This homework covers Lectures 6 and 7.

1. This question is about arithmetic modulo the safe prime 23, i.e., in the group $\mathbb{Z}_{23}^* = \{\pm 1, \ldots, \pm 11\}$.

   (a) Among 3, 4, and -3, which are quadratic residues?

   (b) Which of the equations $4^x \equiv 3$, $(-3)^x \equiv 4$, $4^x \equiv -3$ have a solution?

   (c) Bob samples $X = 4$ as his secret key for El Gamal encryption. What is his corresponding public key? The generator is $g = 2 = 5^2 \bmod 23$.

   (d) Alice wants to send plaintext 7. How does she encode it as a quadratic residue m? What is the encryption of m under randomness $Y = 3$?

   (e) Work out Bob's decryption of the ciphertext from part (d).

2. Each of the following MACs is functional but insecure. Explain how Bob verifies message-tag pairs and how Eve forges. PRF F has 3 input bits, 128 output bits, and its key is shared by Alice and Bob. Assume Eve can control the messages whose MACs she intercepts. All arithmetic is modulo 2.

   (a) $Tag(m) =$ sum of all bits of $F(m)$. (**Hint:** The forgery need not succeed with probability 1.)

   (b) $Tag(m) = (F(m_L), F(m_L + m_R))$, where m_L and m_R are the left and right half of m.

   (c) $Tag(m) = F(m_L\mathtt{0}) + F(m_R\mathtt{1})$. (**Hint:** Eve needs to carefully choose her messages.)

3. This question concerns the PRP Pad encryption scheme from Lecture 5. Recall that encryptions of m are of the form $(x, P(x + m))$. Assume x and m are 4 bits long.

   (a) Eve intercepts ciphertext $(\mathtt{0100}, \mathtt{1110})$. She happens to know that it encrypts message `0000`. How can she turn it into an encryption of `1101`?

   (b) Bob is expecting that Alice's message has Hamming weight at most one. He declares a decryption error if it is not. Eve can observe decryption errors. She intercepts an encryption of either $m = \mathtt{0001}$ or $m' = \mathtt{1000}$. How can she tell the two apart?

   (c) Alice and Bob now authenticate the ciphertext c using a PRF MAC. Describe the resulting encryption and decryption algorithms.

   (d) Why do Eve's attacks from parts (a) and (b) fail in the authenticated encryption from part (c)?

4. In this question you will investigate Eve-in-the-middle attacks to El Gamal and RSA encryptions.

   (a) Suppose Eve observes an El Gamal encryption (h, c) of m under public key pk. How can she maul it into an encryption (h', c') of $4m$? How about an encryption (h'', c'') of m^2?

   (b) Work out the attack from part (a) on the ciphertext from part (d) in question 1. Work out Bob's decryptions of (h', c') and (h'', c'').

   (c) Repeat part (a) for RSA ciphertext c.

   (d) Work out the attack from part (c) on RSA with modulus $15 = 3 \cdot 5$, encryption exponent $e = 3$, and message $m = 2$.