Hardware-Oriented Security and Trust
ECE 4156 HST / ECE 6156 HST
Spring 2024

Assoc. Prof. Vincent John Mooney III
Georgia Institute of Technology

Homework 2, 30 pts. (ECE 4156) 40 pts. (ECE 6156)
Due Friday January 19 prior to 11:55pm

1) (10 pts.) In the Media Gallery on Canvas, listen to the second half (approximately from the 29 minute point in the lecture to the end at 58 minutes) of lecture "03IntroSHA2." There is no need to notify Professor Mooney that you have done so **unless** you have problems. Canvas provides information regarding which GT usernames have accessed / listened to lectures, so there is no need to turn anything in if you have been successful.

2) (10 pts.) Consider the following encryption scheme. The message space is $M = \{0, \ldots, 4\}$. Algorithm Gen chooses a uniform key from the key space $\{0, \ldots, 5\}$. $\text{Enc}_k(m)$ returns result $[k + m \ mod \ 5]$, and $\text{Dec}_k(c)$ returns $[c - k \ mod \ 5]$. Does this scheme fit the definition of "perfect" secrecy, i.e., either Definition 2.3 or Definition 2.5?

(NOTE: this is part a of problem 2.6 on page 38 of Katz and Lindell.)

3) (10 pts.) When using a one-time pad with $k = 0^\ell$, we have $\text{Enc}_k(m) = k \oplus m = m$ and the message is sent in the clear! It has therefore been suggested to modify the one-time pad by only encrypting with $k \neq 0^\ell$ (i.e., have Gen choose k uniformly from the set of *nonzero* keys of length ℓ). Is this modified scheme perfectly secret, i.e., does this scheme fit the definition of either Definition 2.3 or Definition 2.5? Explain.

(NOTE: this is problem 2.7 on page 38 of Katz and Lindell.)

4) [ECE 6156 only!] (10 pts.) Consider the following encryption scheme. The message space is $M = \{m \in \{0,1\}^\ell \mid \text{the last bit of } m \text{ is } 0\}$. (Note that | means "such that." In other words, every message m has ℓ bits with the last bit always equal to zero.) Algorithm Gen chooses a uniform key from the key space $\{0,1\}^{\ell-1}$. $\text{Enc}_k(m)$ returns a ciphertext result of $m \oplus (k \parallel 0)$, and $\text{Dec}_k(c)$ returns $c \oplus (k \parallel 0)$. Does this scheme fit the definition of "perfect" secrecy, i.e., either Definition 2.3 or Definition 2.5?

(NOTE1: $k \parallel 0$ denotes concatenation of k followed by 0. For example, if $k = 0110$ then $k \parallel 0 = 01100$.)

(NOTE2: this is part b of problem 2.6 on page 38 of Katz and Lindell.)

YOU MAY NOT CONSULT HOMEWORK SOLUTIONS OF THESE EXACT PROBLEMS FROM OTHER COURSES, INCLUDING OTHER/PREVIOUS SECTIONS OF ECE COURSES TAUGHT BY PROFESSOR MOONEY SUCH AS THOSE WITH NAMES INCLUDING HARDWARE ORIENTED SECURITY AND TRUST AS WELL AS CRYPTOGRAPHIC HARDWARE FOR EMBEDDED SYSTEMS. ALL HOMEWORK SUBMISSIONS MUST INCLUDE YOUR NAME, COURSE NUMBER, SECTION, AND THE HOMEWORK SET NUMBER. ALL SUBMISSIONS MUST BE DONE ONLINE. ALL WRITING MUST BE EASY TO READ (FOR EXAMPLE, YOU MAY HAVE TO WRITE WITH THICK INK AND MAY NOT BE ABLE TO USE LOW RESOLUTION PHOTOS OF HANDWRITTEN DIAGRAMS). FAILURE TO PROVIDE CLEAR AND LEGIBLE ANSWERS MAY RESULT IN ZERO POINTS. ALL WORK MUST BE YOUR OWN. NO PLAGIARISM IS ALLOWED, AND YOU MUST PROPERLY REFERENCE ALL SOURCES OF YOUR INFORMATION – ALTHOUGH YOU SHOULD NOT LOOK FOR AND MAY NOT CONSULT "SOLUTIONS" AVAILABLE FROM OTHER SOURCES (TO REPEAT, YOU MAY NOT CONSULT HOMEWORK SOLUTIONS OF THESE EXACT PROBLEMS FROM OTHER COURSES!).