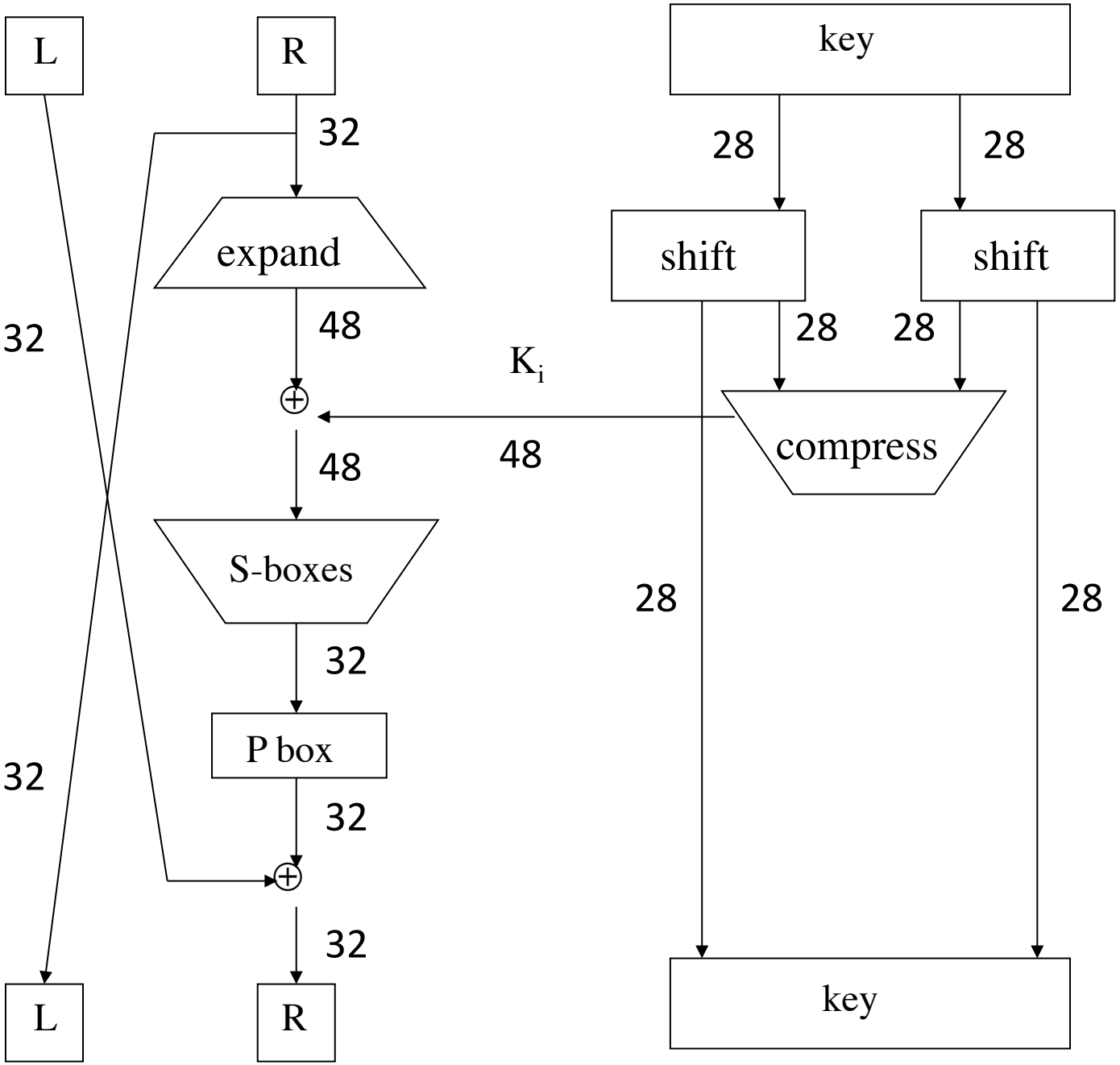
Triple DES

More on DES

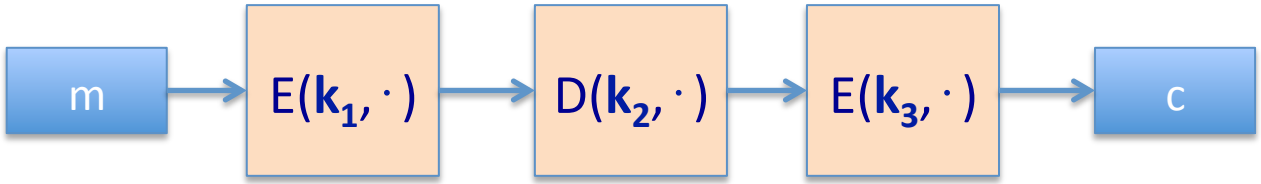
- DES Review
- Improve DES
  - 2DES
  - 3DES wrong
  - 3DES 3key
  - 3DES 2key



One Round of DES

Triple DES

- **Triple DES** or **3DES** with three keys
  - $C = E(D(E(P,K_1),K_2),K_3)$
  - $P = D(E(D(C,K_3),K_2),K_1)$



- Keying options
  - option 1: all different (strongest)
  - option 2: $K_1=K_3$ (most common)
  - option 3: $K_1=K_2=K_3$ (=DES)

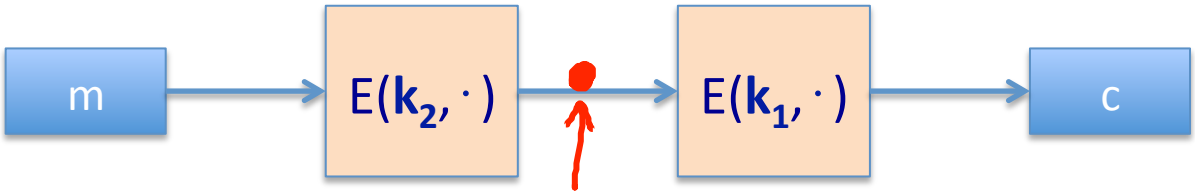
Triple DES

- Q1. Why not double DES (2DES)?
  - Meet In The Middle (MITM) Attack
  - takes 2^{63}
- Q2. Why not E→E→E instead E→D→E?
  - Backward Compatibility (3DES option 3 = DES)
- Q3. MITM against 3DES?
  - Possible, but takes 2^{118}

Why not double DES?

- Define $2E((k_1,k_2), m) = E(k_1, E(k_2, m))$

key-len = 112 bits for DES



Find (k_1, k_2) s.t. $E(k_1, E(k_2, M)) = C$

Equivalently: $E(k_2, M) = D(k_1, C)$

Attack: $M = (m_1, \ldots, m_{10})$, $C = (c_1, \ldots, c_{10})$

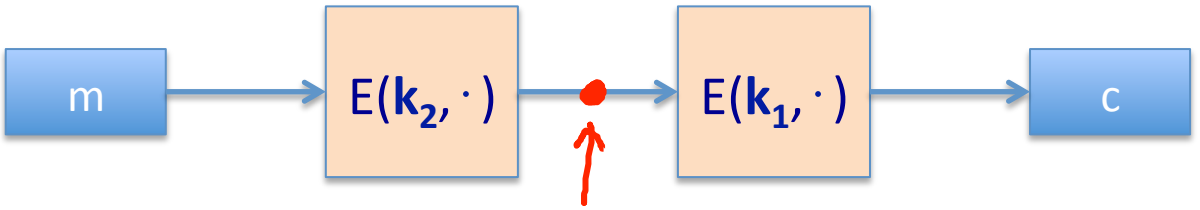
- step 1: build table.

  sort on 2nd column

$k^0 = 00\ldots00$	$E(k^0, M)$
$k^1 = 00\ldots01$	$E(k^1, M)$
$k^2 = 00\ldots10$	$E(k^2, M)$
⋮	⋮
$k^N = 11\ldots11$	$E(k^N, M)$

2^{56} entries

Meet in the middle attack



Attack: $M = (m_1, \ldots, m_{10})$, $C = (c_1, \ldots$

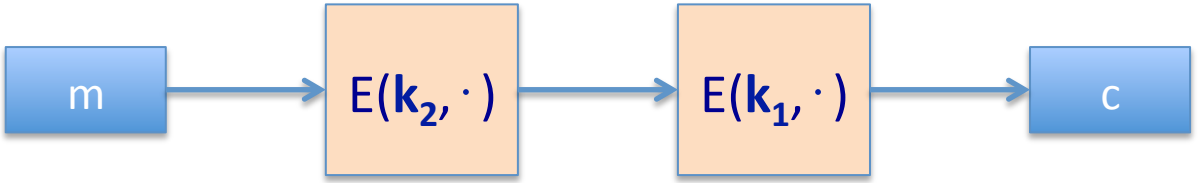
$k^0 = 00\ldots00$	$E(k^0, M)$
$k^1 = 00\ldots01$	$E(k^1, M)$
$k^2 = 00\ldots10$	$E(k^2, M)$
⋮	⋮
$k^N = 11\ldots11$	$E(k^N, M)$

- step 1: build table.
- Step 2: for all $k \in \{0,1\}^{56}$ do:

  test if $D(k, C)$ is in 2^{nd} column.

if so then $E(k^i, M) = D(k, C) \Rightarrow (k^i, k) = (k_2, k_1)$

Meet in the middle attack



Time = $2^{56}\log(2^{56}) + 2^{56}\log(2^{56}) < 2^{63} << 2^{112}$,
space $\approx 2^{56}$

Same attack on 3DES: Time = 2^{118} , space $\approx 2^{56}$