

Encryption Algorithm

3DES Introduction

- In cryptography, Triple DES (3DES), officially the Triple Data Encryption Algorithm (TDEA or Triple DEA), is a symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.
- The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm.

Algorithm

Triple DES uses a "key bundle" that comprises three DES keys, K1, K2 and K3, each of 56 bits (excluding parity bits). The 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.

Each triple encryption encrypts one block of 64 bits of data.

In each case the middle operation is the reverse of the first and last. This improves the strength of the algorithm when using keying option 2, and provides backward compatibility with DES with keying option 3.

Keying options

The standards define three keying options:

Keying option 1 All three keys are independent. Keying option 2 K1 and K2 are independent, and K3 = K1. Keying option 3 All three keys are identical, i.e. K1 = K2 = K3. Keying option 1 is the strongest, with $3 \times 56 = 168$ independent key bits.

Keying option 2 provides less security, with $2 \times 56 = 112$ key bits. This option is stronger than simply DES encrypting twice, e.g. with K1 and K2, because it protects against meet-in-the-middle attacks.

Keying option 3 is equivalent to DES, with only 56 key bits. It provides backward compatibility with DES, because the first and second DES operations cancel out. It is no longer recommended by the National Institute of Standards and Technology (NIST),[5] and is not supported by ISO/IEC 18033-3.

Each DES key is nominally stored or transmitted as 8 bytes, each of odd parity,[12] so a key bundle requires 24 bytes for option 1, 16 for option 2, or 8 for option 3.

Encryption example

Set pinKey: 9D93D15D6A3913AB4151C456A80841EF :

K1 = 9D93D15D6A3913AB
K2 = 4151C456A80841EF
K3 = 9D93D15D6A3913AB

Data M in HEX 3132333435363738 → encryption process →

DES1_RESULT = Ek(M ⊕ K1)
DES2_RESULT = Dk(DES1_RESULT ⊕ K2)
C = Ek(DES2_RESULT ⊕ K3)

Result C C63AABF759BDE968

Decryption example

Set pinKey: 9D93D15D6A3913AB4151C456A80841EF :

K1 = 9D93D15D6A3913AB
K2 = 4151C456A80841EF
K3 = 9D93D15D6A3913AB

Data C in HEX C63AABF759BDE968 → decryption process →

DES1_RESULT = Dk(C ⊕ K3)
DES2_RESULT = Ek(DES1_RESULT ⊕ K2)
M = Dk(DES2_RESULT ⊕ K1)

Results M 3132333435363738

Revision #1

Created 22 July 2021 16:21:18 by zhangkexin

Updated 22 July 2021 16:22:29 by zhangkexin