**Explain the main concepts in DES.**

Step 1:

The National Institute of Standards and Technology (NIST) published the Data Encryption Standard (DES), a symmetric-key block cypher (NIST).

Step 2:

Because the Data Encryption Standard (DES) has been discovered to be vulnerable to extremely powerful attacks, its popularity has been on the wane.

DES is a block cypher that encrypts data in 64-bit blocks. This implies that 64 bits of plain text are fed into DES, which outputs 64 bits of ciphertext. Encryption and decryption employ the same algorithm and key, with slight variations. The key is 56 bits long.

**How can the same key be reused in triple DES?**

Step 1:

The usage of a double-length DATA key made up of two 8-byte DATA keys is supported by a variant of the triple DES algorithm. The first 8-byte key is reused in the final encoding step in this method. Triple-DES encryption may not be available on your processor due to export constraints.

Step 2:

Rather of employing a single key as in DES, 3DES uses three 56-bit keys to perform the DES algorithm three times: The plaintext is encrypted using key one. The text that was encrypted by key one is decrypted using key two. The text decrypted by key two is encrypted using key three.

 Explain the principles of the IDEA algorithm

Sep 1:

IDEA was created at ETH Zurich, a research university in Zurich, Switzerland, and is widely regarded as safe. The IDEA cypher encrypts text under the notion that security in IDEA is based on ignorance of the secret key rather than keeping the algorithm secret.

Step 2:

IDEA operates on 64-bit blocks and employs a 128-bit key. It converts a 64-bit block of plaintext into a 64-bit block of ciphertext in essence. This plaintext input block is broken into four 16-bit subblocks. It consists of a set of eight identical transformations, each of which is referred to as a round, as well as an output transformation referred to as a half-round. Similar to the 16-bit plaintext block, the ciphertext block is also the exact same size.

A block cypher works in round blocks, with each round including a portion of the encryption key, known as the round key, and additional mathematical operations. The ciphertext for that block is generated after a specific number of rounds.