DES

block cipher design

1974: proposed by IBM with input from NSA
- no public crypto before
- reasons for design decisions secret

1976 - 2000: US standard
- 1997: successful brute-force attack
- 2000: replaced with AES
- 3DES still considered secure

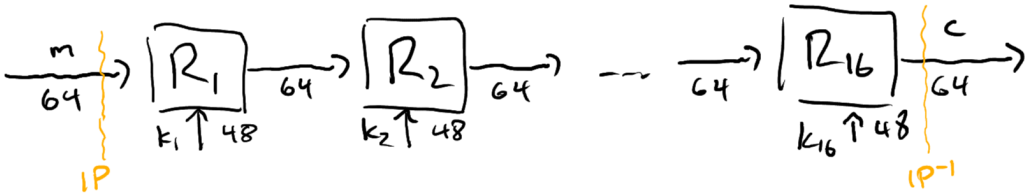
64 bit block ciphers with 56 bit key size

block cipher design

Shannon's guiding principles:

- **confusion**
  S-box
  relationship $k \leftrightarrow c$ obscured + nonlinear
  in particular: each bit in k should change c completely
- **diffusion**
  E-box, P-box
  dissipate structure of m over c
  in particular: each bit in m should change c completely

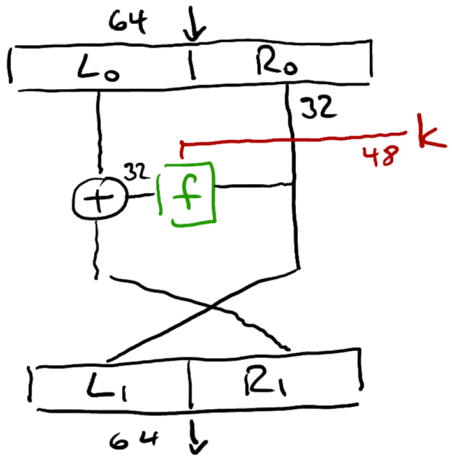
several rounds



DES: 16 identical rounds with round keys $k_1, \dots, k_{16}$

AES: 10/12/14 rounds

the rounds



Feistel network

$$L_1 = R_0$$
$$R_1 = L_0 \oplus f_k(R_0)$$

round function (any works!)

to decrypt:

$$L_0 = R_1 \oplus f_k(R_0)$$
$$R_0 = L_1$$

(R_0 = L_1)