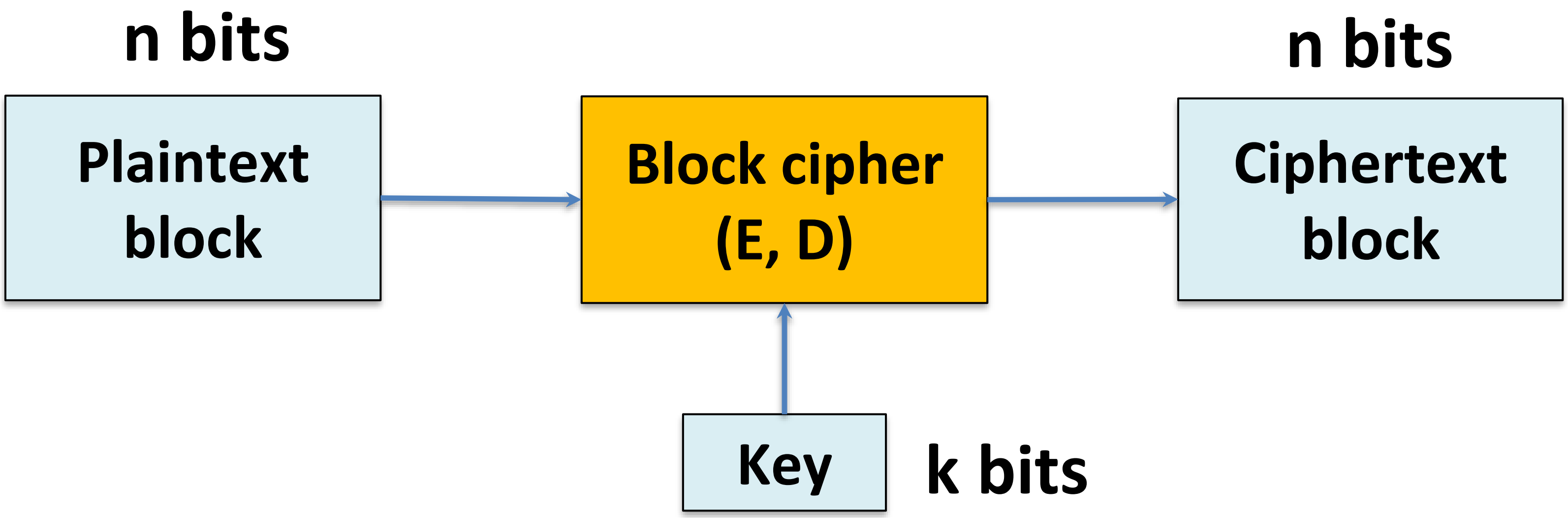
CS915/435 Advanced Computer Security - Elementary Cryptography

Block Cipher I

Roadmap

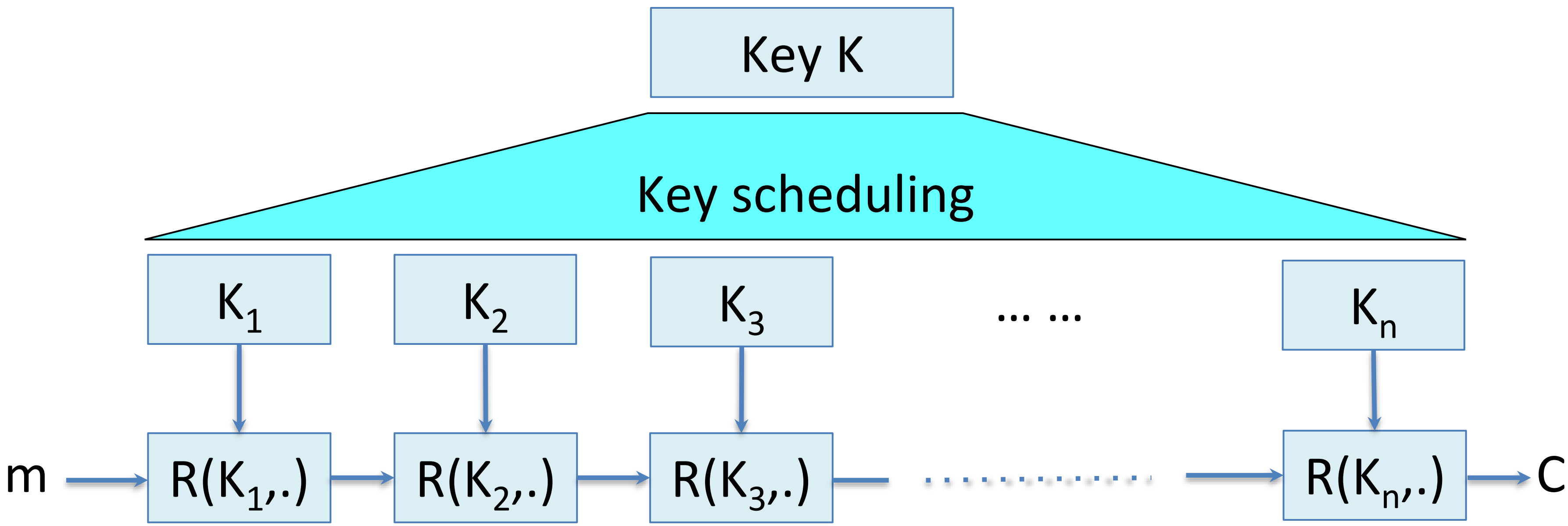
- Symmetric cryptography
  - Classical cryptographic
  - Stream cipher
  - **Block cipher I**, II
  - Hash
  - MAC
- Asymmetric cryptography
  - Key agreement
  - Public key encryption
  - Digital signature

Block cipher: overview



- Canonical examples:
  - DES: n=64 bits k=56 bits
  - 3DES: n=64 bits k=168 bits
  - AES: n=128 bits k=128, 192, 256 bits

Iterated construction



- R(K,.) is called a round function
- DES 16 rounds, 3DES 48 round, AES-128 10 rounds

Performance

- AMD Opteron, 2,2 GHz, Linux, Crypto++ 5.6.0 (Wei Dai)

	Cipher	Block/key size	Speed (MB/sec)
stream	RC4		126
	Salsa20/12		643
	Sosemanuk		727
block	3DES	64/168	13
	AES-128	128/128	109

Abstractly: PRF and PRP

- Pseudo Random Function (PRF) defined over (K, X, Y)

$$F: K \times X \to Y$$

Such that:

1. Exists "efficient" algorithm to evaluate $\mathrm{F}(\mathrm{k}, \mathrm{x})$

- Pseudo Random Permutation (PRP) defined over (K, X)

$$E: K \times X \to X$$

Such that:

1. Exists "efficient" deterministic algorithm to evaluate $\mathrm{E}(\mathrm{k}, \mathrm{x})$
2. The function $\mathrm{E}(\mathrm{k}, .\,)$ is one-to-one
3. Exists "efficient" inversion algorithm $\mathrm{D}(\mathrm{k}, .\,)$

Running example

- Example PRPs: 3DES, AES, …

  AES: $K \times X \rightarrow X$ where $K = X = \{0,1\}^{128}$

  3DES: $K \times X \rightarrow X$ where $X = \{0,1\}^{64}$, $K = \{0,1\}^{168}$

- A PRP is a PRF where

  1) $X = Y$

  2) It is invertible

Data Encryption Standard

- Early 1970s: Horst Feistel designed Lucifer at IBM
- 1973: NBS asked for block cipher proposals
  - IBM submitted a variant of Lucifer (128-bit key and 128-bit block size)
- 1977: NBS adopted DES as a federal standard
  - But reduced key to 56 bits and block size to 64 bits
- 1997: DES broken by exhaustive search
  - 56-bit key is too small
- 2000: NIST adopted AES to replace DES

Historical importance of DES (I)

- Before 1970s, crypto was a *forbidden* science
  - Almost no research papers published
  - National Security Agency had considerable knowledge crypto, but they didn't admit existence
  - But financial transactions must be protected
  - A secure encryption standard was badly needed.

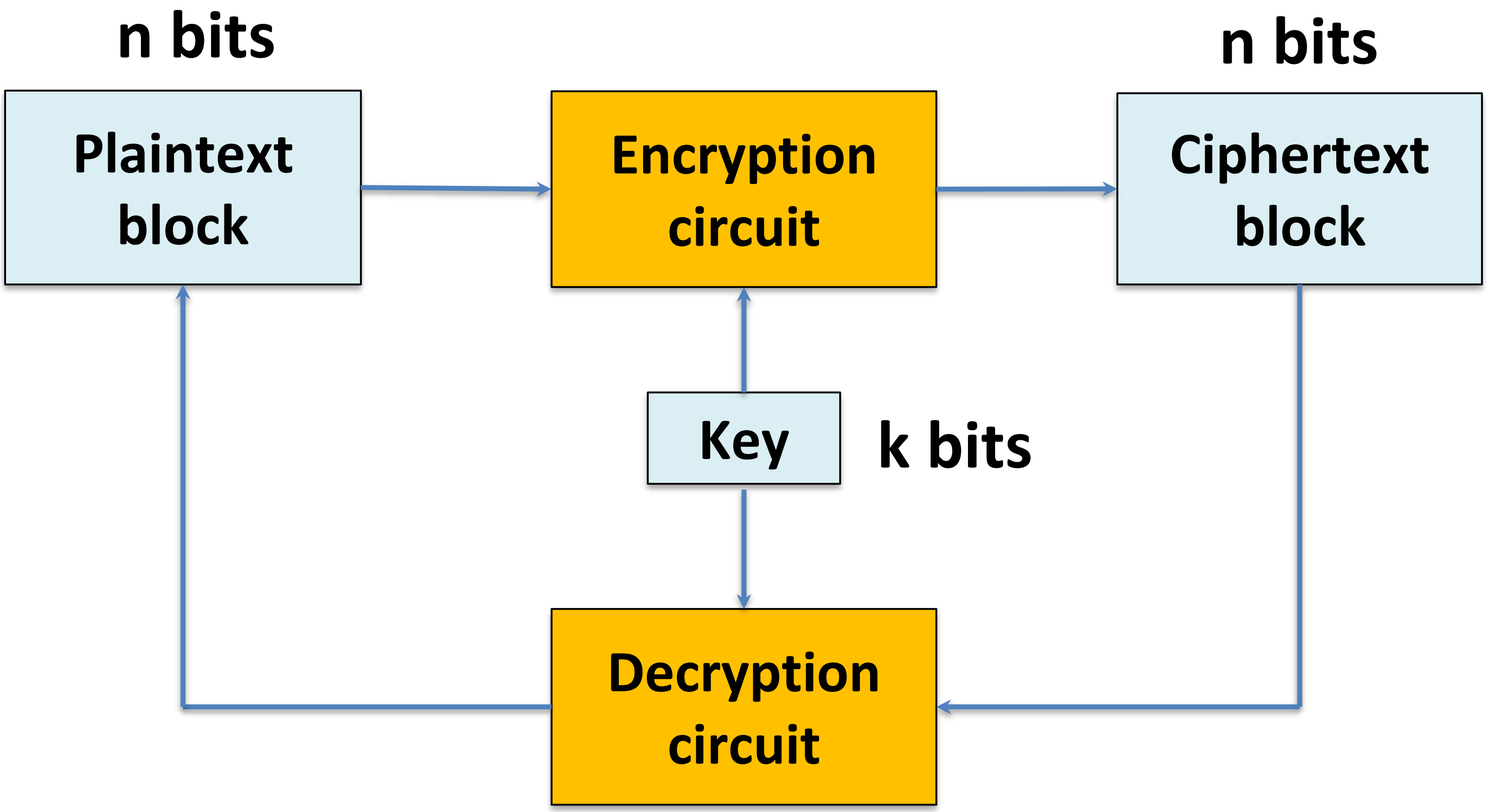
Historical importance of DES (II)

- In 1972, National Bureau of Standards (NBS) initiated to develop a standard cipher
  - Must provide a high level of security
  - Must be completely specified and easy to understand
  - The security must reside in the key not the algorithm
  - Must be available to all users.
  - Must be adaptable for use in diverse applications
  - Must be economically implementable in electronic devices
  - Must be efficient to use
  - Must be able to be validated
  - Must be exportable
- Public interest was high, but public expertise was lacking
- None of the submissions came close to the requirements

Historical importance of DES (III)

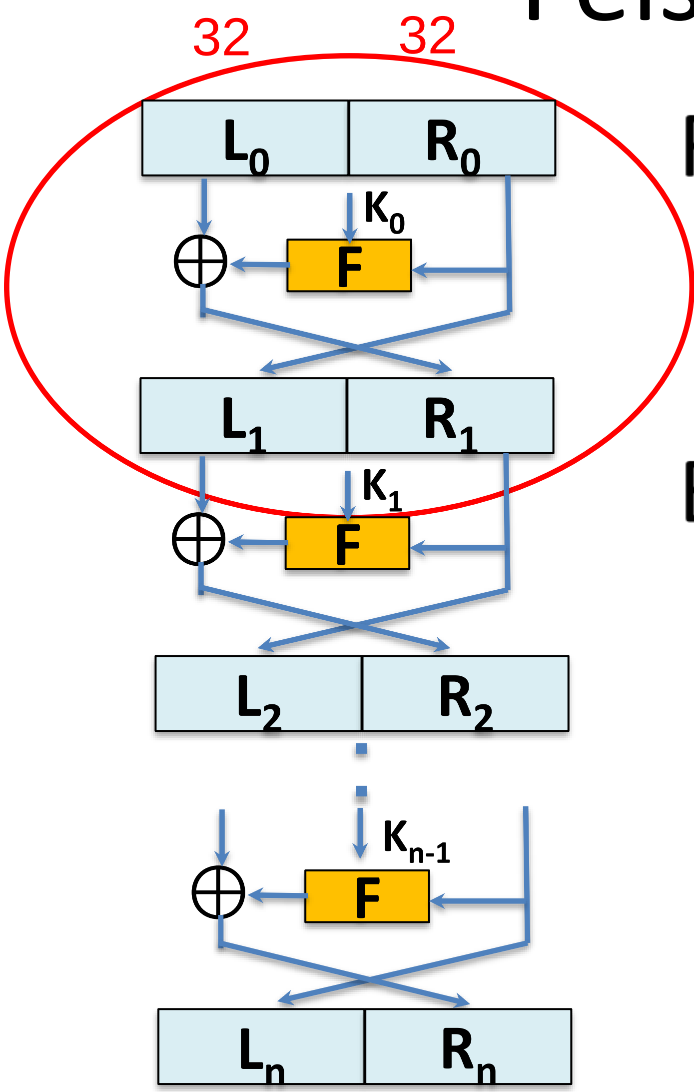
- In 1974, NBS issued a second request
  - IBM submitted Lucifer
- NBS requested NSA to help evaluation
  - NSA reduced the key size from 128 to 56 bits
  - But this received widespread criticisms
- 1976, the modified Lucifer adopted as standard
- After 1976, public research on crypto became unstoppable
- “DES did more to galvanize the field of cryptanalysis than anything else.” (Bruce Schneier)

A challenge in efficiency



Can we use the same circuit for both Enc/Dec?

Feistel Network



For i = 0, 1, … n-1

$$L_{i+1} = R_i$$

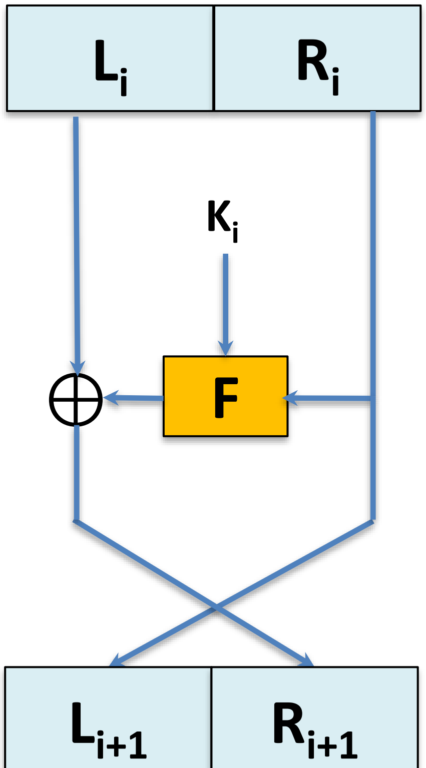
$$R_{i+1} = L_i \oplus F(K_i, R_i)$$

End

L1 = R0

R1 = L0 XOR F(K0,R0)

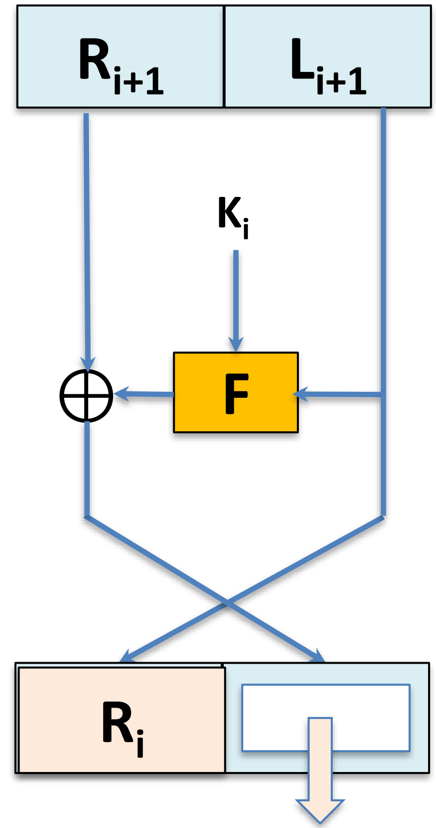
Invertible design



$$L_{i+1} = R_i$$
$$R_{i+1} = L_i \oplus F(K_i, R_i)$$

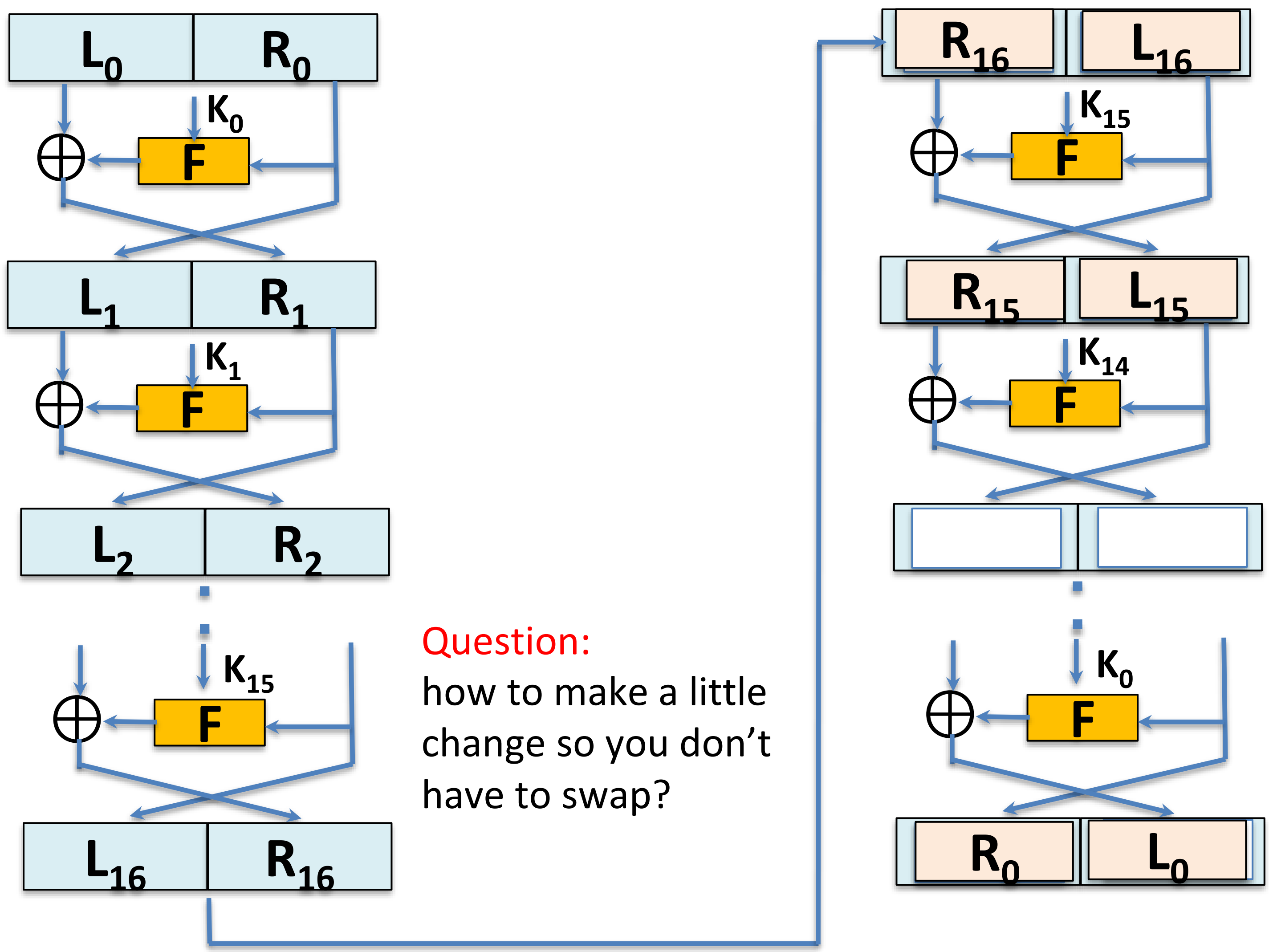
Inverse

$$R_i = L_{i+1}$$
$$L_i = \boxed{}$$



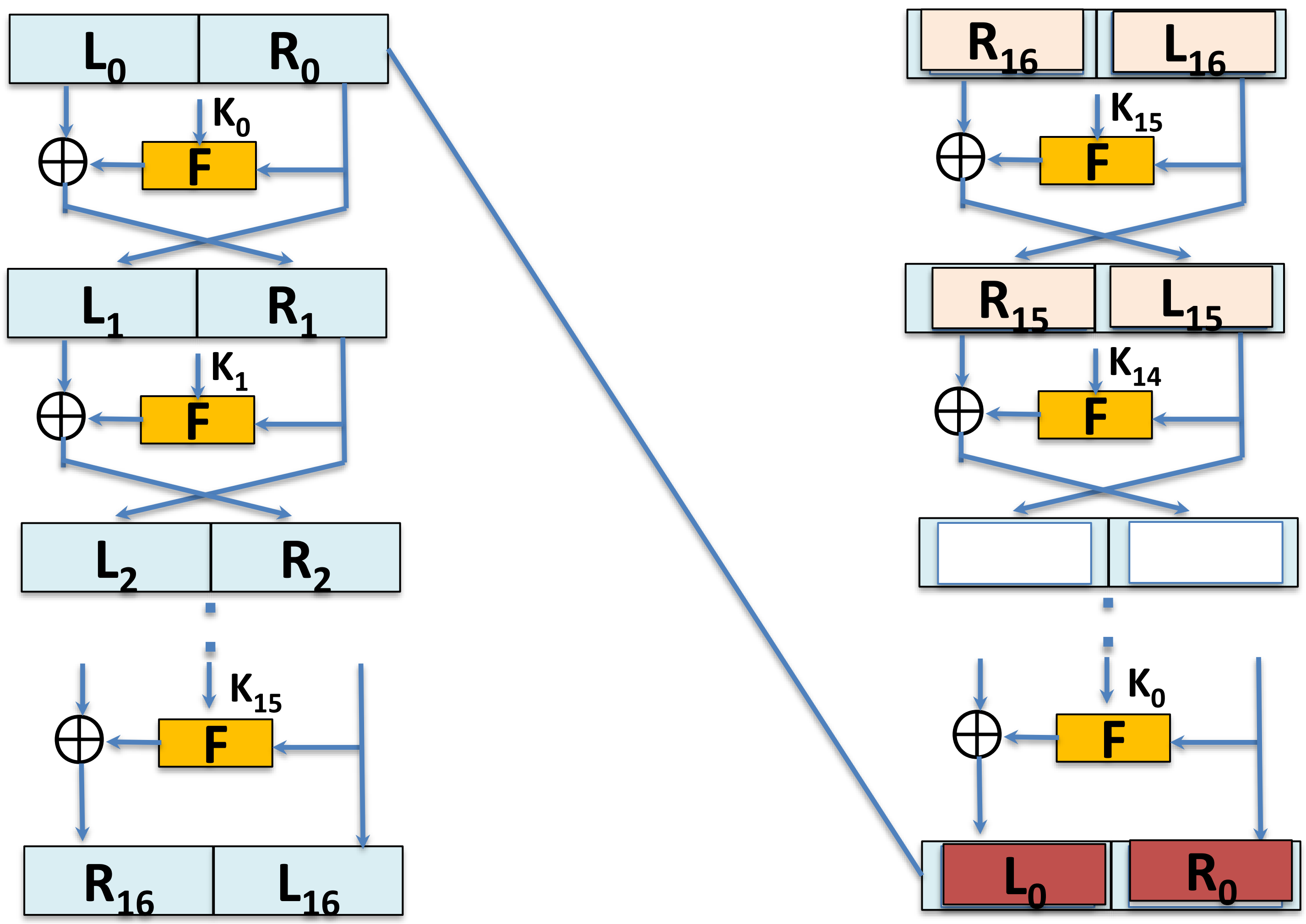
$L_i = R_{i+1}$ XOR $F(K_i , L_{i+1})$

DES Decryption

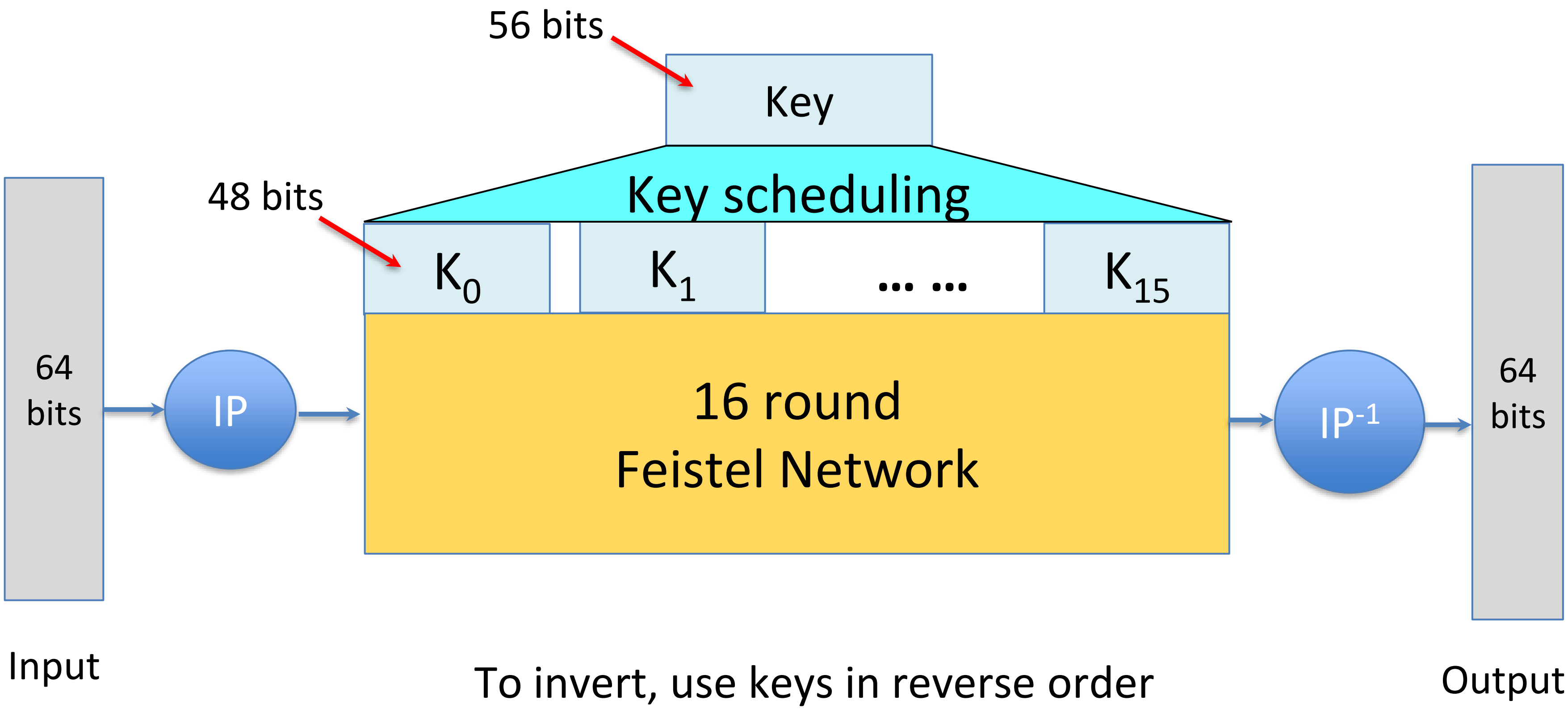


Question:
how to make a little change so you don't have to swap?

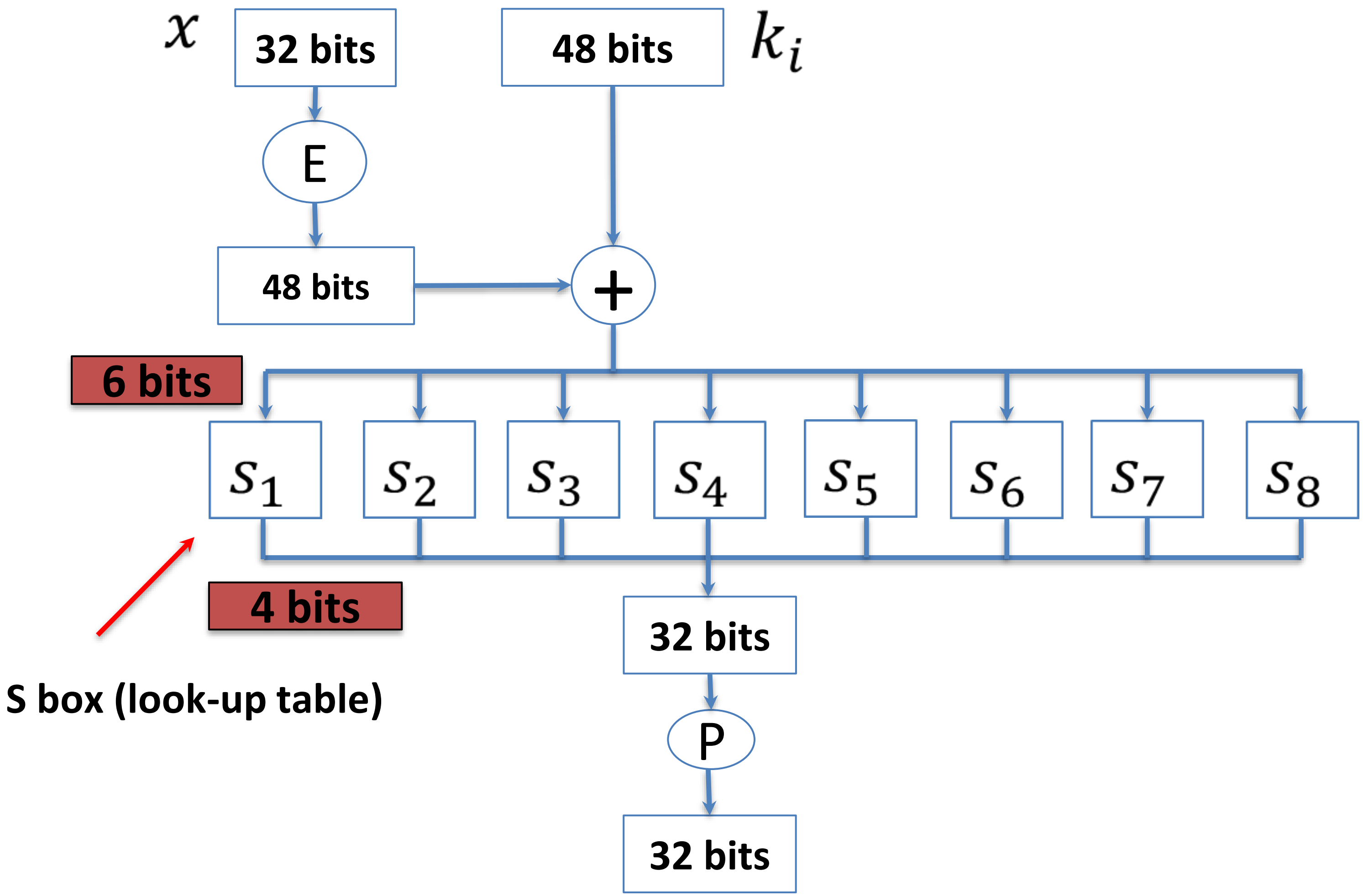
DES Decryption



DES: 16 round Feistel network



The F function: $F(k_i, x)$



The S-boxes

- $$S_i : \{0,1\}^6 \rightarrow \{0,1\}^4$$

	Middle 4 bits of input															
Outer bits	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

For example:

- Input = 011011
- Output = $\boxed{1001}$

Outer bits: 01

Middle bits: 1101

The P-boxes

- $\mathrm{P}: \{0,1\}^{32} \rightarrow \{0,1\}^{32}$

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Suppose $C = (c_1, c_2, c_3, c_4, c_5, \ldots, c_{31}, c_{32})$

Then $\mathrm{P(C)} = (c_{16}, c_7, c_{20}, c_{21}, c_{29}, \ldots, c_4, c_{25})$

Choosing the S-boxes and P-box

- S-boxes and P-box must be a careful choice
- Choosing at random would result in an insecure block cipher
- Several rules used in choice of S and P boxes
  - No output bit should be close to a linear function of the inputs bits
  - S-boxes are 4-to-1 mapping

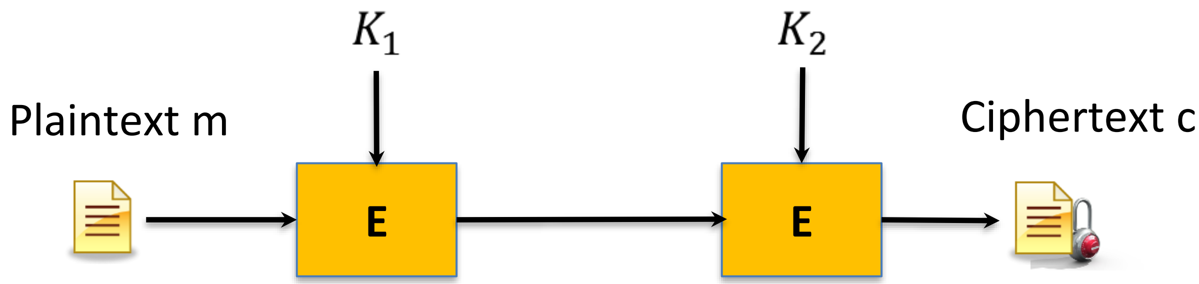
Brute-force attack on DES

- DES challenge by RSA company
  - Given plaintext/ciphertext pairs, find the key
- 1997:
  - Internet search, 96 days
- 1998
  - DES search machine (EFF), 56 hours
  - Cost: US$250K
  - The prize: US$10K
- 1999
  - Combined internet search and DES machine: **22 hours**
- Conclusion: 56-bit is too weak (128-bit key is the standard)

1 sec

2^(128-56)/3600/24/365 = 100 millions millions years

Strengthen DES by double encryption

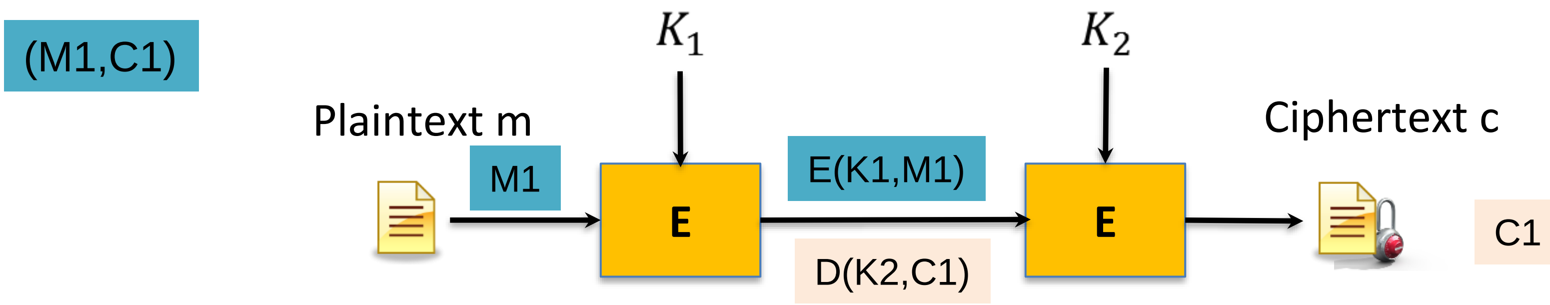


- Use double key 112-bits and encrypt twice

$$c = E(k_2, E(k_1, m))$$

Is this secure?

Breaking double encryptions



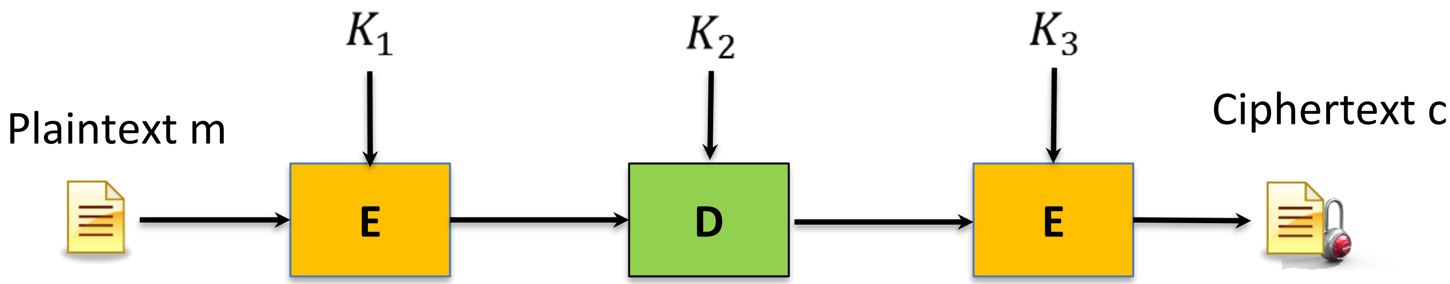
Meet in the middle attack: knowing a few (m, c) pairs

k_1 (56 bits)	$E(k_1, m_1)$
00….000	… …
00…001	
… …	… …
11…111	… …

$D(k_2, c_1)$	k_2(56 bits)
… …	00….000
… …	00…001
	… …
… …	11…111

Time: $2^{56} \times 2 = 2^{57}$ encryptions, Space: $2^{56} \times 2 \times 15$ bytes

A more secure combination: Triple DES

- 

- Variants
  - $k_1 \neq k_2 \neq k_3$: key size 168 bits, security 112 bits
  - $k_1 = k_3$: key size 112 bits, security 80 bits
  - $k_1 = k_2 = k_3$: key size 56 bits, security 56 bits