

|  | send the message "NO" to Jennifer. Show how Ted can send the message to <br> Jennifer if he knows e and n. |  |  |
| :--- | :--- | :--- | :--- |
| Q11 | (a) Is hashing safe for passwords? <br> (b) Can hashed passwords be decrypted? <br> (c) How do I know if a password is hashed? <br> (d) Can two passwords have same hash? <br> (e) Do we need padding if the length of the original message is already a multiple <br> of 1024 bits in SHA-512? | $\mathbf{+ 3 + 8}$ | $\mathbf{C O 2}$ |

