

TRIPLE DES

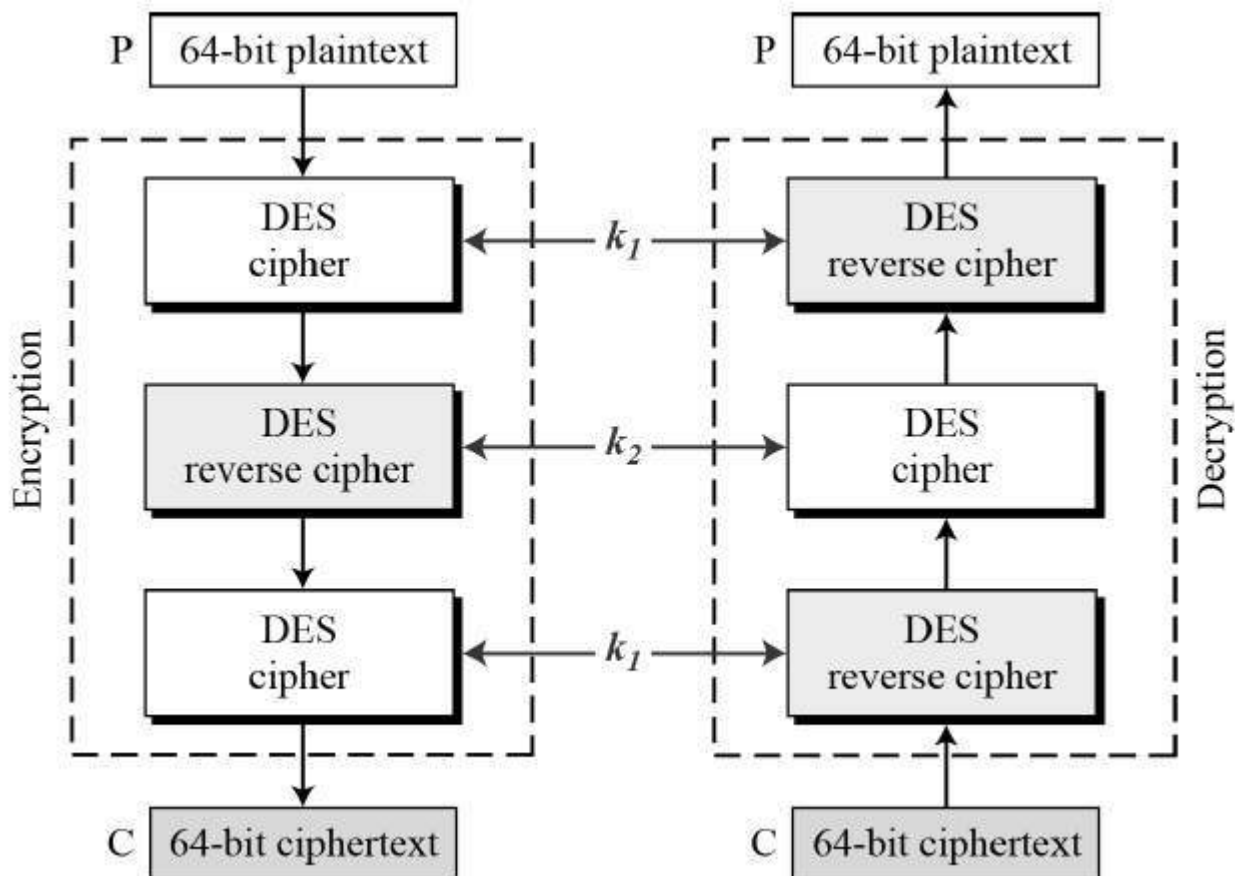
The speed of exhaustive key searches against DES after 1990 began to cause discomfort amongst users of DES. However, users did not want to replace DES as it takes an enormous amount of time and money to change encryption algorithms that are widely adopted and embedded in large security architectures.

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 K_1 , K_2 and K_3 . This means that the actual 3TDES key has length $3 \times 56 = 168$ bits. The encryption scheme is illustrated as follows –



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 .

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.

Loading [MathJax]/jax/output/HTML-CSS/jax.js