Homework 4

Due: Thursday, May 5 at 12PM (noon).

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 `HW4 P1` on Gradescope; this should be a PDF writeup of your solution to Problem 1 (no code). Problem 2 is called `HW4 P2` on Gradescope. This is for submitting your completed Python code for Problem 2, using PlayCrypt. This follows the usual autograder setup; **do not change the file name from `hw4_p2.py`**.

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] The following are a few exercises in computational number theory. The necessary definitions and examples are all in the Lecture 9 slides.

1. List the elements of $\mathbb{Z}_{20}^*$, and give the order $|\mathbb{Z}_{20}^*|$.

2. What is the order of $\mathbb{Z}_{2039}^*$? Note that 2039 is prime.

3. What is $3^{\texttt{0xC5E107}} \mod 967$? (`0xC5E107` is in hex.) See Slide 30 for an example.

4. Compute the extended GCD of 428 and 2022, and show the steps. See Slide 36.

5. Compute $43^{2022} \mod 2039$. See Slide 41 for an example.

Problem 2 [10 points] Let E: $\{0,1\}^k \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ 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 $\perp$
$A[1] \xleftarrow{\$} \{0,1\}^n$; $A[2] \leftarrow M \oplus A[1]$	$C[1]C[2] \leftarrow C$
$C[1] \leftarrow E_K(A[1] \Vert 0^n)$	$A[1] \Vert P[1] \leftarrow E_K^{-1}(C[1])$; $A[2] \Vert P[2] \leftarrow E_K^{-1}(C[2])$
$C[2] \leftarrow E_K(A[2] \Vert 1^n)$	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 $\mathbf{Adv}^{\text{int-ctxt}}_{\mathcal{SE}}(A) \geq 1 - 2^{-n}$.
