Homework 4

Due: Tuesday, November 2 at 9PM.

You may discuss the problems in general terms in a group of size at most three. You are expected to write up your solutions yourself. Please credit your collaborators on your submission. You may use your course notes and slides to solve these problems.

The following problems correspond to two separate Gradescope assignments. Problem 1 is called `Homework 4` on Gradescope. This should be a write-up of your solution to Problem 1; this may be either a PDF compiled from LaTeX or a PDF scan of handwritten work. This write-up should also include your answer to the optional Question 3 if you choose to answer it. Please name your submission `hw4.pdf`. The second Gradescope assignment is called `PlayCrypt 4`. This is for submitting your completed Python code for Problem 2. Do not change the file name from `hw4_p2.py`.

Problem 2 on this PDF complements the PlayCrypt homework problem, which can be found on the course website at `https://cseweb.ucsd.edu/classes/fa21/cse107-a/hw4_p2.py`. You do not need to turn in a written answer for this problem and need only turn in your Python solution to `PlayCrypt 2` on Gradescope. This version is being given out so that you can see what the problem looks like in mathematical notation. We suggest that you start with this version. Work out a solution using pencil and paper. Move to implementation in PlayCrypt only after that.

As usual our convention is that the running time of an adversary does not include the time taken by game procedures to compute responses to adversary queries.

Problem 1 [10 points] Let G be the group $\mathbf{Z}_{10}^*$ under the operation of multiplication modulo 10.

1. List the elements of G

2. What is the order of G?

3. Determine the set $\langle 3 \rangle$

4. Determine the set $\langle 9 \rangle$

5. Is G cyclic? Why or why not?

6. Show that 3 and 7 are generators of G

7. What is $\mathrm{DLog}_{G,3}(7)$?

8. What is $\mathrm{DLog}_{G,7}(9)$?

Problem 2 [10 points] Let $E\colon \{0,1\}^k \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ be a block cipher with $k, n \geq 128$. Let $\mathcal{K}$ be the key generation algorithm that returns a random k-bit key. Let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be the symmetric encryption scheme whose encryption and decryption algorithms are as follows, where the message input to $\mathcal{E}_K$ is an n-bit string $M \in \{0,1\}^n$ and the ciphertext input to $\mathcal{D}_K$ is a $4n$-bit string $C = C[1]C[2] \in \{0,1\}^{4n}$:

Alg $\mathcal{E}_K(M)$	**Alg** $\mathcal{D}_K(C)$
if $\lvert M\rvert \neq n$ then return $\perp$	if $\lvert C\rvert \neq 4n$ then return $\perp$
$A[1] \xleftarrow{\$} \{0,1\}^n$; $A[2] \leftarrow M \oplus A[1]$	$C[1]C[2] \leftarrow C$
$C[1] \leftarrow E_K(A[1] \| 0^n)$	$A[1] \| P[1] \leftarrow E_K^{-1}(C[1])$; $A[2] \| P[2] \leftarrow E_K^{-1}(C[2])$
$C[2] \leftarrow E_K(A[2] \| 1^n)$	if ($P[1] \neq 0^n$ or $P[2] \neq 1^n$) then return $\perp$
return C	$M \leftarrow A[1] \oplus A[2]$
	return M

In the second line of $\mathcal{D}_K(C)$ we are parsing $4n$-bit C into $C = C[1]C[2]$ where each block is $2n$-bits. In the third line, the $2n$-bit output of E_K^{-1} is broken into n-bit blocks.

Present in pseudocode a $\mathcal{O}(n)$ time adversary A making at most two queries to its **Enc** oracle and achieving $\mathbf{Adv}^{\text{int-ctxt}}_{\mathcal{SE}}(A) \geq 1 - 2^{-n}$.

Problem 3 [0 points] How much time did you spend on Problem 1? How much time did you spend on Problem 2?
