Introduction to Cryptography—Homework 5
Due: Sunday, March 28, 2021, 11:59pm

- You may work on and submit your homework in **groups of 2** or individual.
- Submit your solutions to the appropriate dropbox folder on myCourses as **single (readable) pdf**.
- The homework must be entirely your own work.
- Before you start on the homework, please read the rules on collaboration and submission in the syllabus.
- Keep in mind that, as stated in the syllabus, I will not answer questions the day the homework is due.
- Each homework problem indicates the number of points it is worth for grading purposes. While individual problems may be worth more or fewer points than others, each homework assignment carries weight as stated in the syllabus.

1. **(3 points)** Multiplication in $GF(2^4)$: Compute $A(x) \cdot B(x)$ mod $P(x)$ in $GF(2^4)$ using the irreducible polynomial $P(x) = x^4 + x + 1$. Show the details of your work (not program or code). Your answer must be in the form of a polynomial.

   a) $A(x) = x^2 + 1$, $B(x) = x^3 + x^2 + 1$

   b) $A(x) = x^2 + 1$, $B(x) = x + 1$

   c) What is the influence of the choice of the reduction polynomial on the computation?

2. **(2 points)** Compute in $GF(2^8)$:

   $$(x^4 + x + 1)/(x^7 + x^6 + x^3 + x^2),$$

   where the irreducible polynomial is the one used by AES, $P(x) = x^8 + x^4 + x^3 + x + 1$. Note that Table 4.2 (page 99) contains a list of all multiplicative inverses for this field. Show the details of your work. Your answer must be in the form of a polynomial.

3. **(1 point)** Your task is to compute the S-Box, i.e., the ByteSub, values for the input bytes 29, F3, where each byte is given in hexadecimal notation.

4. **(3 points)** We consider AES with 128-bit block length and 128-bit key length. What is the output of the first round of AES if the plaintext consists of 128 ones, and the first subkey k_1 also consists of 128 ones? Fill the table below (assume that the subkey k_0 addition has already been done).

Input after k_0 addition	FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF
After byte substitution layer	
After diffusion layer	
After key addition layer	

5. **(4 points)**

Let a block cipher with secret key K be chained in the following way:

$$C_i = M_{i-1} \oplus E((M_i \oplus C_{i-1}), K),$$

for $i > 0$, where M_0 and C_0 are fixed public initialization vectors, K is the secret key known to both transmitter and receiver, and E and D represent encryption and decryption, respectively.

a) Draw the block diagram for encryption.

b) Determine the equation for decryption and draw the block diagram.

c) Suppose the ciphertext blok C_3 is damaged in transmission. Which plaintext blocks become indecipherable as a result? Explain.