Hardware-Oriented Security and Trust
ECE 4156 HST / ECE 6156 HST
Spring 2025
Assoc. Prof. Vincent John Mooney III
Georgia Institute of Technology
Homework 5, 85 pts. (ECE 4156) 100 pts. (ECE 6156)
Due Friday February 21 prior to 11:55pm

1) (30 pts.) Let F be a pseudorandom function. Show that each of the following MACs is insecure, even if used to authenticate fixed-length messages. (In each case Gen outputs a uniform $k \in \{0,1\}^n$. Let $\langle i \rangle$ denote an $\frac{n}{2}$-bit encoding of the integer i.)

a. (5 pts.) To authenticate a message $m = m_1, \ldots, m_\ell$, where $m_i \in \{0,1\}^n$, compute $t := F_k(m_1) \oplus \ldots \oplus F_k(m_\ell)$.

b. (10 pts.) To authenticate a message $m = m_1, \ldots, m_\ell$, where $m_i \in \{0,1\}^{\frac{n}{2}}$, compute $t := F_k(\langle 1 \rangle \| m_1) \oplus \ldots \oplus F_k(\langle \ell \rangle \| m_\ell)$.

c. (15 pts.) To authenticate a message $m = m_1, \ldots, m_\ell$, where $m_i \in \{0,1\}^{\frac{n}{2}}$, choose uniform $r \in \{0,1\}^n$ and compute
$$t := F_k(r) \oplus F_k(\langle 1 \rangle \| m_1) \oplus \ldots \oplus F_k(\langle \ell \rangle \| m_\ell)$$
where the tag which is transmitted is $< r, t >$.

(NOTE: this is problem 4.7 on page 148 of the 2nd Edition of Katz and Lindell.)

2) (20 pts.) We explore what happens when the basic CBC-MAC construction is used with messages of different lengths.

a. (10 pts.) Say the sender and receiver do not agree on the message length in advance (and so $\text{Vrfy}_k(m,t) = 1$ iff $t \stackrel{?}{=} \text{Mac}_k(m)$, regardless of the length of m), but the sender is careful to only authenticate messages of length $2n$. Show that an adversary can forge a valid tag on a message of length $4n$.

b. (10 pts.) Say the receiver only accepts 3-block messages (so $\text{Vrfy}_k(m,t) = 1$ only if m has length $3n$ and $t \stackrel{?}{=} \text{Mac}_k(m)$), but the sender authenticates messages of any length a multiple of n. Show that an adversary can forge a valid tag on a new message.

(NOTE: this is problem 4.13 on page 149 of the 2nd Edition of Katz and Lindell.)

The rest of this homework is based on the "Cryptography Part VII: Diffie Hellman" lecture the concept was introduced of key exchange where two people Alice and Bob choose secrets `x` and `y` such that when they exchange $\alpha^x \bmod p$ and $\alpha^y \bmod p$ they each can compute a shared secret key $K = (\alpha^x)^y \bmod p = (\alpha^y)^x \bmod p$. This shared secret key cannot be recovered by an adversary with any reasonable probability of success where the adversary records all channel exchanges and thus acquires both $\alpha^x \bmod p$ and $\alpha^y \bmod p$ (as well as α and p which are public). In the following questions you will both provide a discussion of possible scenarios and calculate actual values for Diffie-Hellman key exchange.

3) (20 pts.) The first step in Diffie-Hellman key exchange is the publication of an appropriate prime number p and generator α of Z_p^*. Is this first step a possible weakness in the protocol? In other words, are there scenarios where an adversary may or may not be able to manipulate this first step and gain a significant advantage?

a. (5 pts.) Describe your scenario. In other words, give a specific case, e.g., two embedded devices communicating over a radio link or two personal computers communicating over the internet, in sufficient detail to explain your answers to the rest of this question, question 3 on homework 5. Use Alice and Bob for the two legitimate communicating parties, and use Elektra to refer to the adversary. Please make sure that all relevant details are explained here, e.g., you may want to include (or not include) some form of a "Trusted Third Party" or TTP whose operation you should specify in sufficient detail. HINT: one suggestion is to first answer parts b, c and d below, then return to this part, part a, and write up the scenario.

b. (5 pts.) Describe the attack surface. For the scenario of part a, discuss how the adversary, Elektra, may choose to manipulate the setting of the first step of Diffie-Hellman Key Exchange. You should also discuss how Alice and Bob may choose to set up the scenario such that it is extremely difficult for an adversary to carry out any manipulations successfully. Your answer here should be comprehensive, i.e., the tradeoffs you will show in your answers to parts c and d below should be described here in terms of the strengths and weaknesses of various setups for your chosen scenario. HINT: one suggestion is to first answer parts c and d below, then return to this part, part b, and write up a description of the attack surface.

c. (5 pts.) For this part – part c of question 3 – your overall answer is supposed to be that yes the adversary (Elektra) may be able to set up the scenario with an inherent weakness. Please describe precisely the scenario and attack surface in detail and describe how the attack could be carried out successfully. Please note that all steps in the attack should be reasonable for today's technology, e.g., you are not allowed to assume the availability of a 10,000-bit quantum computer, but you may have some of the hardware (e.g., Alice's phone or Bob's phone) acquired by Elektra somehow.

d. (5 pts.) Now give a set of assumptions, e.g., involving a TTP, such that no attack you can think of could succeed. You should describe at least three attacks that fail including the attack in your answer to part c.

4) (15 pts.) Now we are going to carry out Diffie-Hellman Key Exchange. Consider the case of using $\alpha = 6$ as a generator for Z_{13}^*.

a. (1 pt.) Choose appropriate Alice and Bob secrets `x` and `y`, email the TA, Arman Allahverdi, at aallahverdi3@gatech.edu and then check the course webpage for homeworks
http://mooney.gatech.edu/Courses/ECE4156/hwlabexam/index.html
to see if your number has already been taken or not. You need to make a first attempt to choose a number prior to 2pm on Tuesday Feb. 18. If your first name, first letter of your last name, and selected pair of numbers appears under homework 5, you are done. Otherwise, prior to 2pm on Wednesday Feb. 19, you need to make a second attempt to choose your secrets `x` and `y` and send another email to another email to the TA. Again, if your first name and number appears under homework 5, you are done. Otherwise, prior to 2pm on Thursday Feb. 20, you need to try again.

b. (8 pts.) For your given secrets `x` and `y`, compute the following quantities:
   i. (2 pts.) α^x
   ii. (2 pts.) α^y
   iii. (2 pts.) $(\alpha^x) \bmod p$
   iv. (2 pts.) $(\alpha^y) \bmod p$

c. (6 pts.) Finally, compute the shared secret key $K = (\alpha^x)^y \bmod p = (\alpha^y)^x \bmod p$ and show the intermediate step of $(\alpha^x)^y = (\alpha^y)^x$.

5) [ECE 6156 only!] (15 pts.) Write pseudocode to carry out a brute-force attack against Diffie-Hellman key exchange. Assume that the adversary has acquired α, p, $((\alpha^x) \bmod p)$ and $((\alpha^y) \bmod p)$. Show the steps to carry out the brute-force attack to your answer to the previous question (question 4) on this homework.

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!).