Alice and Dave are in different parts of the world, and they want to communicate by email. They both want to prevent the eavesdropper Eve from reading their email messages, and so they plan to use Public-Key Encryption. Use this list of keys for your answers:

- Alice's Public Key is 42, Cindy's Public Key is 67, Edith's Public Key is 34,
- Alice's Private Key is 117, Cindy's Private Key is 92, Edith's Private Key is 125,
- Bob's Public Key is 50, Dave's Public Key is 101, Frank's Public Key is 91,
- Bob's Private Key is 109, Dave's Private Key is 58, Frank's Private Key is 68.

Indicate what Alice and Dave should do by checking checkboxes and by filling in the keys.

1. **(2 points)** Dave wants to send a confidential message to Alice. What should Dave do first?
   - [ ] Encrypt  [ ] Decrypt  [ ] Sign  [ ] Verify
   - Message #1 using key **42**.

2. **(2 points)** Dave sends the result of the above operation to Alice. What should Alice do to read the message?
   - [ ] Encrypt  [ ] Decrypt  [ ] Sign  [ ] Verify
   - Received Message #1 using key **117**.

3. **(2 points)** Alice wants to send a confidential reply to Dave, and she wants him to be sure that it is from her. What should Alice do?
   - First  [ ] Encrypt  [ ] Decrypt  [ ] Sign  [ ] Verify
   - Message #2 using key **117**.
   - Then  [ ] Encrypt  [ ] Decrypt  [ ] Sign  [ ] Verify
   - the result of the previous step using key **101**.

4. **(2 points)** Alice sends the result of the above operation to Dave. What two steps should Dave perform so that he can read the encrypted message and ensure that it really is from Alice?
   - First  [ ] Encrypt  [ ] Decrypt  [ ] Sign  [ ] Verify
   - Received Message #2 using key **58**.
   - Then  [ ] Encrypt  [ ] Decrypt  [ ] Sign  [ ] Verify
   - the result of the previous step using key **42**.

5. **(2 points)** An advantage of Symmetric-Key Encryption is that it is much simpler compared to the operations of Public-Key Encryption above, but it has two big disadvantages. What is one disadvantage of Symmetric-Key Encryption?
   - [ ] Difficult to secure key management
   - OR
   - [ ] Need exponential number of keys between members
Cindy and Frank are in different parts of the world, and they want to communicate by email. They both want to prevent the eavesdropper Eve from reading their email messages, and so they plan to use Public-Key Encryption. Use this list of keys for your answers:

Alice's Public Key is 42, Cindy's Public Key is 67, Edith's Public Key is 34,
Alice's Private Key is 117, Cindy's Private Key is 92, Edith's Private Key is 125,
Bob's Public Key is 50, Dave's Public Key is 101, Frank's Public Key is 91,
Bob's Private Key is 109, Dave's Private Key is 58, Frank's Private Key is 68.

Indicate what Cindy and Frank should do by checking checkboxes and by filling in the keys.

1. (2 points) Frank wants to send a confidential message to Cindy. What should Frank do first?
   \[
   \begin{array}{c}
   \checkmark \text{ Encrypt} \\
   \text{ Decrypt} \\
   \text{ Sign} \\
   \text{ Verify}
   \end{array}
   \]
   Message #1 using key 67.

2. (2 points) Frank sends the result of the above operation to Cindy. What should Cindy do to read the message?
   \[
   \begin{array}{c}
   \text{ Encrypt} \\
   \checkmark \text{ Decrypt} \\
   \text{ Sign} \\
   \text{ Verify}
   \end{array}
   \]
   Received Message #1 using key 92.

3. (2 points) Cindy wants to send a confidential reply to Frank, and she wants him to be sure that it is from her. What should Cindy do?
   First \[
   \begin{array}{c}
   \checkmark \text{ Encrypt} \\
   \text{ Decrypt} \\
   \text{ Sign} \\
   \text{ Verify}
   \end{array}
   \]
   Message #2 using key 92.
   Then \[
   \begin{array}{c}
   \checkmark \text{ Encrypt} \\
   \text{ Decrypt} \\
   \text{ Sign} \\
   \checkmark \text{ Verify}
   \end{array}
   \]
   the result of the previous step using key 91.

4. (2 points) Cindy sends the result of the above operation to Frank. What two steps should Frank perform so that he can read the encrypted message and ensure that it really is from Cindy?
   First \[
   \begin{array}{c}
   \text{ Encrypt} \\
   \checkmark \text{ Decrypt} \\
   \text{ Sign} \\
   \text{ Verify}
   \end{array}
   \]
   Received Message #2 using key 68.
   Then \[
   \begin{array}{c}
   \text{ Encrypt} \\
   \checkmark \text{ Decrypt} \\
   \text{ Sign} \\
   \checkmark \text{ Verify}
   \end{array}
   \]
   the result of the previous step using key 67.

5. (2 points) An advantage of Symmetric-Key Encryption is that it is much simpler compared to the operations of Public-Key Encryption above, but it has two big disadvantages. What is one disadvantage of Symmetric-Key Encryption?
   * Difficult to secure key management
   or
   * Need exponential number of keys between members
Edith and Bob are in different parts of the world, and they want to communicate by email. They both want to prevent the eavesdropper Eve from reading their email messages, and so they plan to use Public-Key Encryption. Use this list of keys for your answers:

Alice's Public Key is 42, Cindy's Public Key is 67, Edith's Public Key is 34,
Alice's Private Key is 117, Cindy's Private Key is 92, Edith's Private Key is 125,
Bob's Public Key is 50, Dave's Public Key is 101, Frank's Public Key is 91,
Bob's Private Key is 109, Dave's Private Key is 58, Frank's Private Key is 68.

Indicate what Edith and Bob should do by checking checkboxes and by filling in the keys.

1. (2 points) Bob wants to send a confidential message to Edith. What should Bob do first?
   - [ ] Encrypt
   - [X] Decrypt
   - [ ] Sign
   - [ ] Verify
   Message #1 using key 34.

2. (2 points) Bob sends the result of the above operation to Edith. What should Edith do to read the message?
   - [ ] Encrypt
   - [X] Decrypt
   - [ ] Sign
   - [ ] Verify
   Received Message #1 using key 125.

3. (2 points) Edith wants to send a confidential reply to Bob, and she wants him to be sure that it is from her. What should Edith do?
   - [X] Encrypt
   - [ ] Decrypt
   - [ ] Sign
   - [ ] Verify
   Message #2 using key 125.
   Then
   - [X] Encrypt
   - [ ] Decrypt
   - [ ] Sign
   - [ ] Verify
   the result of the previous step using key 50.

4. (2 points) Edith sends the result of the above operation to Bob. What two steps should Bob perform so that he can read the encrypted message and ensure that it really is from Edith?
   - [ ] Encrypt
   - [X] Decrypt
   - [ ] Sign
   - [ ] Verify
   Received Message #2 using key 109.
   Then
   - [ ] Encrypt
   - [X] Decrypt
   - [ ] Sign
   - [ ] Verify
   the result of the previous step using key 34.

5. (2 points) An advantage of Symmetric-Key Encryption is that it is much simpler compared to the operations of Public-Key Encryption above, but it has two big disadvantages. What is one disadvantage of Symmetric-Key Encryption?

   * Difficult to secure key management
   * Need exponential number of keys between members