Please note: These problems only cover material since the second mid-term exam, and even then they do not cover all possible topics or types of problems. Mainly they can serve to provide you with ideas on what types of problems might be asked on this material.

1. Samantha uses the RSA signature scheme with primes \( p = 13 \) and \( q = 23 \) and public verification exponent \( v = 53 \).

(a) What is Samantha’s public modulus? What is her private signing key?

(b) Samantha signs the digital document \( D = 100 \). What is the signature?

Solution: (a) Samantha’s public modulus is \( n = pq = 13 \cdot 23 = 299 \). Her private signing key is \( \frac{1}{53} \pmod{\phi(299)} \). Since \( \phi(299) = 12 \cdot 22 = 264 \), we calculate \( \frac{1}{53} \pmod{264} \) by applying the Euclidean algorithm: we have \( 264 = 4 \cdot 53 + 52 \) and \( 53 = 52 + 1 \), and so \( 1 = 53 - 52 = 53 - (264 - 4 \cdot 53) = 5 \cdot 53 - 264 \).

Therefore, Samantha’s private signing key is \( \frac{1}{53} \equiv 5 \pmod{264} \).

(b) Samantha signs \( D = 100 \) by evaluating \( D^5 \pmod{299} \). Since \( D^5 \equiv 16 \pmod{299} \), the digital signature is \( (100, 16) \).

2. Given that 3 is a primitive root modulo 29, use Shanks’ Babystep-Giantstep Algorithm to find \( x \) so that \( 3^x \equiv 2 \pmod{29} \).

Solution: Let \( N = \lceil \sqrt{p-1} \rceil + 1 \). We calculate two lists:

\[
3^j \pmod{29}, \ 0 \leq j < 6: \quad 1, 3, 9, 27, 23, 11;
\]

\[
2 \cdot 3^{-6k} \pmod{29}, \ 0 \leq k < 6: \quad 2, 15, 11, 10, 17, 26.
\]

Since 11 appears on both lists with \( j = 5 \) and \( k = 2 \), the Babystep-Giantstep Algorithm yields that \( x = j + Nk \equiv 5 + 6 \cdot 2 = 17 \).

A note on calculating the above lists quickly: for the first list, each term is obtained from the previous term by multiplying by 3; for the second list, each term is obtained from the previous term by multiplying by \( 3^{-6} \pmod{29} \).

In answering this question, we did not need to complete the second list — once we got to 11 on the second list, we could stop since we had obtained a match.

3. In this problem we will work modulo 19. Consider the following table.

|      |  1 |  2 |  3 |  4 |  5 |  6 |  7 |  8 |  9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| \(13^m \pmod{19} \) | 13 | 17 | 12 |  4 | 14 | 11 | 10 |  6 |  2 |  7 | 15 |  5 |  8 |  9 |  3 |  1 |

(a) Calculate the discrete logarithms \( L_{13}(7) \) and \( L_{13}(7^{203}) \).

(b) Alice and Bob are using the Diffie-Hellman key exchange protocol with \((p, \alpha) = (19, 13)\) to agree on a key for a shift cipher. Bob’s secret exponent is 5, and he receives the message \( 11, \text{SVVRVBA} \).

What message did Alice send to him?

(c) What information did Bob exchange with Alice to notify her of the key they would be using?
Solution: (a) From the table we see that \( L_{13}(7) = 12 \). Therefore \( L_{13}(7^{203}) \equiv 203 \cdot L_{13}(7) \) (mod 18), and so \( L_{13}(7^{203}) \equiv 203 \cdot 12 \equiv 6 \) (mod 18).

(b) The first part of the message is used to obtain the key for the shift cipher. Bob finds the key by calculating \( K \equiv 11^5 \equiv 7 \) (mod 19). Bob shifts \( \text{SVVRVBA} \) by \(-7\) decrypt and finds the decrypted message \( \text{LOOKOUT} \).

(c) Bob would exchange \( 13^5 \equiv 14 \) with Alice to let her know what key they were agreeing to.

4. Suppose \( p \) is a large prime and \( \alpha \) is a primitive root for \( p \). For \( m \in \mathbb{Z} \), define \( h(m) = \alpha^m \) (mod \( p \)).

(a) Explain how \( h \) is pre-image resistant.

(b) Show that \( h \) is not strongly collision-free by finding a counterexample.

Solution: (a) To show that \( h \) is pre-image resistant, we need to show that for a given \( y \in \{1, 2, \ldots, p-1\} \), it is difficult to find \( m \in \mathbb{Z} \) such that \( h(m) = y \). Now finding such an \( m \) is equivalent to solving the congruence
\[
\alpha^m \equiv y \pmod{p}.
\]
In other words, finding \( m \) is equivalent to the Discrete Logarithm Problem modulo \( p \), which is computationally infeasible for large \( p \).

(b) For numbers \( m_1, m_2 \), we know that
\[
m_1 \equiv m_2 \pmod{p-1} \implies \alpha^{m_1} \equiv \alpha^{m_2} \pmod{p} \implies h(m_1) = h(m_2).
\]
Therefore, since we can easily pick two distinct numbers \( m_1 \) and \( m_2 \) with \( m_1 \equiv m_2 \pmod{p-1} \), in which case \( h(m_1) = h(m_2) \), it follows that it is easy to find collisions for \( h \).

5. Alice is signing a document using the ElGamal signature scheme. She is using \( p = 23 \) and \( \alpha = 5 \). She chooses \( a = 9 \) for her private exponent.

(a) What is Alice’s public key?

(b) Demonstrate how Alice signs the document \( D = 10 \). Be specific.

(c) How does Bob verify that Alice has signed the document?

Solution: (a) Much like in 3(a), Alice’s public key is \((p, \alpha, \beta)\) with \( \beta \equiv \alpha^a \pmod{p} \). Since \( \alpha^a \equiv 5^9 \equiv 11 \pmod{23} \). Therefore, her public key is \( \{(p, \alpha, \beta) = (23, 5, 11)\} \).

(b) Alice selects a secret number \( k \), with \( 2 \leq k \leq p-1 \) and \( \gcd(k, p-1) = 1 \). Suppose she selects \( k = 7 \). She computes
\[
r \equiv \alpha^k \equiv 5^7 \equiv 17 \pmod{23},
\]
and she computes
\[
s \equiv \frac{1}{k} (D - ar) \equiv 19(10 - 9 \cdot 17) \equiv 11 \pmod{22}.
\]
The signed document is then \( (D, r, s) = (10, 17, 11) \).

(c) Bob uses Alice’s public key to compute
\[
v_1 \equiv \beta^r \cdot r^s \equiv 11^{17} \cdot 17^{11} \equiv 9 \pmod{23}
\]
and
\[
v_2 \equiv \alpha^D \equiv 5^{10} \equiv 9 \pmod{23}.
\]
Since \( v_1 = v_2 \pmod{23} \), Bob concludes that Alice’s signature is valid.
6. Using our coin flipping protocol, Alice selects \( n = 35 \), and then Bob chooses \( x_0 = 11 \).

(a) What is the number \( y \) that Bob sends to Alice?

(b) Alice computes the four solutions to \( x^2 \equiv y \pmod{35} \). What are they?

(c) Alice chooses the smallest of the solutions in (b) and sends it to Bob. Who does Bob declare as the winner, and why?

Solution: (a) \( y \equiv x_0^2 \pmod{35} \), so \( y \equiv 11^2 \equiv 16 \pmod{35} \).

(b) Alice sees that \( y \equiv 1 \pmod{5} \) and \( y \equiv 2 \pmod{7} \), so she wants to solve simultaneously \( x^2 \equiv 1 \pmod{5} \) and \( x^2 \equiv 2 \pmod{7} \). By inspection, we see that

\[
x \equiv \pm 1 \pmod{5}, \quad x \equiv \pm 3 \pmod{7}.
\]

Using the Chinese Remainder Theorem, we find that \( x \equiv \pm 4 \pmod{35} \) and \( x \equiv \pm 11 \pmod{35} \).

(c) Alice sends 4 back to Bob. Since \( 4 \not\equiv \pm 11 \pmod{35} \), Bob wins.