MULTIPLE DES:
2DES
3DES

Triple DES (3-DES)

In cryptography, Triple DES (3-DES) is a symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.

DES is now considered to be insecure for many applications. This is mainly due to the 56-bit effective key size being too small. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks without designing an entirely new block cipher algorithm.

Triple DES uses a "key bundle" comprising three DES keys, K1, K2, and K3, each of 56 bits (excluding parity bits).
encryption algorithm is:

ciphertext = EK3(DK2(EK1(plaintext)))
i.e., **DES encrypt with K1, DES decrypt with K2, then DES encrypt with K3.**

Decryption is the reverse:

plaintext = DK1(EK2(DK3(ciphertext)))
i.e., **decrypt with K3, encrypt with K2, then decrypt with K1.**

Applications:

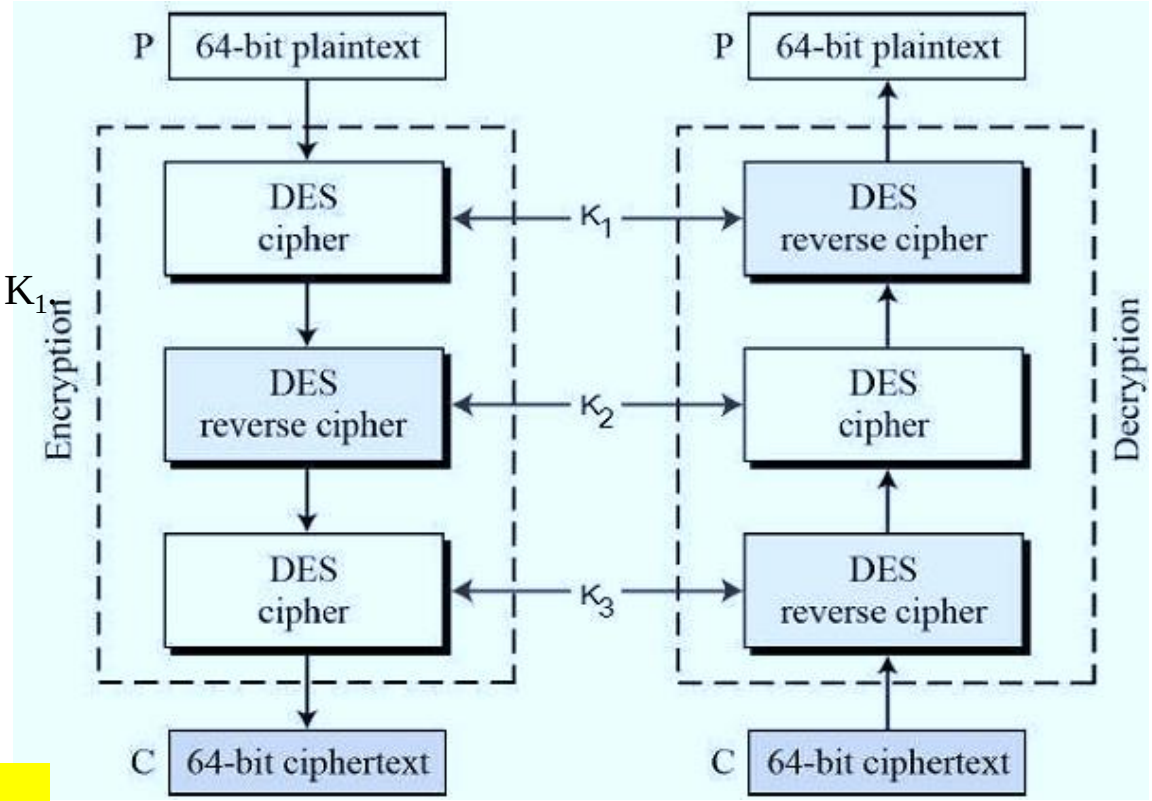
- The electronic payment industry uses Triple DES and continues to develop and promulgate standards based upon it .
- Microsoft OneNote and Microsoft Outlook 2007 use Triple DES to password protect user content.

The encryption-decryption process is as follows –

- Encrypt the plaintext blocks using single DES with key K_1.
- Now decrypt the output of step 1 using single DES with key K_2.
- Finally, encrypt the output of step 2 using single DES with key K_3.
- The output of step 3 is the ciphertext.
- Decryption of a ciphertext is a reverse process.

User first decrypt using K_3, then encrypt with K_2, and finally decrypt with K_1

Structure of 3-KEY Triple DES



NOTE:

- **Due to this design of Triple DES as an encrypt–decrypt–encrypt process, it is possible to use a 3TDES (hardware) implementation for single DES by setting K_1, K_2, and K_3 to be the same value. This provides backwards compatibility with DES.**
- **Second variant of Triple DES (2TDES) is identical to 3TDES except that $K_3$is replaced by K_1. In other words, user encrypt plaintext blocks with key K_1, then decrypt with key K_2, and finally encrypt with K_1 again. Therefore, 2TDES has a key length of 112 bits.**
- **Triple DES systems are significantly more secure than single DES, but these are clearly a much slower process than encryption using single DES.**

- **Benefits of using 3DES**

➢ With 168-bit key length, it overcomes the vulnerability to brute-force attack of DEA.
➢ Since it is based on the DES algorithm, it is very easy to modify existing software to use Triple DES.

- **Drawbacks**

➢ It has three times as many rounds as DES, is correspondingly slower.
➢ Uses 64-bit block size. For reasons of both efficiency and security, a larger block size is desirable.
➢ The National Institute of Standards and Technology (NIST) issued a call for proposals to develop the Advanced Encryption Standard (AES) as a replacement for DES