CRYPTO M2 (p-4)

techworldthink • March 19, 2022

Double Strength Encryption

Double strength encryption, also called as multiple encryption, is the process of encrypting an already encrypted text one or more times, either with the same or different algorithm/pattern.

The other names for double strength encryption include cascade encryption or cascade ciphering.

Levels of Double Strength Encryption

Double strength encryption includes various levels of encryption that are explained here under −

First layer of encryption

The cipher text is generated from the original readable message using hash algorithms and symmetric keys. Later symmetric keys are encrypted with the help of asymmetric keys. The best illustration for this pattern is combining the hash digest of the cipher text into a capsule. The receiver will compute the digest first and later decrypt the text in order to verify that text is not tampered in between.

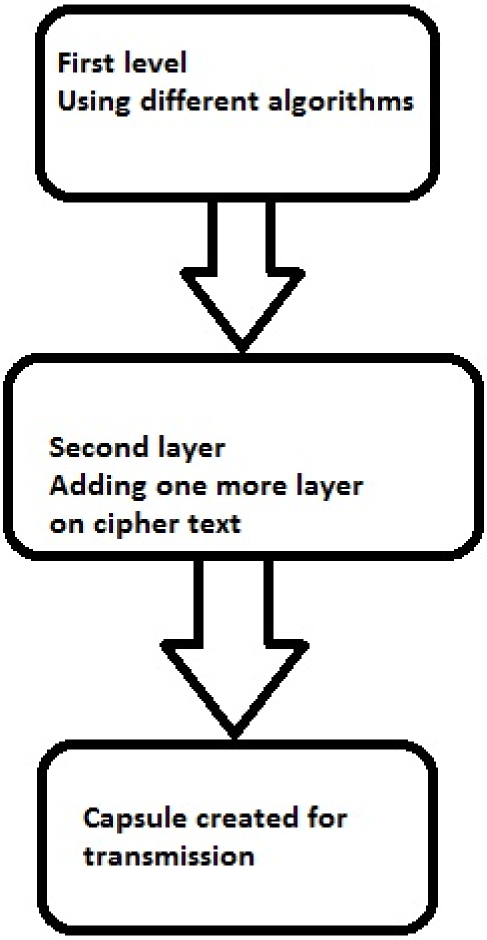
Second layer of encryption

Second layer of encryption is the process of adding one more layer to cipher text with same or different algorithm. Usually, a 32-bit character long symmetric password is used for the same.

Third layer of encryption

In this process, the encrypted capsule is transmitted via SSL/TLS connection to the communication partner.

The following diagram shows double encryption process pictorially −



Strength Encryption

Hybrid Cryptography

Hybrid cryptography is the process of using multiple ciphers of different types together by including benefits of each of the cipher. There is one common approach which is usually followed to generate a random secret key for a symmetric cipher and then encrypt this key via asymmetric key cryptography.

Due to this pattern, the original message itself is encrypted using the symmetric cipher and then using secret key. The receiver after receiving the message decrypts the message using secret key first, using his/her own private key and then uses the specified key to decrypt the message.

Triple DES

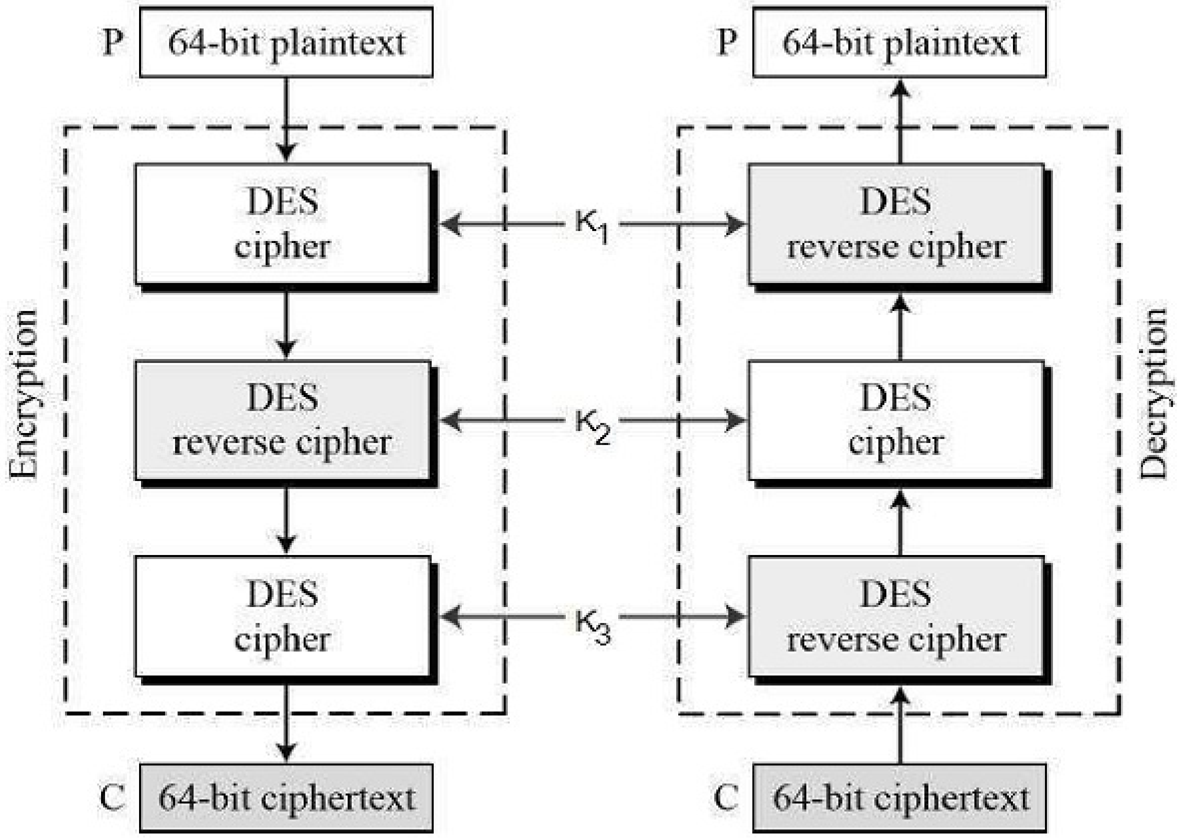
The speed of exhaustive key searches against DES after 1990 began to cause discomfort amongst users of DES. However, users did not want to replace DES as it takes an enormous amount of time and money to change encryption algorithms that are widely adopted and embedded in large security architectures.

The pragmatic approach was not to abandon the DES completely, but to change the manner in which DES is used. This led to the modified schemes of Triple DES (sometimes known as 3DES).

Incidentally, there are two variants of Triple DES known as 3-key Triple DES (3TDES) and 2-key Triple DES (2TDES).

3-KEY Triple DES

Before using 3TDES, user first generate and distribute a 3TDES key K, which consists of three different DES keys K1, K2 and K3. This means that the actual 3TDES key has length 3×56 = 168 bits. The encryption scheme is illustrated as follows −



Encryption Scheme

The encryption-decryption process is as follows −

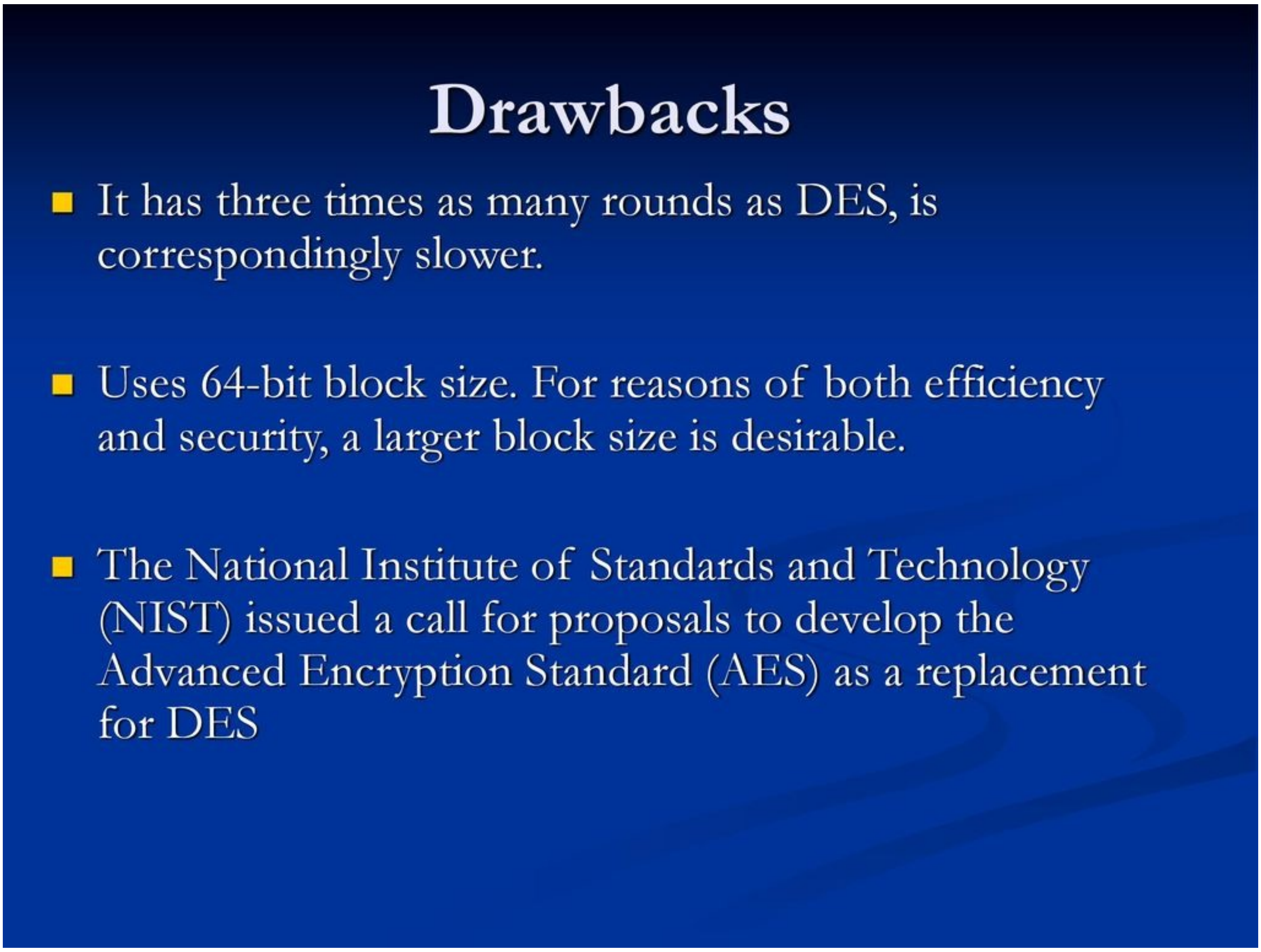
- Encrypt the plaintext blocks using single DES with key K1.
- Now decrypt the output of step 1 using single DES with key K2.
- Finally, encrypt the output of step 2 using single DES with key K3.
- The output of step 3 is the ciphertext.

- Decryption of a ciphertext is a reverse process. User first decrypt using K3, then encrypt with K2, and finally decrypt with K1.

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 K1, K2, and K3 to be the same value. This provides backwards compatibility with DES.

Second variant of Triple DES (2TDES) is identical to 3TDES except that K3is replaced by K1. In other words, user encrypt plaintext blocks with key K1, then decrypt with key K2, and finally encrypt with K1 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.



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

Benefits of using 3DES