Triple DES (Triple Data Encryption Algorithm - TDEA)

- Triple DES was conceived in response to concerns about the weakness of DES to the exhaustive key-search attacks. The basic concept is to use double or triple length keys. In fact, double length keys have been recommended for the financial industry for many years.

- The procedure for decrypting something is the same as the procedure for encryption, except it is executed in reverse. In DES, data is encrypted and decrypted in 64 -bit chunks. The input key for DES is 64 bits long; the actual key used by DES is only 56 bits in length.

- Recall that the least significant (right-most) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56 bits.

- Triple DES algorithm uses three iterations of common DES cipher. It receives a secret 168-bit key, which is divided into three 56-bit keys.

- Use of multiple length keys leads to the Triple-DES algorithm, in which DES is applied three times. If we consider a triple length key to consist of three 56-bit keys K1, K2, K3 then encryption is as follows:

    - Encrypt with K1
    - Decrypt with K2
    - Encrypt with K3

- This can be stated mathematically as follows:

    $\mathbf{C = E_{K3}\,[D_{K2}\,[E_{K1}[M]]]}$

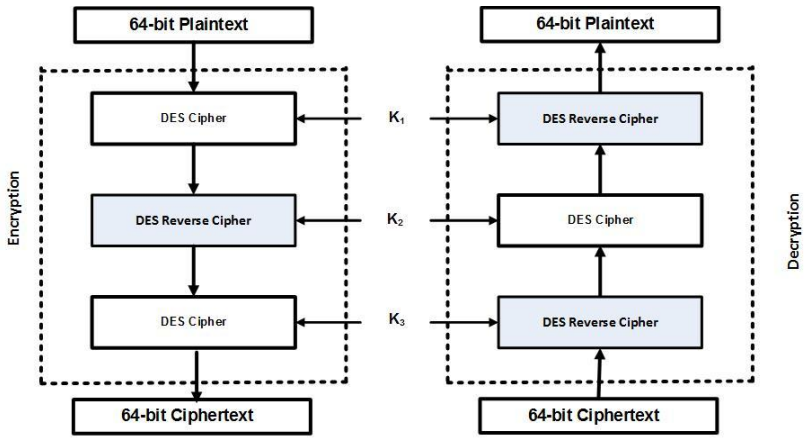
- Decryption is the reverse process:

    - Decrypt with K3
    - Encrypt with K2
    - Decrypt with K1

- This can be stated mathematically as follows:

    $\mathbf{M = D_{K1}\,[E_{K2}\,[D_{K3}[C]]]}$

- The following diagram illustrates the process:



Triple-DES Flow Diagram

- The standard specifies three modes of operation:
    - Keying option 1: All three keys are independent: $K_1 \neq K_2 \neq K_3$
    - Keying option 2: K_1 and K_2 are independent, and $K_3 = K_1$.
    - Keying option 3: All three keys are identical, i.e. $K_1 = K_2 = K_3$.

- Using keying option 1: the key space is 56 x 3 = 168 bits (2^{168}) ; there is no known practical attack against it.

- Using keying option 2: the key space is 56 x 2 = 112 bits (2^{112}); this is double the key length of DES.

- Using keying option 3: the key space is the same as using a single-length (56-bit key). Thus it is possible for a system using triple-DES to be backward-compatible with a system using single-DES.

- This means that the effective key strength for Triple DES is actually 168 bits because each of the three keys contains 8 parity bits that are not used during the encryption process.

- **Triple DES systems are significantly more secure than single DES, but it is a much slower process than encryption using single DES, and requires much more in the way of computing resources.**

- Many protocols/applications use 3DES (example PGP).

- The electronic payment industry uses Triple DES and continues to develop and promulgate standards based upon it (e.g. EMV, Europay-Visa-Mastercard).

- The effective security 3DES provides is only 112 bits due to meet-in-the-middle attacks (see the accompanying paper on MITM analysis). Triple DES runs **three times slower** than DES, but is much more secure if the high security key exchange protocols are adhered to.