1. Use the square and multiply algorithm to evaluate $234^{231} \mod 535$. Show all steps.

2. Illustrate RSA encryption and decryption for the choice of $p=7$, $q=13$
   i. What is $\phi(n)$?
   ii. Assuming that the minimum possible encryption exponent is chosen, what is the encryption exponent $e$?
   iii. What is the corresponding decryption exponent $d$?
   iv. Illustrate RSA encryption and decryption with the above choices of $e$ and $d$ for
      (a) $P = 6$
      (b) $P = 7$.
   v. It was discussed in the class that the working of RSA rests on the generalized Euler-Fermat theorem which states that $a^\phi(n) \equiv 1 \mod n$ only for $(a, n) = 1$, where $k$ is any integer. In the second example ($P = 7$) this requirement is not satisfied as 7 is not relatively prime to $n$. Nevertheless, RSA encryption / decryption still works! Can you explain?

3. Illustrate Diffie-Helman Key exchange when Alice and Bob choose $p=41$, $g=3$.
   • Assume that Alice chooses a secret $a=13$ and Bob chooses $b=4$. What is the common secret computed by Alice and Bob?

4. Alice chooses an El Gamal encryption scheme with $p=41$ and $g=3$. Alice chooses a private key $a=21$.
   i. What is Alice's public key?
   ii. Bob desires to send the message $P=11$ to Alice such that no one except Alice can decrypt the value. Illustrate how Bob will send the message to Alice (assume that Bob chooses $k=5$ for masking).
   iii. Illustrate how Alice can sign a message which has a hash of $h=21$ (for a choice of $k=7$).