Course Business

- Homework 2 Due <u>Now</u>
- Midterm is on <u>March 1</u>
- Final Exam is <u>Monday, May 1 (7 PM)</u>
  - <u>Location: Right here</u>

Cryptography
CS 555

Topic 17: DES, 3DES

Recap

Goals for This Week:

- Practical Constructions of Symmetric Key Primitives

Last Class: Block Ciphers

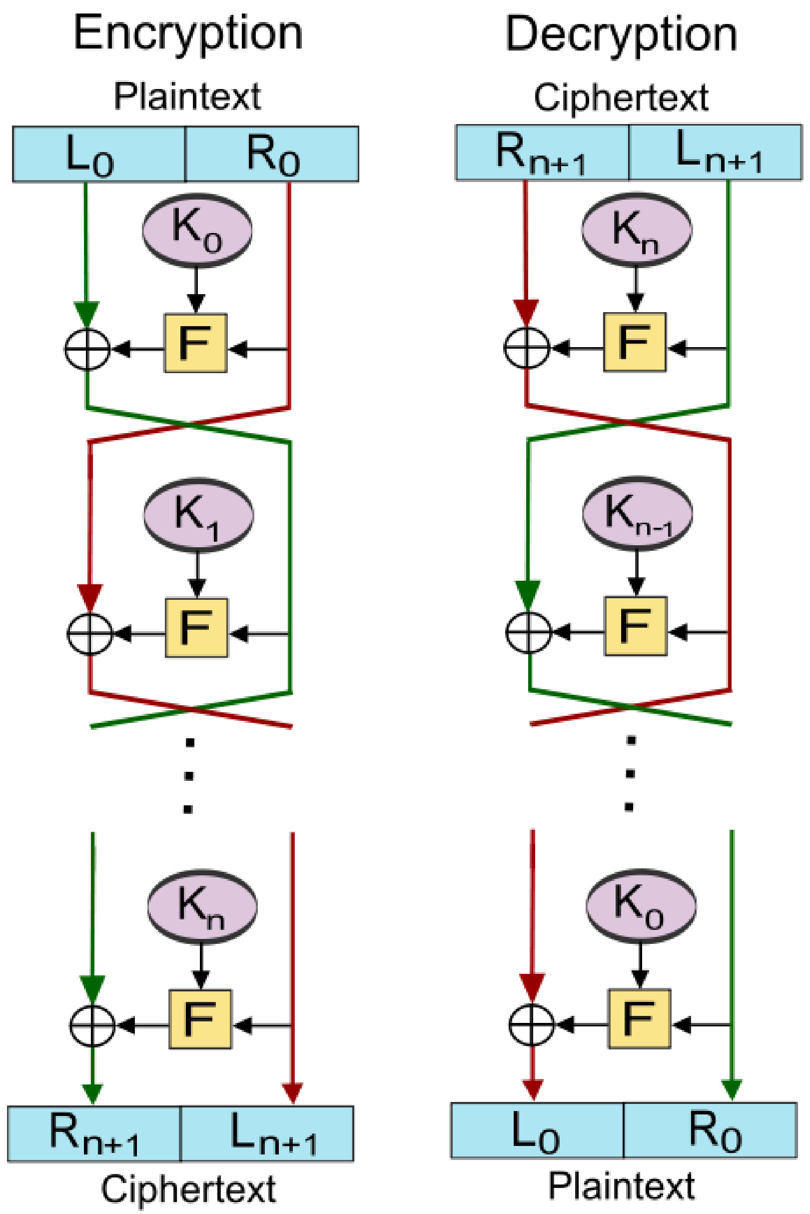
Today's Goals: DES/3DES

- Data Encryption Standard

Feistel Networks

- Alternative to Substitution Permutation Networks

- **Advantage**: underlying functions need not be invertible, but the result is still a permutation



- $L_{i+1} = R_i$
- $R_{i+1} := L_i \oplus F_{k_i}(R_i)$

Proposition: the function is invertible.

Data Encryption Standard

- Developed in 1970s by IBM (with help from NSA)
- Adopted in 1977 as Federal Information Processing Standard (US)
- Data Encryption Standard (DES): 16-round Feistel Network.
- Key Length: 56 bits
  - Vulnerable to brute-force attacks in modern times
  - 1.5 hours at 14 trillion keys/second (e.g., Antminer S9)

DES Round

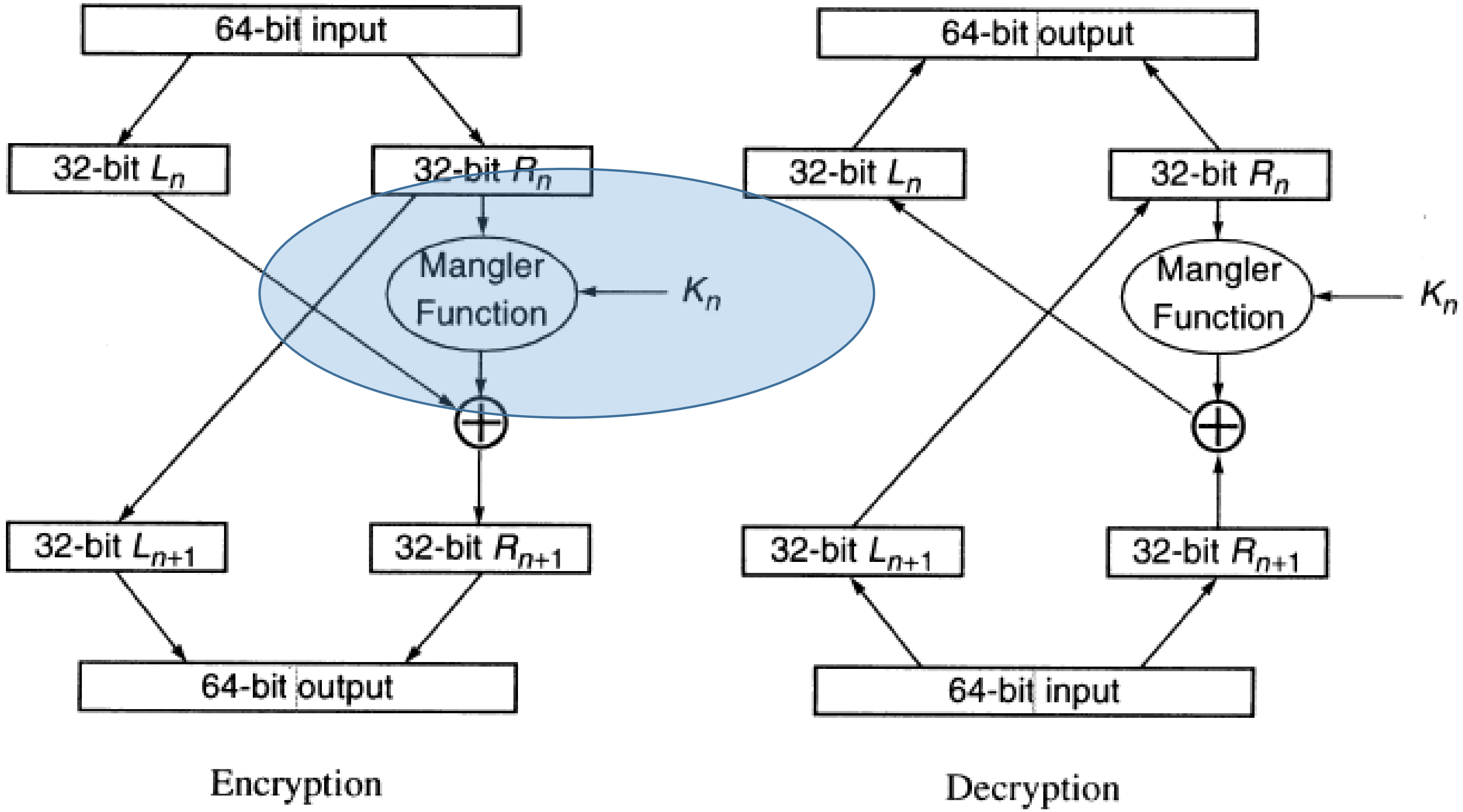
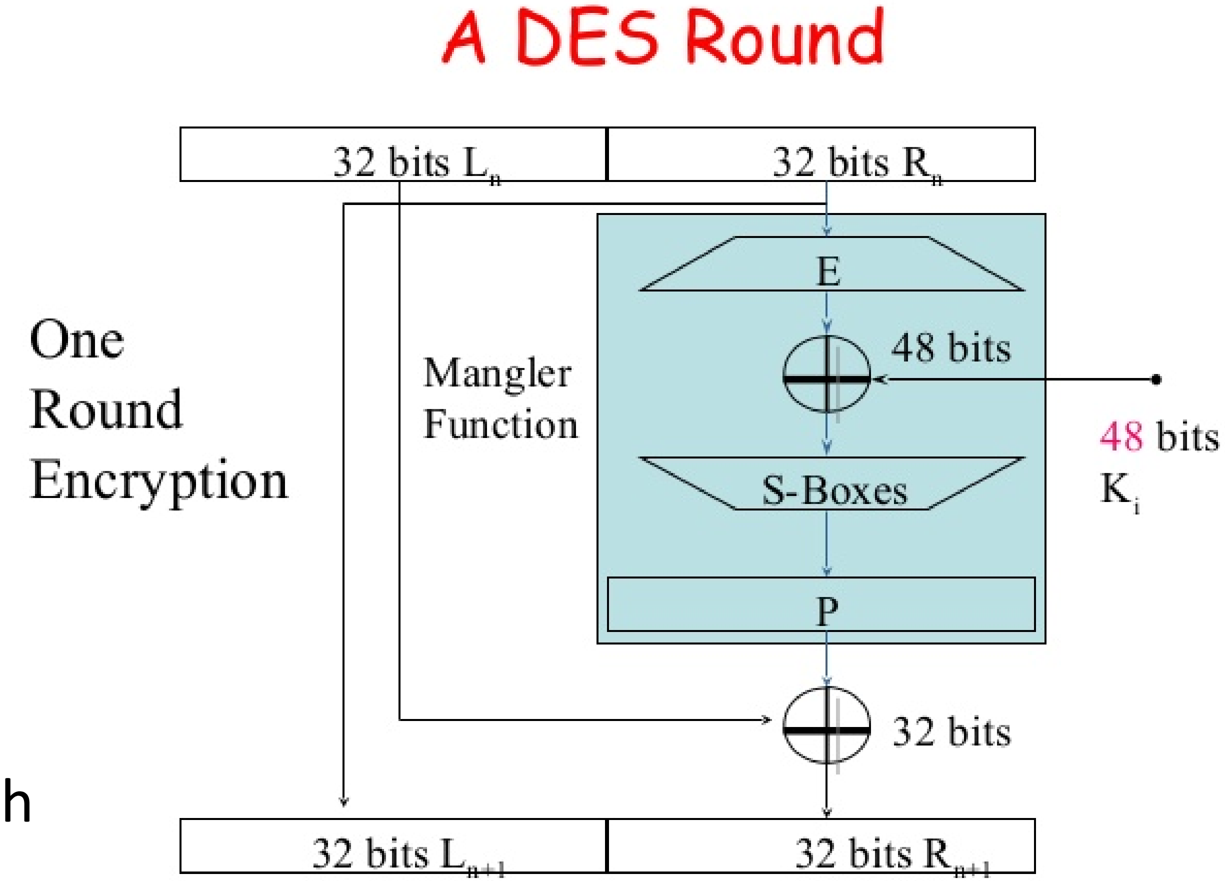


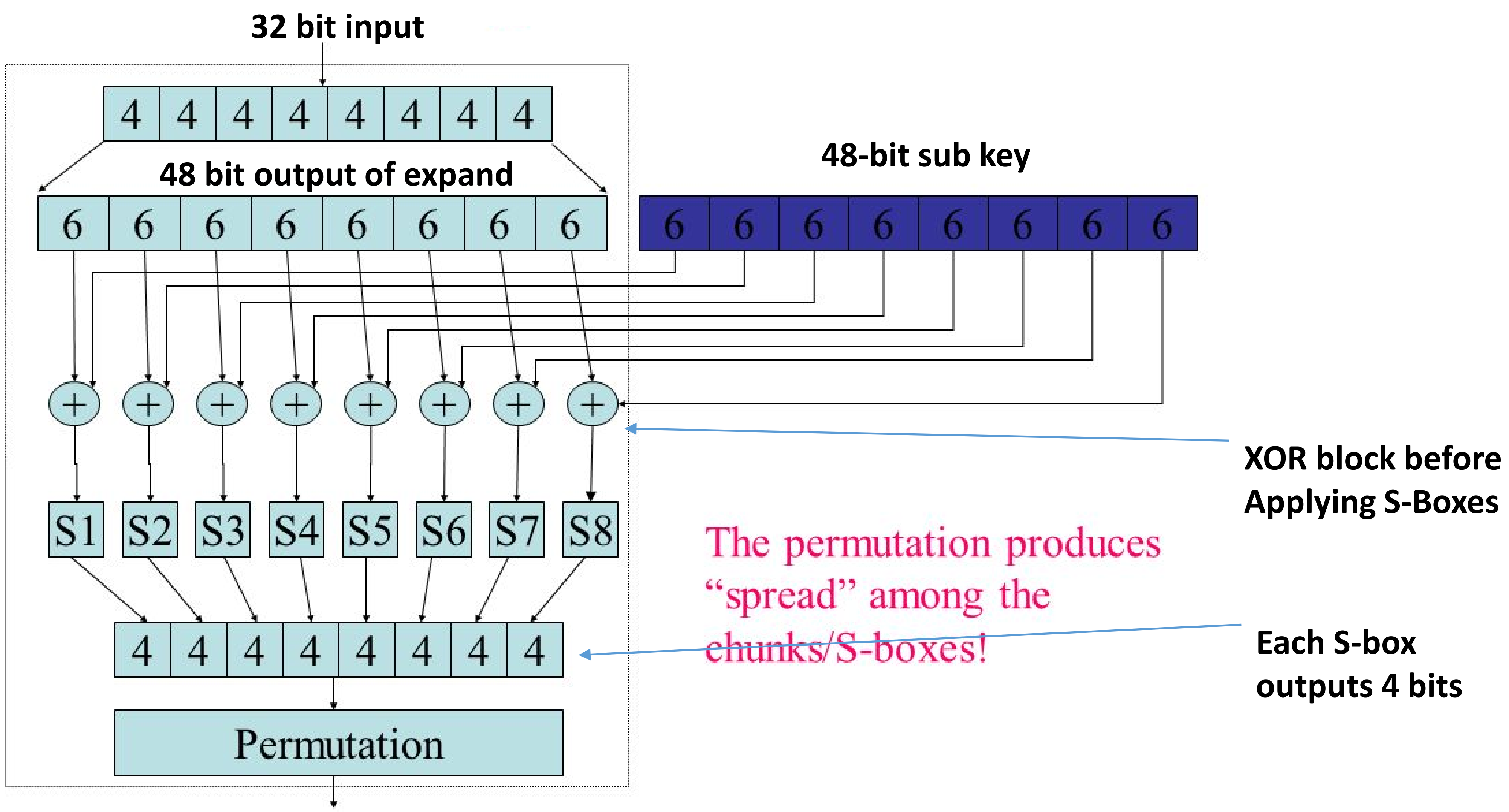
Figure 3-6. DES Round

DES Mangle Function

- Expand E: 32-bit input → 48-bit output (duplicates 16 bits)
- S-boxes: $S_1,\ldots,S_8$
  - Input: 6-bits
  - Output: 4 bits
  - Not a permutation!
- 4-to-1 function
  - Exactly four inputs mapped to each possible output



Mangle Function



S-Box Representation as Table

4 columns (2 bits)

16 columns (4 bits)

	00	01	10	11
0000				
0001				
0010				
0011				
0100				
0101				
0110				S(x)=1101
….	….	….	….	….
1111				

x =101101 S(x) = Table[0110,11]

S-Box Representation

Each column is permutation

4 columns (2 bits)

16 columns (4 bits)

	00	01	10	11
0000				
0001				
0010				
0011				
0100				
0101				
0110				S(x)=1101
….	….	….	….	….
1111				

x =101101

S(x) = T[0110,11]

Pseudorandom Permutation Requirements

- Consider a truly random permutation $\mathrm{F} \in \mathbf{Perm}_{\mathbf{128}}$
- Let inputs x and x’ differ on a single bit
- We expect outputs F(x) and F(x’) to differ on approximately half of their bits
  - F(x) and F(x’) should be (essentially) independent.
- A pseudorandom permutation must exhibit the same behavior!
- **Requirement**: DES Avalanche Effect!

DES Avalanche Effect

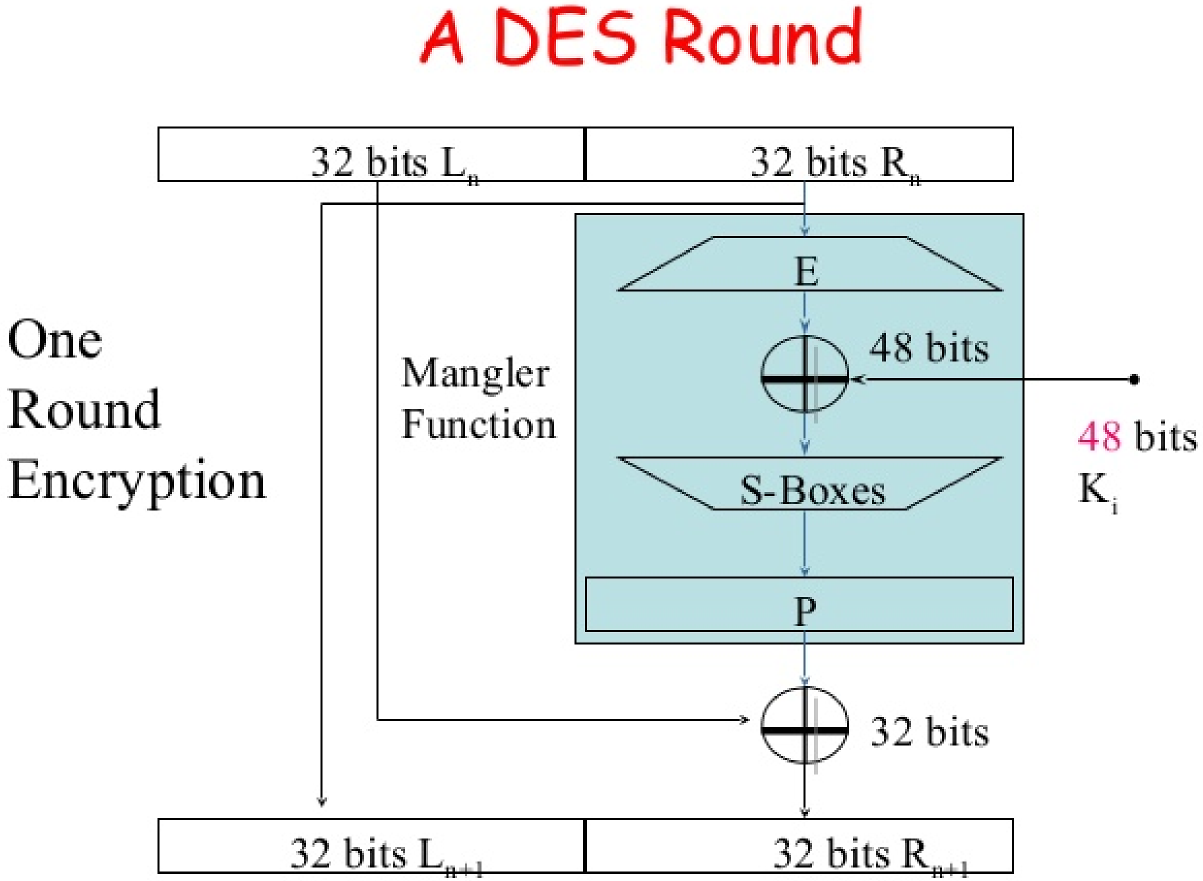
- Permutation the end of the mangle function helps to mix bits

- Special S-box property #1

Let x and x’ differ on one bit then $S_i(x)$ differs from $S_i(x')$ on two bits.

Avalanche Effect Example

- Consider two 64 bit inputs
  - (L_n,R_n) and $(L_n',R'_n=R_n)$
  - L_n and L_n' differ on one bit
- This is worst case example
  - $L_{n+1} = L_{n+1}'=R_n$
  - But now R'_{n+1} and R_{n+1} differ on one bit
- Even if we are unlucky $E(R'_{n+1})$ and $E(R_{n+1})$ differ on 1 bit
- → R_{n+2} and R'_{n+2} differ on two bits
- → $L_{n+2} = R'_{n+1}$ and $L_{n+2}' = R'_{n+1}$ differ in one bit



Avalanche Effect Example

- R_{n+2} and R'_{n+2} differ on two bits
- $L_{n+2} = R_{n+1}$ and $L_{n+2}' = R'_{n+1}$ differ in one bit

→R_{n+3} and R'_{n+3} differ on four bits since we have different inputs to two of the S-boxes

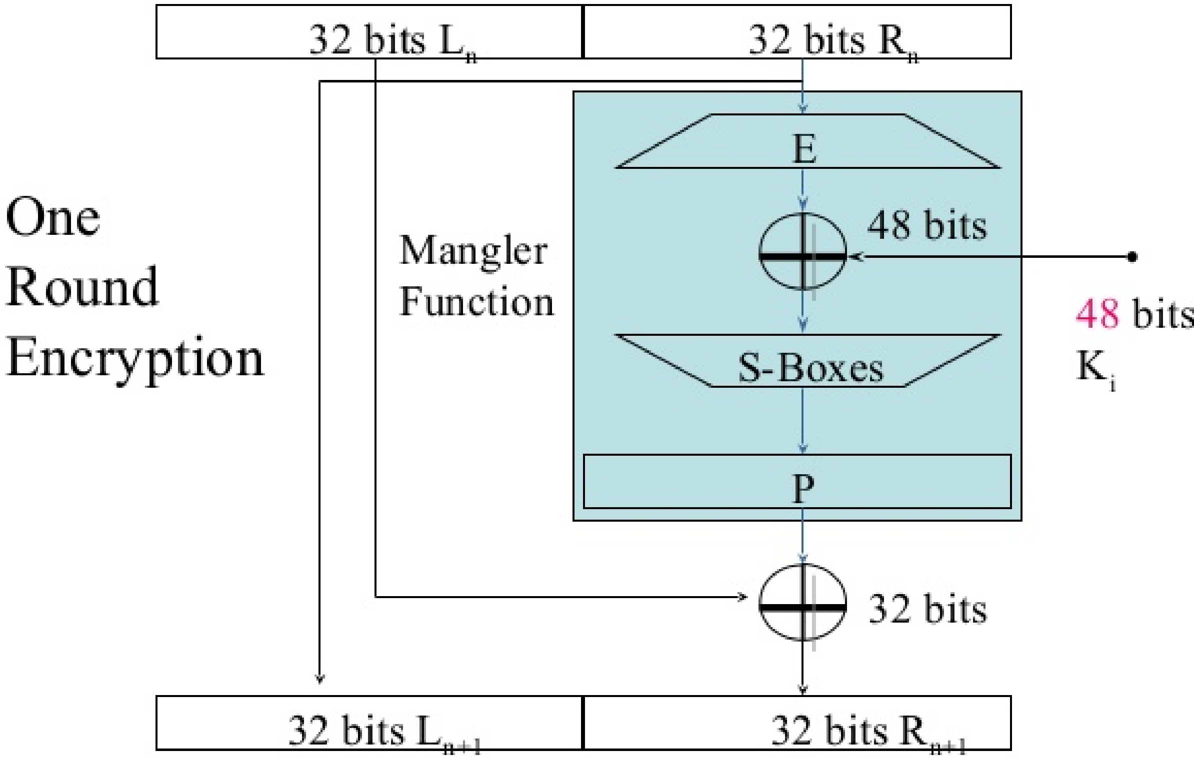
→$L_{n+3} = R'_{n+2}$ and $L_{n+2}' = R'_{n+2}$ now differ on two bits

- Seven rounds we expect all 32 bits in right half to be “affected” by input change

…

DES has sixteen rounds

A DES Round



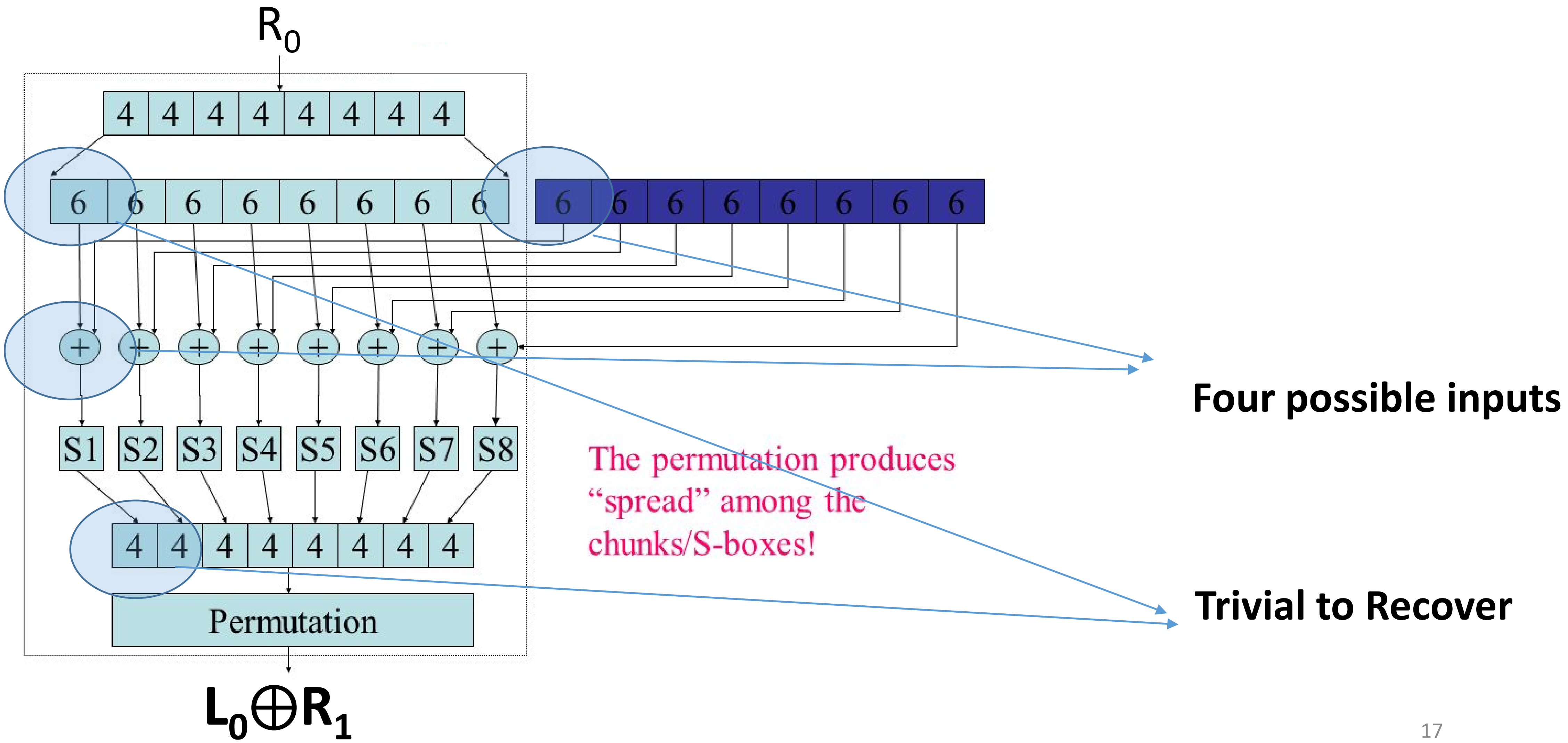
Attack on One-Round DES

- Given input output pair (x,y)
  - y=(L_1,R_1)
  - X=(L_0,R_0)
- Note: $R_0=L_1$
- Note: $R_1=L_0 \oplus f_1(R_0)$ where f is the Mangling Function with key k_1

Conclusion:

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

Attack on One-Round DES



Attack on Two-Round DES

- Output y =(L_2,R_2)
- Note: R_1=$L_0 \oplus f_1(R_0)$
  - Also,R_1= L_2
  - Thus, $f_1(R_0)$=$L_2 \oplus L_0$
- So we can still attack the first round key k1 as before as R_0 and $L_2 \oplus L_0$ are known
- Note:R_2=$L_1 \oplus f_2(R_1)$
  - Also,L_1=R_0 and R_1= L_2
  - Thus, $f_2(L_2)$=$R_2 \oplus R_0$
- So we can attack the second round key k2 as before as L_2 and $R_2 \oplus R_0$ are known

Attack on Three-Round DES

$$f_1(\mathbf{R_0}) \oplus f_3(\mathbf{R_2}) = (\mathrm{L}_0 \oplus \mathrm{L}_2) \oplus (\mathrm{L}_2 \oplus \mathrm{R}_3)$$
$$= \mathrm{L}_0 \oplus \mathrm{R}_3$$

We **know all of the values** L_0,R_0, R_3 and $L_3 = R_2$.

Leads to attack in time $\approx 2^{n/2}$

(See details in textbook)

Remember that DES is 16 rounds

DES Security

- Best Known attack is brute-force 2^{56}
  - Except under unrealistic conditions (e.g., 2^{43} known plaintexts)
- Brute force is not too difficult on modern hardware
- Attack can be accelerated further after precomputation
  - Output is a few terabytes
  - Subsequently keys are cracked in 2^{38} DES evaluations (minutes)
- Precomputation costs amortize over number of DES keys cracked
- Even in 1970 there were objections to the short key length for DES

Double DES

- Let $F_k(x)$ denote the DES block cipher

- A new block cipher F' with a key $k = (k_1, k_2)$ of length 2n can be defined by

$$F'_k(x) = F_{k_2}\left(F_{k_1}(x)\right)$$

- Can you think of an attack better than brute-force?

Meet in the Middle Attack

$$F'_k(x) = F_{k_2}\left(F_{k_1}(x)\right)$$

Goal: Given (x, $F'_k(x)$) try to find secret key k in time and space $O(n2^n)$.

- **Solution?**

See Homework 1 ☺

Triple DES Variant 1

- Let $F_k(x)$ denote the DES block cipher

- A new block cipher F' with a key $k = (k_1, k_2, k_3\,)$ of length 2n can be defined by

$$F'_k(x) = F_{k_3}\left(F_{k_2}^{-1}\left(F_{k_1}(x)\right)\right)$$

- Meet-in-the-Middle Attack Requires time $\Omega(2^{2n})$ and space $\Omega(2^{2n})$

Triple DES Variant 1

Allows backward compatibility with DES by setting k_1=k_2=k_3

- Let $F_k(x)$ denote the DES block cipher

- A new block cipher F' with a key $k = (k_1, k_2, k_3)$ of length 2n can be defined by

$$F'_k(x) = F_{k_3}\left(F^{-1}_{k_2}\left(F_{k_1}(x)\right)\right)$$

- Meet-in-the-Middle Attack Requires time $\Omega(2^{2n})$ and space $\Omega(2^{2n})$

Triple DES Variant 2

Just two keys!

- Let $F_k(x)$ denote the DES block cipher

- A new block cipher F' with a key $k = (k_1, k_2)$ of length 2n can be defined by

$$F'_k(x) = F_{k_1}\left(F_{k_2}^{-1}\left(F_{k_1}(x)\right)\right)$$

- Meet-in-the-Middle Attack still requires time $\Omega(2^{2n})$ and space $\Omega(2^{2n})$

- Key length is still just 112 bits (128 bits is recommended)

Triple DES Variant 1

$$F'_k(x) = F_{k_3}\left(F_{k_2}^{-1}\left(F_{k_1}(x)\right)\right)$$

- Standardized in 1999
- Still widely used, but it is relatively slow (three block cipher operations)
- Current gold standard: AES

Next Class

- Read Katz and Lindell 6.2.5-6.3
- AES & Differential Cryptanalysis + Hash Functions