3DES

3DES NIST approved until 2030 for sensitive gov data

$$C = E_{k_3}(D_{k_2}(E_{k_1}(m)))$$

3 keying options:

	key size	effective key size
• k_1, k_2, k_3 independent	$3 \cdot 56 = 168$ bit	112 bit
• $k_1 = k_3$	$2 \cdot 56 = 112$ bit	80 bit
• $k_1 = k_2 = k_3$ usual DES	56 bit	56 bit

meet-in-the-middle attack on 2DES
(+ reason for reduced effective key sizes in 3DES)

$$C = E_{k_2}(E_{k_1}(m)) \qquad k_1, k_2 \text{ 56 bit}$$

brute-force go through all pairs (k_1, k_2) ($2^{56} \cdot 2^{56} = 2^{112}$ many)
+ check if $C = E_{k_2}(E_{k_1}(m))$
$\rightsquigarrow 2 \cdot 2^{112} = 2^{113}$ DES op's

C, m more than 1 block

MITM $D_{k_2}(C) = E_{k_1}(m)$

① go through all k_2, compute $D_{k_2}(C)$
+ store in lookup table
$\rightsquigarrow 2^{56}$ DES op's

② go through all k_1, compute $E_{k_1}(m)$
+ see if stored in lookup table
$\rightsquigarrow 2^{56}$ DES op's

in total: $2^{56} + 2^{56} = 2^{57}$ DES op's

same as for brute-forcing DES

example of time-memory trade-off