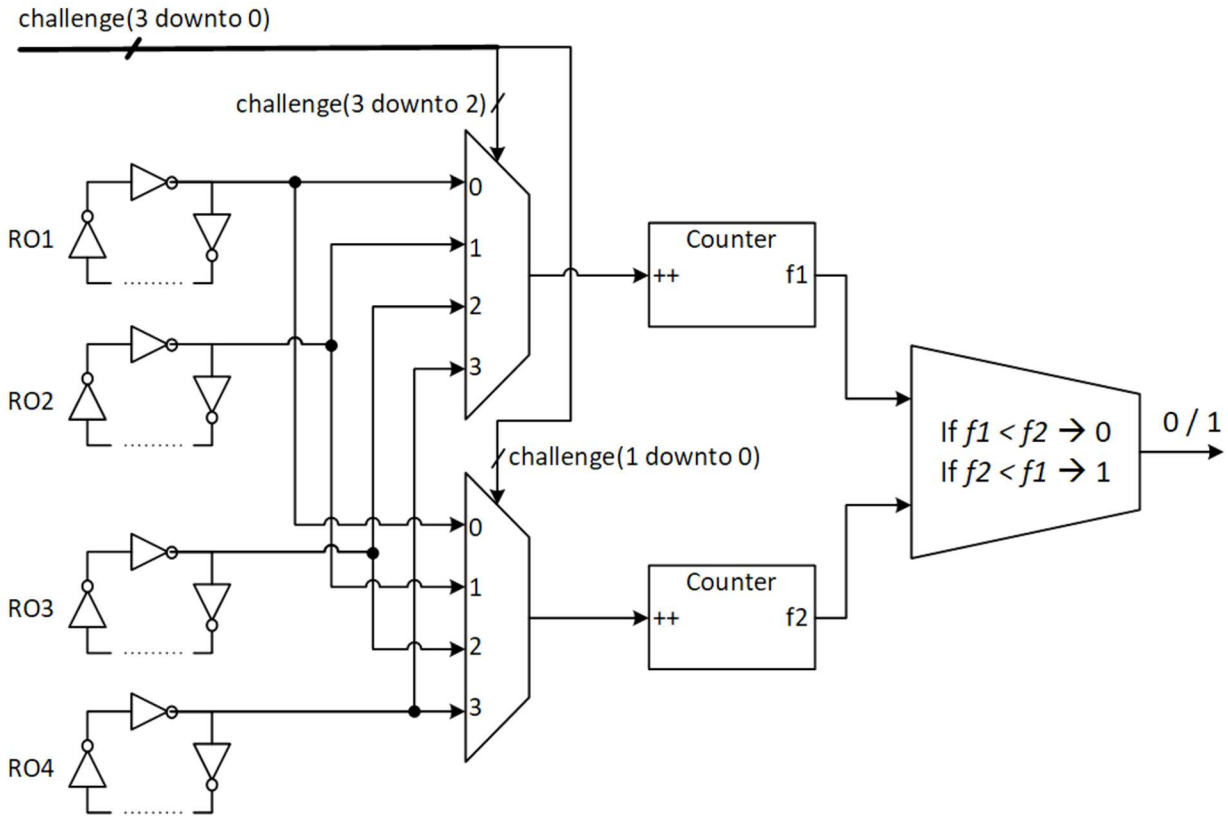
(a) (5 pts.) Consider what happens if $HD_{intra}(r'_{i+1}, r_{i+1})$ is greater than 1% three times in a row. What happens in the proposed protocol (see previous page)?

(b) (5 pts.) Consider the last two steps in the proposed protocol. Is it OK to increment the nonce n_i by one? What do these two steps achieve?

(c) (20 pts.) Does the proposed protocol achieve two-way authentication? Why or why not?

7. (15 pts.) Ring Oscillator PUF.

Consider the following Ring Oscillator PUF (RO-PUF) with n = 4. The ROs are numbered RO-1 through RO-4 and have the following respective frequencies at nominal temperature and voltage: 1.00 MHz, 0.90 MHz, 0.95 MHz and 1.1 MHz. (i.e., RO-1 has frequency 1.00 MHz, etc.). The nominal temperature is 25 °C, and the nominal voltage is 1.0 V. When issuing a challenge, we enable the oscillators for a time period of Δt = 1ms.



(a) (5 pts.) Consider the case where we pair any one of the four ROs with any other RO; under this pairing strategy, what is the maximum number of unique response bits (where each response bit is deemed unique if it corresponds to a unique pair of ROs)? (HINT: please note that for this question, we are assuming that any RO can be paired with any other.)

(b) (5 pts.) For each RO, find the value the counter corresponding to the RO would have when the number of rising edges output by the RO is counted for $\Delta t = 1ms$ at nominal temperature and voltage. (HINT1: neglect any possible impact due to temperature and voltage variations.) (HINT2: use the frequencies for the ring oscillators as given at the beginning of the problem.)

(c) (5 pts.) Assume we feed the RO-PUF with the following challenge bits:

$$challenge(3\ downto\ 0)\ =\ \text{“}0001\text{”}$$

What would the generated response bit be? For full credit in case of a correct answer, and for partial credit in case of an incorrect answer, please explain your work/reasons.

8. **(15 pts.) RSA Encryption.**

Consider the following RSA key generation. First, choose two prime numbers p and q as 3 and 7. Compute $n = p * q = 21$. Next choose an encryption key e such that e and $(p-1)(q-1)$ have no factor in common. Choose $e = 5$ which has no factor in common with $(p-1)(q-1) = (3-1)(7-1) = 12$. Next $d = 5$ is chosen since this value for d satisfies the requirement that d is the multiplicative inverse of e.

(a) (5 pts.) Explain both with words and mathematical equations what it means for d to be the multiplicative inverse of e for this RSA key pair example.

(b) (5 pts.) Encrypt 6 using the public key for this RSA example. For full credit, show and explain all steps.

(c) (5 pts.) Is there a problem with using the same value for both *e* and *d* ? In other words, if the RSA keys for encryption and decryption are identical, is this a problem? Please give one reason why this **is** or **is not** a problem. If you write **more** than 10 sentences, please circle the ten sentences (or less) you want graded, otherwise you will receive zero points. Also, if you give **more than one** reason, please pick the one reason you want graded and circle it (otherwise you will receive zero points as well!).

9. **(10 pts.) Three Ways to Combine Encryption with Message Integrity.**

The three ways typically considered to combine encryption with message integrity are (i) encrypt-and-authenticate, (ii) authenticate-then-encrypt and (iii) encrypt-then-authenticate. For this question, please assume that all three options are implemented with approximately the same hardware usage and execution time; in other words, from an area, delay or energy consumption (power) perspective, all three approaches are equal. Now here is the question to be answered:

From a security perspective, are there any conditions under which option (i) encrypt-and-authenticate is preferred? Why or why not? Please give at least one solid reason for your answer. Please note that you will be graded primarily on whether or not you provide a good reason for your answer; there may be many such reasons. If you give more than one reason or write down more than 10 sentences, please indicate the 10 sentences or less as well as the single reason you wish to submit for your answer.

10. **[ECE 6156 only] (10 pts.)**

Let F be a pseudorandom function and G be a pseudorandom generator with expansion factor $\ell(n) = n + 1$. Consider the encryption scheme where to encrypt $m \in \{0,1\}^n$, output the ciphertext $m \oplus F_k(1^n)$. The key is a uniform $k \in \{0,1\}^n$.

(a) (5 pts.) Does the encryption scheme have indistinguishable encryptions in the presence of an eavesdropper? Why or why not?

(b) (5 pts.) Is the encryption scheme CPA-secure? Why or why not?

THIS IS THE LAST PAGE OF THE EXAM!