- In a cipher, S-boxes can be either static or dynamic. The parameters in a static S-box do not depend on the key.
  - State some advantages and some disadvantages of static and dynamic S-boxes.
  - Are the S-boxes(substitution tables) in AES static or dynamic?

The aim or benefit of dynamic key-dependent S-Box algorithm is to **increase the security of exiting AES** by introducing different and dynamic S-box in each round of AES, which increases security against algebraic attacks. Earlier number of algebraic attacks designed to break AES

The S-Box component that used in AES is **fixed, and not changeable**. If we can generate this S-Box dynamically, we increase the cryptographic strength of AES cipher system.

(a) Advantages/disadvantages-

1. implementation is simple for static S-Boxes as it can be programmed using fixed tables whereas in dynamic S-boxes, implementation in programming becomes difficult as S-Boxes are now dependent upon the secret keys.

2. Computation of S-Boxes for every encryption/decryption is time consuming and it increases encryption/decryption time

3. Hardware implementation is possible for Cryptographic algorithms using static S-Boxes. For algorithms using dynamic S-Boxes, hardware implementation is either impossible of very expensive.

- AES has a larger block size than DES. Is this an advantage or disadvantage?

  AES allows you to choose a 128-bit, 192-bit or 256-bit key, making it **exponentially stronger than the 56-bit key of DES**. In terms of structure, DES uses the Feistel network which divides the block into two halves before going through the encryption steps.

- AES defines different implementation with three different numbers of rounds. DES defines only one implementation with 16 rounds. What are the

advantages and disadvantages of AES over DES with respect to this difference?

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

- AES defines three different cipher-key sizes(128, 192 and 256); DES defines only one cipher key size(56). What are the advantages and disadvantages of AES with respect to this difference?

Additionally, AES has built-in flexibility of key length, which allows a degree of 'future-proofing' against progress in the ability to perform exhaustive key searches.