Hardware-Oriented Security and Trust
ECE 4156 HST / ECE 6156 HST
Spring 2023

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

Homework 3, 55 pts. (ECE 4156) 75 pts. (ECE 6156)
Due Friday February 2 prior to 11:55pm

1) (5 pts.) In the Media Gallery on Canvas, listen to the lecture "05MerkleDamgard." 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) (15 pts.) Consider the following keyed function F: for security parameter n, the key is an $n \times n$ Boolean matrix A and an n-bit Boolean vector b. Define $F_{A,b} : \{0,1\}^n \rightarrow \{0,1\}^n$ by $F_{A,b}(x) \stackrel{\text{def}}{=} Ax + b$, where all operations are done modulo 2. Show that F is not a pseudorandom function. (NOTE: this is problem 3.13 on page 103 of Katz and Lindell.)

3) (25 pts.) Let F be a pseudorandom permutation, and define a fixed-length encryption scheme (Enc, Dec) as follows: On input $m = \{0,1\}^{n/2}$ and key $k \in \{0,1\}^n$, algorithm Enc chooses a uniform string $r \in \{0,1\}^{n/2}$ of length $n/2$ and computes $c := F_k(r||m)$.

Show how to decrypt and provide an intuitive reason why this scheme is CPA-secure for messages of length $n/2$. (NOTE1: $r||m$ denotes unambiguous concatenation of r and m. For example, if $r = 0110$ and $m = 1100$ then one possibility is $r||m = 01101100$.) (NOTE2: this problem is very similar to problem 3.18 on page 104 of Katz and Lindell.) (NOTE3: the "intuitive reason" requested will not be graded in a harsh manner – in other words, if you provide a solid reason you will receive full credit even if there are a variety of solid, intuitive reasons possible. Of course, if you provide a "reason" which is vague or incorrect, you will lose points.)

4) (15 pts.) Let G be a pseudorandom generator with expansion factor $\ell(n) = n + 1$. For the following encryption scheme, state whether the scheme has indistinguishable encryptions in the presence of an eavesdropper and whether it is CPA-secure. (Note that the shared key is a uniform $k \in \{0,1\}^n$.) Explain your answer.

Encryption scheme: To encrypt $m \in \{0,1\}^{n+1}$, choose uniform $r \in \{0,1\}^n$ and output the ciphertext $\langle r, G(r) \oplus m \rangle$.

(NOTE: this is part a of problem 3.19 on page 104 of Katz and Lindell.)

5) [ECE 6156 only!] (20 pts.) Let F be a pseudorandom function and G be a pseudorandom generator with expansion factor $\ell(n) = n + 1$. For each of the following encryption schemes, state whether the scheme has indistinguishable encryptions in the presence of an eavesdropper and whether it is CPA-secure. (In each case, the shared key is a uniform $k \in \{0,1\}^n$.) Explain your answer.

a. To encrypt $m \in \{0,1\}^n$, output the ciphertext $m \oplus F_k(0^n)$.
b. To encrypt $m \in \{0,1\}^{2n}$, parse m as $m_1||m_2$ with $|m_1| = |m_2|$, then choose uniform $r \in \{0,1\}^n$ and output the ciphertext $\langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r+1)\rangle$.

(NOTE: this is part b and part c of problem 3.19 on page 104 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!).