1. In a DES process, a permutation process is applying on the Key *K=1011101110.*  The fifth bit is remaining unchangeable. If the permutation process is going according to the PC given bellow:

3 4 6 2

7 9 1 8

Answer the following:

1. What is the size of the output key?
2. What will be the sequence of the generated new key?
3. Suppose we have the following sub key and need to apply the shifting bit within the process of a DES algorithm, what will be the output in the following cases?

 *K=101011010001*

1. Find the output of shifting process for *K*, when it is in the 2nd round.
2. Apply the shifting process for the result obtained in the step before when applied to the round three of the DES.
3. Caeser Ciphering is used to encrypt the following information using row number two of the
Table-1.

 *M=MANINTHEMIDDELATTACK*

 Find out the cipher text of the message M.

1. Caeser Ciphering is used to encrypt the following information using a reversed alphabet considering the index of each character in the plaintext. As an example, first letter of the M will be substituted with (Z), second letter with (Y), and so on.

 *M=MANINTHEMIDDELATTACK*

 Find out the cipher text of the message M.

1. Caeser Ciphering is used to encrypt the following information using a reversed alphabet considering the index of each character in the plaintext. As an example, first letter of the M will be substituted with (Z), second letter with (Y), and so on.

 *M=MANINTHEMIDDELATTACK*

 Find out the cipher text of the message M.

1. Caeser Ciphering is used to encrypt the following information using a reversed alphabet considering the index of each character in the plaintext. As an example, first letter of the M will be substituted with (Z), second letter with (Y), and so on.

 *M=MANINTHEMIDDELATTACK*

 Find out the cipher text of the message M.

Table 1

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |