Introduction to Cryptography CS 355

Lecture 14

Block Ciphers: DES

Announcements

- No class on Monday Sept 26
  - Class cancelled due to evening exam for midterm
- On Wednesday Sept 28, Prof. Sam Wagstaff will teach AES

Review: Stream Ciphers

- Idea: replace “rand” by “pseudo rand”
  - Use Pseudo Random Number Generator
  - Secret key is the seed
  - $\mathbf{E}_{seed}[M] = M \oplus \text{PRNG(seed)}$
  - $\mathbf{D}_{seed}[C] = C \oplus \text{PRNG(seed)}$
  - PRNG: $\{0,1\}^s \rightarrow \{0,1\}^n$
    - expand a short random seed into a long bit string that “looks random”
  - Don’t reuse the same stream

Review: Example Stream Ciphers

- RC4 (widely used)
  - Internal state: a 256-byte array, containing permutation of 0..255
  - Usage: drop the first 256 bytes of output
- LFSR:
  - vulnerable to known-plaintext attack
  - a m-stage LFSR can be completely broken given 2m bits outputs

Lecture Outline

- Block ciphers.
- DES

Block Ciphers

- A n-bit plaintext is encrypted to a n-bit ciphertext
  - P : $\{0,1\}^n$
  - C : $\{0,1\}^n$
  - K : $\{0,1\}^s$
  - **E**: $K \times P \rightarrow C$: E_k: a permutation on $\{0,1\}^n$
  - **D**: $K \times C \rightarrow P$: D_k is E_k^{-1}
  - Block size: n
  - Key size: s

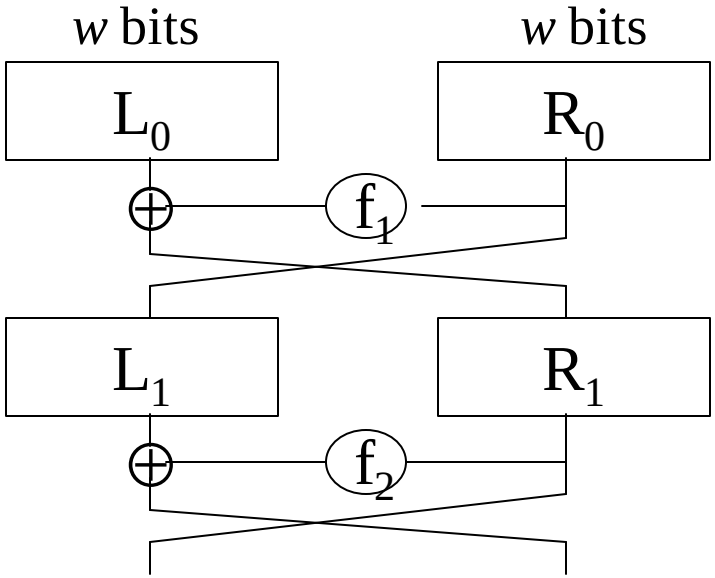
An Insecure Block Cipher

- Use linear equations
  - each output bit is a linear combination of the input bits
  - the key *k* is a matrix
    - $C = k\,M$
    - $M = k^{-1}\,C$
  - known as the Hill cipher
  - easily breakable by known-plaintext attack

Feistel Network

- A Feistel Network is fully specified given
  - the block size: n = 2w
  - number of rounds: d
  - d round functions $f_1, \ldots, f_d: \{0,1\}^w \rightarrow \{0,1\}^w$
- Used in DES, IDEA, RC5, and many other block ciphers.
- Not used in AES

Feistel Network



Encryption:

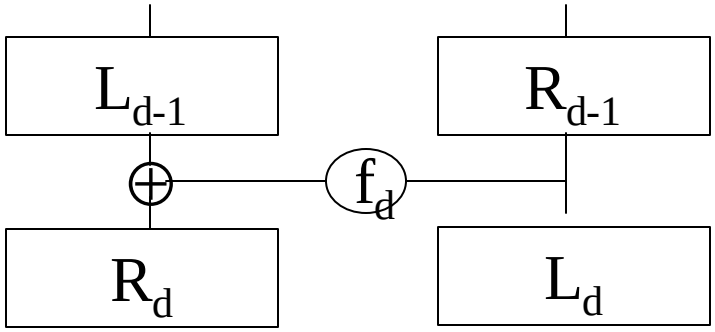
$L_1=R_0 \qquad R_1=L_0 \oplus f_1(R_0)$

$L_2=R_1 \qquad R_2=L_1 \oplus f_2(R_1)$

…

$L_d=R_{d-1} \qquad R_d=L_{d-1} \oplus f_d(R_{d-1})$

Decryption:



$R_{d-1}=L_d \qquad L_{d-1}=R_d \oplus f_d(L_d)$

…

$R_0=L_1; \qquad L_0=R_1 \oplus f_1(L_1)$

Property of Feistel Network

- Always invertible no matter what the round function is.

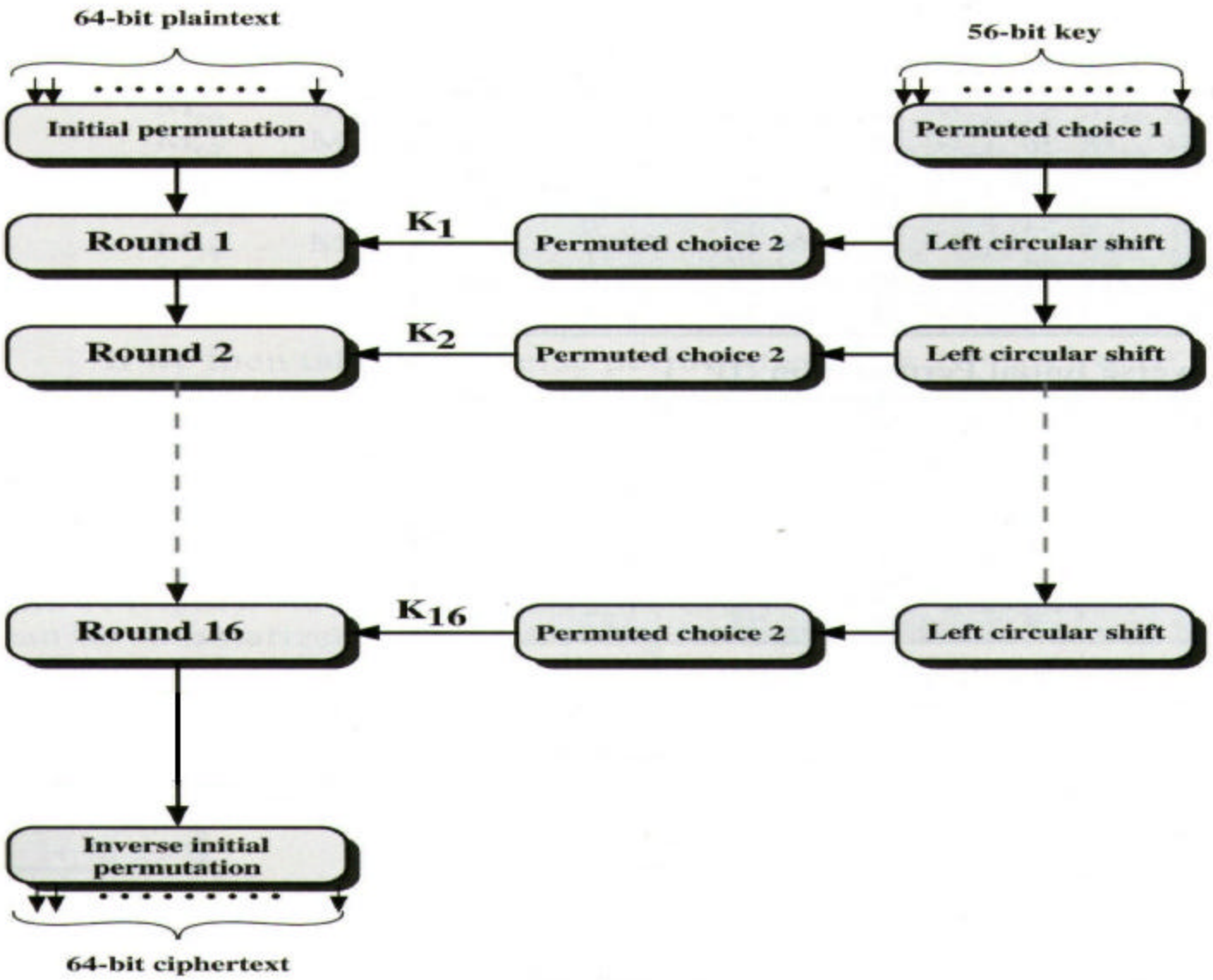
History of Data Encryption Standard (DES)

- 1967: Feistel at IBM
  - Lucifer: block size 128; key size 128 bit
- 1972: NBS asks for an encryption standard
- 1975: IBM developed DES (modification of Lucifer)
  - block size 64 bits; key size 56 bits
- 1975: NSA suggests modification
- 1977: NBS adopts DES as encryption standard in (FIPS 46-1, 46-2).
- 2001: NIST adopts Rijndael as replacement to DES.

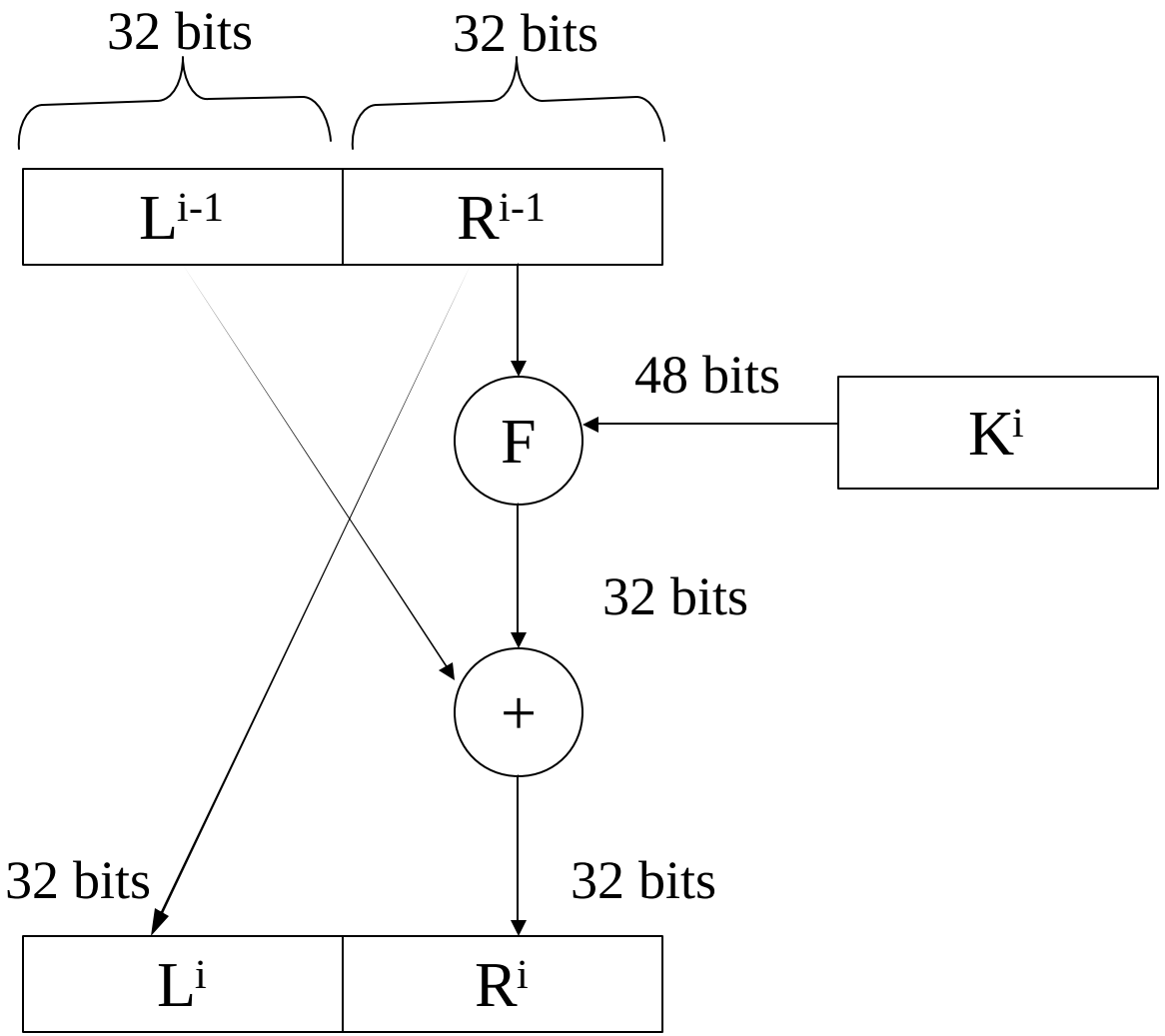
DES

- 16-round Feistel network with an initial permutation at the beginning and a reverse permutation at the end

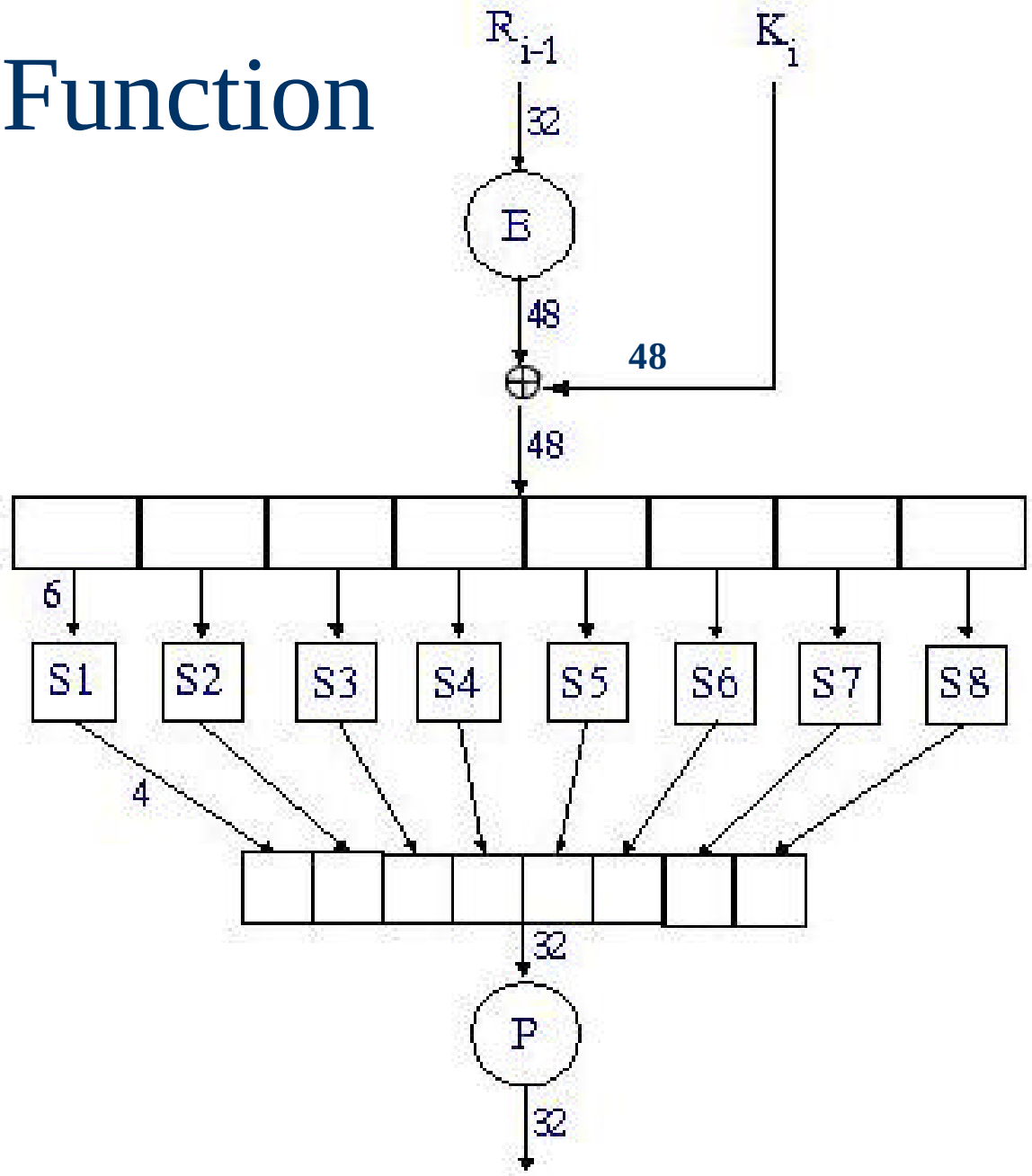
DES Rounds


64-bit plaintext
56-bit key
Initial permutation
Permuted choice 1
Round 1
K1
Permuted choice 2
Left circular shift
Round 2
K2
Permuted choice 2
Left circular shift
Round 16
K16
Permuted choice 2
Left circular shift
Inverse initial permutation
64-bit ciphertext

DES Round i



Round Function



About the S-boxes …

Example: S_1

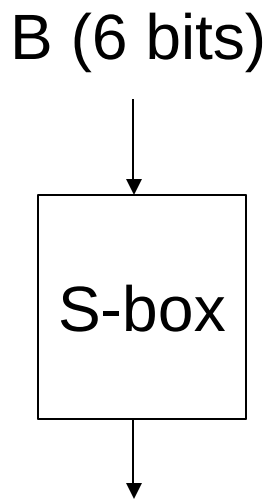
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S(i, j) <16, can be represented with 4 bits

- Some of the design features of s-boxes were made public only recently.

S-boxes

- S-boxes are the only non-linear elements in DES design



$B = b_1 b_2 b_3 b_4 b_5 b_6$

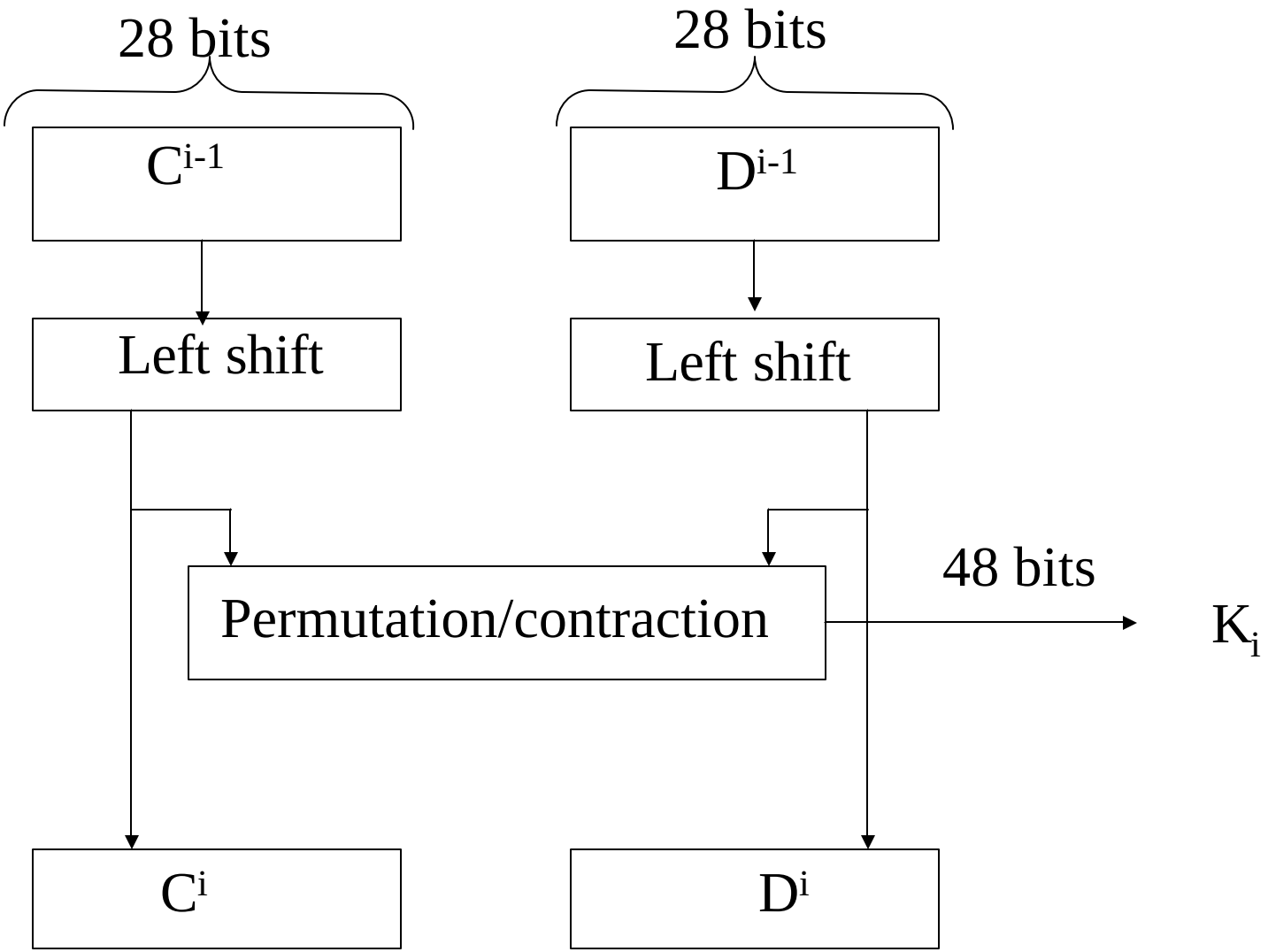
$b_1 b_6$ = r = row c = column

S = matrix 4 x 16, values from 0 to 15

C = Binary representation of S(r,c)

8 S-boxes

DES Key Scheduling



Coming Attractions …

- AES

- Recommended reading for next lecture:
  - Trappe & Washington: Chapter 5