1. Analyse the double encryption in RSA using two different \( e \), but the same \( n \). Does it increase the security?

2. Make the following for the elliptic curve \( E: y^2 = x^3 - 2 \) modulo 7:
   
   a) List the points on \( E \).
   
   b) Find the sum \((3, 2) + (5, 5)\) on \( E \).
   
   c) Find the sum \((3, 2) + (3, 2)\) on \( E \).

3. Show that if \( P = (x, 0) \) is a point on an elliptic curve, then \( 2P = \infty \).

4.

   a) Show that \( Q = (0, 1) \) on \( y^2 = x^3 + 1 \) satisfies \( 6Q = \infty \). (Hint: Compute \( 3Q \), then use the previous exercise.)

   b) Your computations in a) probably have shown that \( 2Q \neq \infty \) and \( 3Q \neq \infty \). Use this to show that the points \( \infty, Q, 2Q, 3Q, 4Q, 5Q \) are distinct.

5. Show how an opponent can use the vulnerability of the following protocol in order to decrypt the messages. Each node \( N \) in the network has been assigned a unique secret key \( K_n \). This key is used to secure communication between the node and a trusted server. That is, all the keys are stored also on the server. User A, wishing to send a secret message \( M \) to user B, initiates the following steps:

   **Step1.** A generates a random number \( R \) and sends to the server his name \( A \), destination \( B \), and \( E(K_a, R) \).

   **Step2.** Server responds by sending \( E(K_b, R) \) to \( A \).

   **Step3.** A sends \( E(R, M) \) together with \( E(K_b, R) \) to \( B \).

   **Step4.** B knows \( K_b \), thus decrypts \( E(K_b, R) \) to get \( R \) and will subsequently use \( R \) to decrypt \( E(R, M) \) to get \( M \).

6. Consider the following protocol for communication between two parties, for example, user A wishing to send message \( M \) to user B. In the protocol, \( PU_b \) and \( PU_a \) are the public keys of B and A, respectively. The symbol \( E(PU, M) \) means encryption of the message \( M \) with the public key \( PU \).

   **Step1.** A sends B the following block: \((A, E(PU_b, [M, A]), B)\).

   **Step2.** B acknowledges receipt by sending to A the following block:
   \((B, E(PU_a, [M, B]), A)\).

   Is it possible to simplify the protocol as follows:

   **Step1.** A sends B the following block: \((A, E(PU_b, M), B)\).
Step 2. B acknowledges receipt by sending to A the following block:

\((B, E(PU_a, M), A)\).

7. Consider the following protocol, where \(A\) and \(B\) authenticate each other with the help of a trusted server. \(A\) and \(B\) have secret keys \(K_{AS}\) and \(K_{BS}\), respectively, with the server.

\begin{align*}
1. & A \rightarrow B: \ A \\
2. & B \rightarrow A: \ N_B \\
3. & A \rightarrow B: \ \{N_B\}^{K_{AS}} \\
4. & B \rightarrow S: \ \{A, \{N_B\}^{K_{AS}}\}^{K_{BS}} \\
5. & S \rightarrow B: \ \{N_B\}^{K_{BS}}
\end{align*}

Develop an attack, where an intruder \(I\) makes \(B\) to accept the run in which \(I\) is masquerading as \(A\). In order to achieve this result, the intruder must start two runs with \(B\), in one of which \(I\) claims to be \(A\). The two protocol runs continue in parallel but \(I\) simply sends a random value \(R\) when asked to respond to the challenge intended for \(A\).