**CSIC 4331/6331** November 6, 2019

# Homework Assigment 5

**Due Nov. 18**

Please answer each of the below questions. Remember, you may work together, but everyone MUST type up and understand their solutions. Solutions that appear copied will be considered a violation of the academic honesty code. Also, you must list all people you work with on this homework as well as any outside resources (e.g., web search, books, etc.) that you use.

For problems 1-3, do not use a computer or calculator. Show your work. Problems 4-6 cover material that we will cover in class on Monday, November 11.

1. Exercise 8.5 in the book
   Compute the final two (decimal) digits of $3^{1000}$ (by hand).
   **Hint:** The answer is $[3^{1000} \bmod 100]$.

2. Exercise 8.6 in the book
   Compute $[101^{4,800,000,002} \bmod 35]$ (by hand).

3. Exercise 8.7 in the book
   Compute $[46^{51} \bmod 55]$ (by hand) using the Chinese remainder theorem.

4. Exercise 10.4 in the book
   Consider the following key-exchange protocol:

   (a) Alice chooses uniform $k, r \in \{0,1\}^n$, and sends $s = k \oplus r$ to Bob.

   (b) Bob chooses uniform $t \in \{0,1\}^n$, and sends $u = s \oplus t$ to Alice.

   (c) Alice computes $w = u \oplus r$ and sends $w$ to Bob.

   (d) Alice output $k$ and Bob outputs $w \oplus t$.

   Show that Alice and Bob output the same key. Analyze the security of the scheme (i.e., either prove its security or show a concrete attack).

5. Exercise 11.6 in the book
   Consider the following public-key encryption scheme. The public key is $(G, q, g, h)$ and the private key is $x$, generated exactly as in the El Gamal encryption scheme. In order to encrypt a bit $b$, the sender does the following:

   (a) If $b = 0$ then choose a uniform $y \in \mathbb{Z}_q$ and compute $c_1 = g^y$ and $c_2 = h^y$. The ciphertext is $(c_1, c_2)$.

   (b) If $b = 1$ then choose independent uniform $y, z \in \mathbb{Z}_q$, compute $c_1 = g^y$ and $c_2 = g^z$, and set the ciphertext equal to $(c_1, c_2)$.

   Show that it is possible to decrypt efficiently given knowledge of $x$. Prove that this encryption scheme is CPA-secure if the decision Diffie-Hellman problem is hard relative to $G$.

6. Exercise 11.7 in the book
   Consider the following variant of El Gamal encryption. Let $p = 2q + 1$, let $G$ be the group of squares modulo $p$ (so $G$ is a subgroup of $\mathbb{Z}_p^*$ of order $q$), and let $g$ be a generator of $G$. The private key is $(G, q, g, x)$ and the public key is $(G, q, g, h)$, where $h = g^x$ and $x \in \mathbb{Z}_q$ is chosen uniformly. To encrypt a message $m \in \mathbb{Z}_q$, choose a uniform $r \in \mathbb{Z}_q$, compute $c_1 = g^r \bmod p$ and $c_2 = h^r + m \bmod p$, and let the ciphertext be $(c_1, c_2)$. Is this scheme CPA-secure? Prove your answer.
   **Hint:** Recall that it is easy to tell whether or not an element $g \in \mathbb{Z}_p^*$ is a quadratic residue (simply see if $g^q = 1 \bmod p$).