



3DES

- 3DES Triple DES Triple Data Encryption Algorithm DE



- $E_k()$ $D_k()$ DES K DES M C
- $3DES C = E_k3(D_k2(E_k1(M)))$
- $3DES M = D_k1(E_k2(D_k3(C)))$
- $K1 K2 K3$ $K1 K3$ ECB/NoPadding



pinKey[9D93D15D6A3913AB4151C456A80841EF]:

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

M[3132333435363738]

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

[C63AABF759BDE968]



pinKey[9D93D15D6A3913AB4151C456A80841EF]:

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

C[C63AABF759BDE968]

$DES1_RESULT = Dk(C \oplus K3)$

$DES2_RESULT = Ek(DES1_RESULT \oplus K2)$

$M = Dk(DES2_RESULT \oplus K1)$

☐ 3132333435363738

Revision #1

Created 22 July 2021 14:30:58 by zhangkexin

Updated 23 July 2021 10:52:09 by zhangkexin