Hardware-Oriented Security and Trust
ECE 4156 A / ECE 6156 A
Spring 2025
Assoc. Prof. Vincent John Mooney III
Georgia Institute of Technology
Homework 7, 110 pts. (ECE 4156) 115 pts. (ECE 6156)
Due Friday March 28 prior to 11:55pm

1) (20 pts.) Read Section 5.2 and Appendix A of the Federal Information Processing Standard (FIPS) Publication 197, "ADVANCED ENCRYPTION STANDARD (AES)," in preparation for this question. For a 128-bit AES key please describe the Key Expansion step in response to the following two questions.

   a. (10 pts.) Describe how key expansion works using pseudocode. You may modify Figure 11 of the AES standard, but make sure **not** to include elements (i.e., variables and/or code) needed for 192-bit or 256-bit keys; instead, **only** provide pseudocode for the 128-bit key case. Please describe how the pseudocode works with a paragraph or two (or three but length is **not** required). Make sure to clearly define all aspects of your pseudocode so that a reader with a bachelor's degree in ECE or CS could follow your description without being required to read the AES standard.

   b. (10 pts.) Now describe intuitively how entropy / randomness is maintained. In other words, assuming that the initial 128-bit number is a (truly) random number, comment on how an adversary might try to predict the individual key expansion step results given that the adversary does not know the initial 128-bit key. (Note that you are being asked to think about cryptanalysis in this question; due to lack of time, unfortunately this course does **not** cover cryptanalysis in general, although obviously this question is asking you to think about a very specific subcase of cryptanalysis, i.e., w.r.t. key expansion in AES.) Explain at least one clear reason why, intuitively, entropy / randomness is not decreased.

2) (20 pts.) During your next job interview you mention that you learned the internals of AES, and so you are asked a series of questions as follows:

   a. (5 pts.) What are the different key sizes supported and what is the advantage of maintaining the same plaintext to ciphertext size of 128 bits while supporting increasing key sizes?

   b. (5 pts.) In the final round MixColumns is not performed – why not?

   c. (5 pts.) What cryptographic property do ShiftRows and MixColumns provide to AES, and why is this property important?

   d. (5 pts.) Are any of the AES operations (e.g., SubBytes or ShiftRows) non-invertible – i.e., without an inverse? If so, which operations do not have an inverse and why? If on the other hand all operations are invertible, why do you think that this is so?

3) (45 pts.) Consider the following scenario. A server SAM is communicating with an IoT device TOM. TOM has a PUF. SAM is provided with 2^{30} challenge-response pairs from the enrollment process for TOM's PUF. Each challenge is 128 bits and each response is 128 bits.

You are supervising a team where one of your superstar engineers, Alex, comes up with an idea. Alex proposes that PUF-based encryption can serve both as an encryption method as well as an authentication method at the same time. Specifically, SAM sends a challenge to TOM. TOM uses the 128-bit PUF response *kt* to encrypt a message m_{status}. Specifically, TOM sends SAM the following: $\{m_{status}\}_{kt}$. Based on the decrypted value of m_{status}, SAM sends TOM instructions $m_{instructions}$ as follows: $\{m_{instructions}\}_{kt}$.

a. (15 pts.) Describe the protocol using a diagram similar to what was shown in Authentication Part II. Explain each step in the protocol.

b. (15 pts.) Is the protocol vulnerable to a Man-in-the-Middle (MITM) attack? Please redraw the diagram from your answer to part a. Show the best effort you can to attack using MITM. Explain whether the attack works or not with details.

c. (15 pts.) Is the protocol vulnerable to a replay attack? Please redraw the diagram from your answer to part a. Show the best effort you can to attack using replay. Explain whether the attack works or not with details. Assume that TOM does not store all past challenges received.

4) (25 pts.) During class Professor Mooney explained why it is possible to model-build the Arbiter PUF. Use your own words to explain how an adversary can "learn" the challenge-response space of a 100-bit Arbiter PUF. As in problem 2 above, you are on a job interview where there is great interest in probing your understanding of PUFs in general with the Arbiter PUF as a specific example. You are asked to provide a detailed explanation of why far less than 2^{100} challenges suffices to learn the challenge-response space. Your answer should include (i) what is the underlying source of entropy or randomness, (ii) how long a typical adversary may be in possession of the microchips each of which has an Arbiter PUF to be learned, (iii) what is the overall technique applied by the adversary, and finally (iv) a few specific examples of challenge pairs that the adversary may apply to learn some specific parameter or parameters of the Arbiter PUF challenge-response model being built.
(Note: Try to write down your best answer in two pages or less please!)

5) [ECE 6156 only!] (5 pts.) In Lecture 17, some of the NIST tests for randomness were described. What does the following statement mean (quoting from the abstract of the NIST document): "However, no set of statistical tests can absolutely certify a generator as appropriate for usage in a particular application, i.e., statistical testing cannot serve as a substitute for cryptanalysis." Please explain in your own words what this means; do not quote from any other source but instead do your best to express the concerns being raised here. You may not give an answer longer than 10 sentences; if you do, please circle the 10 sentences you want graded or else you will receive a zero.

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!).