How about 2DES ?

$$2DES_{k1,k2}(m) = E_{k2}(E_{k1}(m))$$

Meet-in-the-middle attack - known-plaintext attack

1. Brute force $E_{k1}(m)$ and save results in a table called TE (2^{56} entries)
2. Brute force $D_{k2}(c)$ and save results in a table called TD (2^{56} entries)
3. Match the two tables together to get the key candidates

➡ The more plaintext you know, the lesser key candidates

➡ Effective key-length (entropy) is **57 bits**

➡ This attacks applies to every encryption algorithm used as such

3DES (Triple DES)

$$3DES_{k1,k2,k3}(m) = E_{k3}(D_{k2}(E_{k1}(m)))$$

➡ Effective key length (entropy) : 112 bits

✓ Very popular, used in PGP, TLS (SSL) …

◉ But terribly slow