1. Evaluate the following (4 points)
   a) \(4^{283} \mod 10\)
   b) \(9^{682} \mod 10\)

   a) \(\Phi(10) = (2-1)(5-1) = 4\)
      We can reduce the exponent modulo 4. 238 is 3 mod 4
      \(4^{283} = 4^3 \mod 10 = 4\)

   b) 9 is just -1 mod 10. All even powers are 1!

2. A and B use Diffie Helman key exchange with parameters \(p = 79\), \(g=3\). A chooses private key 5 and B choose its private key as 7. What is the common secret computed by A and B? (6 points)

   \[K(AB) = g^{(5 \times 7)} \mod p = 39.\]
   Note that \(g^5 = 6\) and \(6^7 = 39\).
   Similarly \(g^7 = 54\) and \(54^3 = 39\).

3. To generate its RSA key pairs, A generates two primes \(p=59\) and \(q=67\). What is the smallest encryption exponent that can be chosen by A? What is the corresponding decryption exponent? (8 points)

   \(n = 59 \times 67 = 3953\)
   \(\Phi(n) = (59-1)(67-1) = 3828\)
   We cannot choose \(e=3\) as 3828 is a multiple of 3 (3828/3 = 1276).
   We can choose \(e=5\). Inverse of \(e\) mod 3828 is 2297.
   Decryption exponent is \(d = 2297\).
   Check \(5 \times 2297 \mod 3828 = 1\)

   Example: Let \(P = 1496\)
   \(C = 1496^5 \mod 3953 = 3543.\)
   \(P' = 3543^2296 \mod 3953 = 1496 = P\)

   Square and Multiply Algorithm:
   \[2297 = 2^11 + 2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^0 = [100011111001] \text{ in binary notation}\]
   \[z=1\]
   \[b=1; z = z \times 2 \times 3543 \mod 3953 = 3543\]
   \[b=0; z = 3543 \times 2 = 2074\]
   \[b=0; z = 2074^2 = 612\]
   \[b=0; z = 612^2 = 2962\]
   \[b=1; 2962^2 \times 3543 = 1737 \times 3543 = 3323\]
   \[b=1; 3323^2 \times 3543 = 1600 \times 3542 = 198\]
   \[b=1; 198^2 \times 3543 = 3627 \times 3543 = 3211\]
   \[b=1; 3211^2 \times 3543 = 1097 \times 3543 = 872\]
   \[b=1; 872^2 \times 3543 = 1408 \times 3543 = 3811\]
   \[b=0; 3811^2 = 399\]
   \[b=0; 399^2 = 1081\]
   \[b=1; 1081^2 \times 3543 = 2426 \times 3543 = 1496\]

4. Explain why it is very much desirable to lower the verification complexity for digital signatures (and not as crucial to lower the signing complexity) (4 points)

   To prevent denial of service attacks. If a server requires to check the signature enclosed in packets by every client, an attacker can simply send random packets to the server. The server will recognize that the packet is meaningless only after it verifies the signature. Thus with very little effort an attacker can bring down the efficiency of the server.
5. State True or False (8 points)
   (a) Generating RSA key pairs is more expensive than generating El Gamal key pairs
       True. For RSA the operation of primality testing to choose two random primes can be substantially more expensive. For El Gamal we just need to choose a random private key and compute the public key (one exponentiation operation).
   (b) An RSA key pair can be used for both encryption and digital signatures.
       True
   (c) An El Gamal key pair can be used for both encryption and digital signatures.
       True. Alice can use the same private key \( a \) and public key \( \alpha \) for both encryption and signatures.
   (d) RSA signatures require less verification complexity compared to El Gamal signatures.
       True. In RSA we normally choose very low value of the encryption exponent. If the encryption exponent is a 3 bit value the verifiers who compute \( S^e \mod n \) need to perform only 3 iterations of the square and multiply algorithm.
   (e) For RSA the complexity of decryption is generally more than the complexity of encryption.
       True. For decryption we need to exponentiate with the private exponent.
   (f) For El Gamal the complexity of encryption and decryption are comparable.
       True.
   (g) If a 1024 bit prime modulus is used for El Gamal, the bandwidth required for sending an encrypted 128 bit key is at least 2048 bits.
       True. Encrypting the key results in two 1024 bit values – the mask and the encrypted value.
   (h) The security of RSA depends on the assumption that computing discrete logarithms is an intractable problem.
       False. It depends on the assumption that factorization (of a product of two large primes) is a hard problem.