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?

   Solution: There are 11 nonzero quadratic residues modulo 23. Residuosity can be checked using Euler's criterion, by raising a nonzero element to the 11th power. The element 3 is a residue because

   $$3^{11} = 3 \cdot 9^5 = 3 \cdot 9 \cdot 81^2 \equiv 4 \cdot (-11)^2 = 4 \cdot 121 \equiv 4 \cdot 6 = 24 \equiv 1 \pmod{23}.$$

   Also, 4 is a quadratic residue because $4 = 2^2$. Finally, -3 is a nonresidue because -1 is a nonresidue modulo 23, whereas 3 is a residue. Alternatively,

   $$(-3)^{11} = (-1)^{11} 3^{11} \equiv -1 \pmod{23}.$$

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

   Solution: The first two equations have solutions: indeed, $4^4 \equiv 3$ and $(-3)^{14} \equiv 4 \pmod{23}$. The third equation does not have a solution because every power of the residue 4 is a residue, whereas -3 is a nonresidue.

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

   Solution: Bob's public key is

   $$pk = g^X = 2^4 = 16 \pmod{23}.$$

   (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 $Y = 3$?

   Solution: The plaintext 7 is a quadratic nonresidue modulo 23. Alice encodes it by squaring:

   $$m = 7^2 = 49 \equiv 3 \pmod{23}.$$

   Since $pk = 16$, the El Gamal ciphertext is

   $$(h, c) = (g^Y, pk^Y m) = (2^3, 16^3 \cdot 3) \equiv (8, 6) \pmod{23},$$

   because $16^3 \equiv 2 \pmod{23}$.

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

   Solution: Bob computes

   $$h^X = 8^4 \equiv 2 \pmod{23}$$

   and recovers

   $$m = c(h^X)^{-1} = 6 \cdot 2^{-1} \equiv 6 \cdot 12 \equiv 3 \pmod{23}.$$

   The square roots of 3 are $\pm 3^6 = \pm 16 = \pm 7$. The plaintext is 7.

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.)

   Solution: Bob recomputes the parity of $F(m)$ and accepts precisely when it equals the claimed one-bit tag. Eve forges the MAC of any message of her choice, say $m = \texttt{000}$, as 0. Her forgery succeeds provided the sum of the bits of $F(\texttt{000})$ is zero. As F is pseudorandom, the forgery succeeds with probability 1/2.

(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.

Solution: Bob recomputes both PRF values and compares them with the two components of the tag. Here is one way for Eve to forge. She requests a tag for $m = \texttt{000001}$. The tag is $(F(\texttt{000}), F(\texttt{001}))$. By swapping the two halves, she obtains $t^* = (F(\texttt{001}), F(\texttt{000}))$, which is a valid tag for $m^* = \texttt{001001}$. The pair (m^*, t^*) is a forgery.

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

Solution: Bob recomputes the two PRF values, adds them, and compares the result with the claimed tag. Eve requests tags for the three messages

$$\texttt{0010}, \qquad \texttt{0111}, \qquad \texttt{0011}.$$

Their respective tags are

$$F(\texttt{000}) + F(\texttt{101}), \qquad F(\texttt{010}) + F(\texttt{111}), \qquad F(\texttt{000}) + F(\texttt{111}).$$

Their sum is $t^* = F(\texttt{010}) + F(\texttt{101})$, which is a tag of the fresh message $m^* = \texttt{0110}$. The pair (m^*, t^*) is a forgery.

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

Solution: Eve keeps the second component and replaces x by

$$x' = x + m + m' = \texttt{0100} + \texttt{0000} + \texttt{1101} = \texttt{1001}.$$

Then $x' + m' = x + m$, so $(\texttt{1001}, \texttt{1110})$ decrypts to $\texttt{1101}$.

(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 $m = \texttt{0001}$ or $m' = \texttt{1000}$. How can she tell the two apart?

Solution: Eve replaces x by $x + \texttt{0001}$. This changes the decrypted message by $\texttt{0001}$. If the original message was $\texttt{0001}$, the result is $\texttt{0000}$ and no error occurs. If it was $\texttt{1000}$, the result is $\texttt{1001}$ and Bob reports an error.

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

Solution: To encrypt, Alice samples x and outputs $(x, P(x + m), F(x, P(x + m)))$. where F is a PRF whose (independent) secret key is shared by Alice and Bob. Upon receiving (x, y, t), Bob first verifies that $t = F(x, y)$. If verification fails, he returns an error without decrypting. If verification succeeds, he decrypts to $P^{-1}(y) + x$.

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

Solution: In part (a), the original tag is $F(\texttt{01001110})$, whereas the mauled ciphertext would require the tag $F(\texttt{10011110})$. Eve does not know the MAC key, so she cannot produce the new tag except with negligible probability. Similarly, the modification in part (b) changes the authenticated ciphertext from (x, y) to $(x + \texttt{0001}, y)$ and therefore requires a new valid tag. Bob rejects the modified ciphertext before decrypting it, so Eve cannot observe the plaintext-validity error.

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?

Solution: Write $(h, c) = (g^r, pk^r \cdot m)$. Then $(h', c') = (h, 4c)$ decrypts to $4m$, while

$$(h'', c'') = (h^2, c^2) = (g^{2r}, pk^{2r} \cdot m^2)$$

is an encryption of m^2 with randomness $2r$. It decrypts to 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'').

Solution: From Question 1(d), $(h, c) = (8, 6)$ encrypts $m = 3$, and Bob's secret exponent is $X = 4$.
For the first attack, Eve computes

$$(h', c') = (h, 4c) = (8, 24) \equiv (8, 1) \pmod{23}.$$

Bob computes $(h')^X = 8^4 \equiv 2 \pmod{23}$ and decrypts to

$$c'((h')^X)^{-1} = 1 \cdot 2^{-1} \equiv 12 \equiv 4m \pmod{23}.$$

For the second attack, Eve computes

$$(h'', c'') = (h^2, c^2) = (8^2, 6^2) \equiv (18, 13) \pmod{23}.$$

Bob computes $(h'')^X = 18^4 \equiv 4 \pmod{23}$ and decrypts to

$$c''((h'')^X)^{-1} = 13 \cdot 4^{-1} \equiv 13 \cdot 6 \equiv 9 = m^2 \pmod{23}.$$

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

Solution: If $c = m^e \bmod n$, then $c' = 4^e c \bmod n$ is an encryption of $4m \bmod n$, and $c'' = c^2 \bmod n$ is an encryption of $m^2 \bmod n$.

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

Solution: Since $15 = 3 \cdot 5$, and $2 \cdot 4 = 8$, and $3^{-1} \equiv 3 \pmod{8}$, the decryption exponent is also $d = 3$. The original ciphertext is

$$c = 2^3 \equiv 8 \pmod{15}.$$

For the first attack,

$$c' = 4^3 c \equiv 4 \cdot 8 \equiv 2 \pmod{15}.$$

Bob decrypts $(c')^d = 2^3 \equiv 8 = 4m \pmod{15}$. For the second attack,

$$c'' = c^2 \equiv 8^2 \equiv 4 \pmod{15},$$

and Bob decrypts $(c'')^d = 4^3 \equiv 4 = m^2 \pmod{15}$.