CS 463/563 — Cryptography for Cybersecurity
Homework 4: Fields and AES

DUE DATE HERE

STUDENT NAME HERE
UIN HERE
SECTION HERE
Instructor: J. Takeshita. Institution: Old Dominion University.

Submission instructions: If you don't already have the necessary tools, then install 1) a LaTeX distribution (probably the `texlive-full` package on most Linux distributions) and 2) an IDE or other text editor suitable for LaTeX. For the latter, I suggest the use of the Kile IDE, which is available in most Linux distributions' default packages. You can also just use a web IDE such as **Overleaf**.

Download the source file(s) for this assignment. Edit the file(s) to include your solutions using the text editor or LaTeX IDE of your choice. Type your answers and personal information (e.g., name, section, etc.) into the source file at the appropriate places, and double-check that the variable `solutions` is set to be false. (I should have done this for you, but it's good to be sure.) Make sure to properly format your math! See `https://latex-tutorial.com/tutorials/` if you're not already familiar with LaTeX.

Compile the source to a PDF, either through your IDE or by using the command `pdflatex`. Make sure your compilation has no errors, and address all reasonably actionable warnings (you can ignore small things like badbox warnings, as long as they don't affect the output badly). You can toggle the variable `boilerplate` to hide these instructions, if you like.

Turn in 1) the PDF and 2) any and all `.tex` source files, `.bib` bibliography files, source code, or other artifacts. Submissions that are handwritten or typeset with other methods will not be accepted! If you wrote any software in the course of this work, please include it using the `listing` package's utilities.

Cite any external sources, and include any code you write. The use of unauthorized outside assistance, including any AI/LLM, is strictly prohibited.

A note: While it is possible and allowed to solve these questions by writing your own computer programs, you should be able to also do them by hand, as similar questions may appear on exams.

Questions:

1. Consider the prime field $GF(19)$. (10 points)
   (a) What are the elements of this prime field?
   (b) What is the additive inverse of 9 in this field?

(c) What is the multiplicative inverse of 9 in this field?

Answer:

(a) 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18

(b) 10
$10 + 9 \pmod{19} = 0$

(c) 17
$9 * 17 \pmod{19} = 1$

2. Consider the extension field $GF(2^6)$. (10 points)

(a) What is $A(x) = 17$ in this field? (Hint: it will be a polynomial. Another hint: what is 17 as a six-bit binary number?)

(b) What is $B(x) = 8$ in this field?

(c) What is $C(x) = 1$ in this field?

(d) Determine $A(x) + B(x)$ as a polynomial and express it an integer.

(e) Determine $B(x) + C(x)$ as a polynomial and express it an integer.

Answer:

(a) 010001
$x^4 + 1$

(b) 001000
x^3

(c) 000001
1

(d) $x^4 + x^3 + 1 = 25$

(e) $x^3 + 1 = 9$

3. Using Table 4.2, in $GF(2^8)$, determine the multiplicative inverses of `0x4D` and `0x4E`. (Hint: this can be done with a quick table lookup.) (4 points)

Answer: $4D = 25$
$4E = E9$

4. Using Table 4.3, in $GF(2^8)$, determine the AES S-box substitutions for `0x5E` and `0x5F`. (Hint: this can be done with a quick table lookup.) (4 points)

Answer: $5E = 58$
$5F = CF$

5. Suppose you are given the 128-bit input `0xE5C2D6A8B0C8F99C7B1F8E0682337485` as input to the AES ShiftRows sublayer (for a single round). What is the output? (12 points)

   Hint 1: the output should be 128 bits, which are expressed using 32 hexadecimal characters.

   Hint 2: Refer to page 104 of the textbook. First, arrange the input data into a matrix of bytes. For example, the 1st two characters `E5` become a single byte. This byte will go to the B_0 cell of Table 1:

Table 1: AES ShiftRows State Matrix

B_0	B_4	B_8	B_{12}
B_1	B_5	B_9	B_{13}
B_2	B_6	B_{10}	B_{14}
B_3	B_7	B_{11}	B_{15}

   Similarly, the next two characters in the input `C2` become a single byte. This value will go to the B_1 cell of the matrix given above. Once the matrix is populated with the input bytes, shift the elements in each row as shown in Matrix 4.1 on page 104. Finally, express the output as a matrix or as a sequential string reading column-wise.

E5	B0	7B	82
C8	1F	33	C2
8E	74	D6	F9
85	A8	9C	06

6. Give a new question on the topic of this week's material and its solution, suitable for inclusion in future versions of this homework assignment. Your question should be different from the other questions here – don't just change some values around! Programming problems are acceptable too, but should be nontrivial. You can use textbooks, scholarly papers, or other reputable sources of information for inspiration, but you should not directly copy someone else's work. Your question should show

me that you understand the content well enough to ask and answer an interesting question about it. Include any source code used to generate/solve the problem. (10 points)

Some free online textbooks include *The Joy of Cryptography* by Mike Rosulek (Oregon State University), or *A Graduate Course in Applied Cryptography* by Dan Boneh (Stanford University) and Victor Shoup (Offchain Labs, formerly at New York University). Your course text, *Understanding Cryptography* by Christof Paar (Universität Bochum) and Jan Pelzl (Universität Bochum), is also an excellent starting point. For HW4, textbooks and online courses on abstract algebra will also be helpful sources.

Possible topics include fields, finite fields, prime fields, extension fields, or AES.

Answer: in GF (2^8) what is $25 * 100$ in polynomial form
$A(x) = 25 = x^4 + x^3 + 1$
$B(x) = 100 = x^6 + x^5 + x^2$
$P(x) = x^8 + x^4 + x^3 + x + 1$

$A(x)B(x) \pmod 2 = x^{10} + x^8 + x^3$
$A(x)B(x) \pmod{P(x)} = x^6 + x^4 + x + 1$