1. Suppose you wish to establish a session key with Alice using the DH algorithm. Suppose that you agreed with her that you will be both using a group $\mathbb{Z}_{27}^*$ generated by 5. Explain how do you establish a common session key with Alice, provided that Alice's share of the session key is 2.

   (a) Select my private key $x \in \{1, 2, \ldots, \varphi(27)\}$ uniformly at random. Let $x = 6$.

   (b) Send $5^6 \bmod 27 = 19$ to Alice.

   (c) Receive Bob's share $y = 2$.

   (d) Obtain the session key by computing $2^6 \bmod 27 = 10$.

2. Suppose you are Carol who is eavesdropping on the communication session between Alice and Bob, who are about to establish a common session key using the DH algorithm. You know that they both use group $\mathbb{Z}_9$ generated by 2. You see that Alice sent 7 to Bob, and Bob sent 5 to Alice. You have intercepted both messages - what are your subsequent actions to execute a MITM attack? Why is this attack possible?

   (a) Select my private key $z \in \{1, 2, \ldots, \varphi(27)\}$ uniformly at random. Let $z = 3$.

   (b) Send your share of the session key $2^3 \bmod 9 = 8$ to Alice and Bob

   (c) Compute the session key to communicate with Alice as $7^3 \bmod 9 = 1$.

   (d) Compute the session key to communicate with Bob as $5^3 \bmod 9 = 8$.

   The MITM attack is possible due to the lack of authentication of the communicating parties.

3. Which computational problem does the security of DH rely on?

   The security of DH is based on the assumption about one–wayness of the modular exponentiation operation. It is believed that the inverse operation $\phi : x \mapsto g^x \bmod n$, the discrete logarithm problem (given $g^x \bmod n$, find x) cannot be efficiently solved.

4. Given an RSA public exponent value $e = 3$, find suitable values of primes p and q.

   Suitable values of p and q must satisfy the identity $\gcd(e, p - q) = \gcd(e, q - 1) = 1$.

5. What is wrong with making RSA calculations in rings $\mathbb{Z}_p$ or $\mathbb{Z}_{p^2}$ instead of a ring $\mathbb{Z}_n$ with composite modulus?

   An attacker can efficiently calculate $\varphi(p) = p - 1$ and $\varphi(p^2) = p^2 - p$ and obtain the private exponent.

6. Given $p = 5, q = 11, e = 3$, encrypt a message $m = 32$, and decrypt it.

   Encryption: $32^3 \bmod 55 = 43$. Decryption: $43^{27} \bmod 55 = 32$.

7. Given $p = 13, q = 17, e = 5$, sign a message $m = 19$, and verify the signature it.

   Signature: $19^{77} \bmod 221 = 15$. Verification: $15^5 \bmod 221 = 19$

8. Factor RSA modulus $n = 323$ into its prime factors p and q, given a square root of unity in $\mathbb{Z}_{323}$, which is 305.

$$\gcd(323, 304) = 19$$
$$\gcd(323, 306) = 17$$

   Hence, $323 = 17 \cdot 19$.

9. Find the square roots of 1 in $\mathbb{Z}_{143}$, where $143 = 11 \cdot 13$.

   By the Bézout identity, $6 \cdot 11 - 5 \cdot 13 = 1$, hence applying $\psi : \mathbb{Z}_{11} \times \mathbb{Z}_{13} \to \mathbb{Z}_{143}$, the two of the non-trivial square roots are

$$(1, 12) \mapsto 13 \cdot (-5) + 12 \cdot 6 \cdot 11 \bmod 143 = 12$$
$$(10, 1) \mapsto 10 \cdot (-5) \cdot 13 + 1 \cdot 6 \cdot 11 \bmod 143 = 131$$

   The other two square roots of unity are trivial roots 1 and 142.

10. Solve for x:

$$x \equiv 2 \bmod 3$$
$$x \equiv 3 \bmod 4$$

    Solution: $x \equiv 2 \cdot 4 - 3 \cdot 3 \bmod 12 = 11$.

11. Show that $\mathbb{Z}_5^*$ is generated by 2.

    $\langle 2 \rangle = \{2, 4, 3, 1\} = \mathbb{Z}_5^*$. Therefore, 2 generates $\mathbb{Z}_5^*$.

12. Find $\text{ord}(4) \in \mathbb{Z}_{11}^*$.

    $\langle 4 \rangle = \{4, 5, 9, 3, 1\}$. It can be seen that 5 is the smallest integer satisfying $4^5 \equiv 1 \bmod 11$, and hence $\text{ord}(4) = 5$.

13. Show that all non-identity elements are generators of $\mathbb{Z}_7$.

    $\mathbb{Z}_7$ is a prime order group, and by the Lagrange theorem, for any $a \in \mathbb{Z}_7$, either $\text{ord}(a) = 1$ or $\text{ord}(a) = 7$. Since the identity 0 is unique and $\text{ord}(0) = 1$, all the other elements must have order 7, which makes them generators of $\mathbb{Z}_7$.

14. Show that an element of order 6 cannot exist in $\mathbb{Z}_{16}^*$.

    $\text{ord}(\mathbb{Z}_{16}^*) = \varphi(16) = 8$, and by the Lagrange theorem, a group with 8 elements can have elements of orders $1, 2, 4, 8$. $\mathbb{Z}_{16}^*$ cannot contain an element of order 6.

15. Show that a subgroup of order 5 cannot exist in $\mathbb{Z}_{15}^*$.

    It can be seen that $\text{ord}(\mathbb{Z}_{15}^*) = \varphi(15) = 8$, and by the Lagrange theorem, possible orders of subgroups are $1, 2, 4, 8$. A subgroup of order 5 cannot exist in $\mathbb{Z}_{15}^*$.

16. If a group $\mathbb{G}$ contains elements of order 4 and order 7, what are possible orders of $\mathbb{G}$?

    Any multiple of $\text{lcm}(4, 7)$.

17. A group $\mathbb{G}$ contains an element $a \in \mathbb{G}$ such that a^{12} is the identity element in $\mathbb{G}$. What are the possible orders of a?

    Any $\text{ord}(a) \in \{d \in \mathbb{N} : d | 12\}$, that is, $1, 2, 3, 4, 6, 12$.

18. Show that RSA is homomorphic w.r.t multiplication.

$$(m_1^e \bmod n)(m_2^e \bmod n) = m_1^e m_2^e \bmod n = (m_1 m_2)^e \bmod n$$
$$(m_1^d \bmod n)(m_2^d \bmod n) = m_1^d m_2^d \bmod n = (m_1 m_2)^d \bmod n$$

19. Find a collision of a hash function $h : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_6$ defined by $h : (a, b) \mapsto ab \bmod 6$.

    An example of a collision is $(0, a), (b, 0)$ for all $a, b \in \mathbb{Z}$. Another example of a collision is $(1, 1)$ and $(1, 7)$, also $(1, 8)$ and $(2, 4)$, also $(3, 3)$ and $(3, 5)$, …

20. Given a hash function $h : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_{12}$ defined by $h : (a, b) \mapsto ab \bmod 12$ find a pre–image of 9.

    One of the pre–images of 9 is, in example, $(3, 7)$.

21. Given a hash function $h : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_{11}$ defined by $h : (a, b) \mapsto ab \bmod 11$, given a hash value 10, and a pre–image $(10, 1)$, find a second pre–image of 10.

    $(3, 7)$ is a second pre–image of 10.

22. Given a hash function $h : \mathbb{Z} \to \mathbb{Z}_{11}^*$ defined by $\psi : x \mapsto 2^x \bmod 11$, given a hash value 8 and a pre–image 3, find a second pre–image of 8.

    Examples of such collisions are elements in the set $\{13 + 10k\}$ for $k \in \mathbb{N}$.

$h(13) = 2^{13} \bmod 11 = 8$	$h(23) \mapsto 2^{23} \bmod 11 = 8$	$h(33) \mapsto 2^{33} \bmod 11 = 8$
$h(43) \mapsto 2^{53} \bmod 11 = 8$	$h(63) \mapsto 2^{53} \bmod 11 = 8$	$h(33) \mapsto 2^{63} \bmod 11 = 8$
$\dots$	$\dots$	$\dots$