1. Show that DES decryption can be done by applying the DES encryption algorithm to the ciphertext with the key schedule reversed.

Ans:

\[ \begin{align*}
L^i &= R^{i-1} \\
R^i &= L^{i-1} \oplus f(R^{i-1}, K^i).
\end{align*} \]

We observe that the function \( f \) does not need to satisfy any type of injective property. This is because a Feistel-type round function is always invertible, given the round key:

\[ \begin{align*}
L_{i-1} &= R^i \oplus f(L^i, K^i) \\
R_{i-1} &= L^i.
\end{align*} \]

Hence we only have to show the effect of the IP and IP–1 functions.

First step is to take the ciphertext and pass it through IP.

Because IP is the inverse of IP–1, the result of this operation is just R16 | LE16, which is equivalent to L0 | R0. Then, we follow the same reasoning as with the Feistel cipher to reach a point where L0 = R16 and R0 = L16. Decryption is completed by passing L0 | R0 through IP–1. Again, because IP is the inverse of IP–1, passing the plaintext through IP as the first step of encryption yields L0 || R0, thus showing that decryption is the inverse of encryption.

2. Describe how DES can be used for message authentication.

Ans:

Suppose Alice wants to Authenticate her to Bob both share the same key.

Alice has a message m. She encrypts c = E(k, m) and send (m, c) to Bob. He verifies D(k, c) = m or E(k, m) = c. Which confirms that it came from Alice.

3. Suppose, the text Alice sends Bob is not encrypted, how would you make sure that the text Alice sends Bob is encrypted and authenticated?

Ans:

Let m be the plain text.
First Encrypt \( c = E(K, m). \)
Then \( c' = E(K, c) \) send (c, c’) to Bob
Bob can verify \( D(K,c') = c \)

4. If the input to S-box S1 is 011010
   a) What bits select the row? Column?

   Ans: Row: 00 = 0 (1, 6 bits)
       Col: 1101 = 13 (2, 3, 4, 5)

   b) What is the output? 9