Modern Block Ciphers

- most widely used types of cryptographic algorithms

  DES, 3DES and AES

- provide privacy /authentication services

DES （Data Encryption Standard）
（数据加密标准）

1973年，美国国家标准局 NBS公开征集标准加密算法

设计要求:

① 必须提供高度的安全性

② 必须有详细的说明,并易于理解

③ 算法安全性取决于密钥,不依赖于算法

④ 适用于所有用户

⑤ 适用于不同应用场合

⑥ 实现必须经济（电子器件）

⑦ 必须被证实有效

⑧ 必须可出口

⑨ 必须高效

美国联邦政府密码标准

- 密码技术标准，主要包括：

  加密标准

  数字签名

  安全HASH 函数

  消息鉴别码

  密钥管理

  实体认证和访问控制

  口令用法

  随机数产生

  密码工程实施与密码产品检验

RFC中使用的关键字和关键短语的指导原则

RFC 2119 Harvard University

- “MUST”（必须）、“REQUIRED”（要求）或 “SHALL”（应该）：
  规范的绝对要求。

  “MUST NOT”（切勿）或 “SHALL NOT”（不应该）：
  规范的绝对禁止。

- “SHOULD”（应）或“RECOMMENDED”（建议）：
  表示在特定情形中可能存在忽略具体项目的合理原因，
  但是必须理解整个含义

  “SHOULD NOT”（不应）或 “NOT RECOMMENDED”（不建议）
  表示在特定情形下可能存在具体行为可被接受或可能有用的合理原因，
  但应理解整个含义

- “MAY”（可能） “OPTIONAL”（可选）
  表示项目是可选的

DES算法的产生

- **1974: 美国国家标准局(NBS)**征集

  IBM提交LUCIFER算法（**W. Tuchman 和 C. Meyer**研制）
- **1975**: NBS公开算法全部细节
- **1976**: NBS评估并采纳为联邦标准，用于非军事场合
- **1977**：DES ： FIPS PUB 46 发布生效

  规定每五年审查一次，十年后采用新标准
- **1994**：评估决定1998年12月以后，DES不再作为联邦加密标准
- **1999**：确认标准FIPS 46—3，采用三重密钥算法3-DES

  2004年之后，禁止在联邦政府中使用一重密钥DES，

  而3DES仍可继续使用

DES 算法特点

DEA：Data Encryption Algorithm, FIPS 46—3

- 分组加密算法：明文和密文为 **64位分组长度**
- 对称算法：加密和解密除密钥编排不同外，使用同一算法
- 密钥长度：56位 （56＋8）＝64 其中 8位为奇偶校验位
- 采用混乱和扩散的组合，每个组合先替代后置换，共16轮
- 只使用**标准的算术和逻辑运算**，易实现.

保密性均依赖于密钥

DES Encryption Overview

输入64比特明文数据

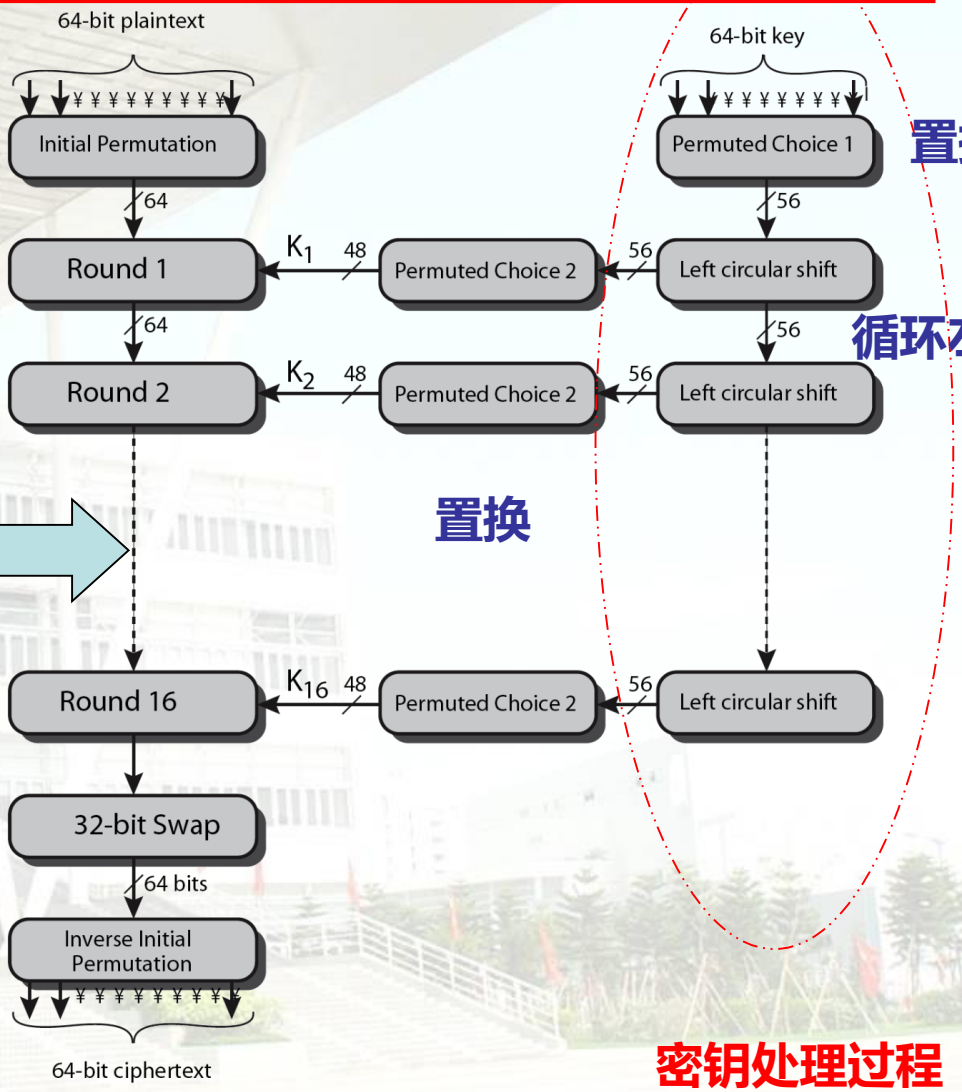
初始置换IP

在密钥控制下
16轮迭代

交换左右32比特

初始逆置换IP^{-1}

输出64比特密文数据



初始置换IP和初始逆置换IP - 1

初始置换 IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

初始逆置换 IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

IP和IP-1

把明文第20位置换到第14位

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

$$M_{20} \rightarrow M'_{14}$$

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56

IP−1

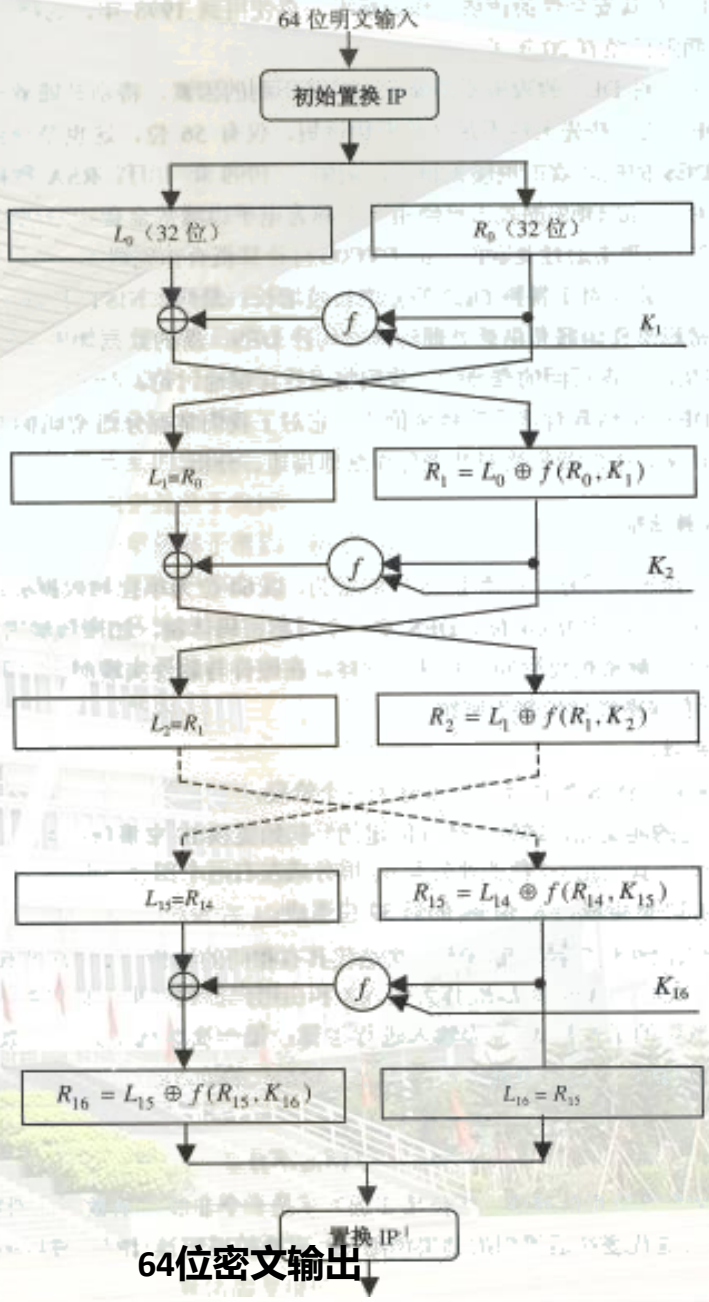
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

$$M'_{14} \rightarrow M''_{20}$$

第14位置换到第20位

DES的加密过程

16次迭代具有相同结构

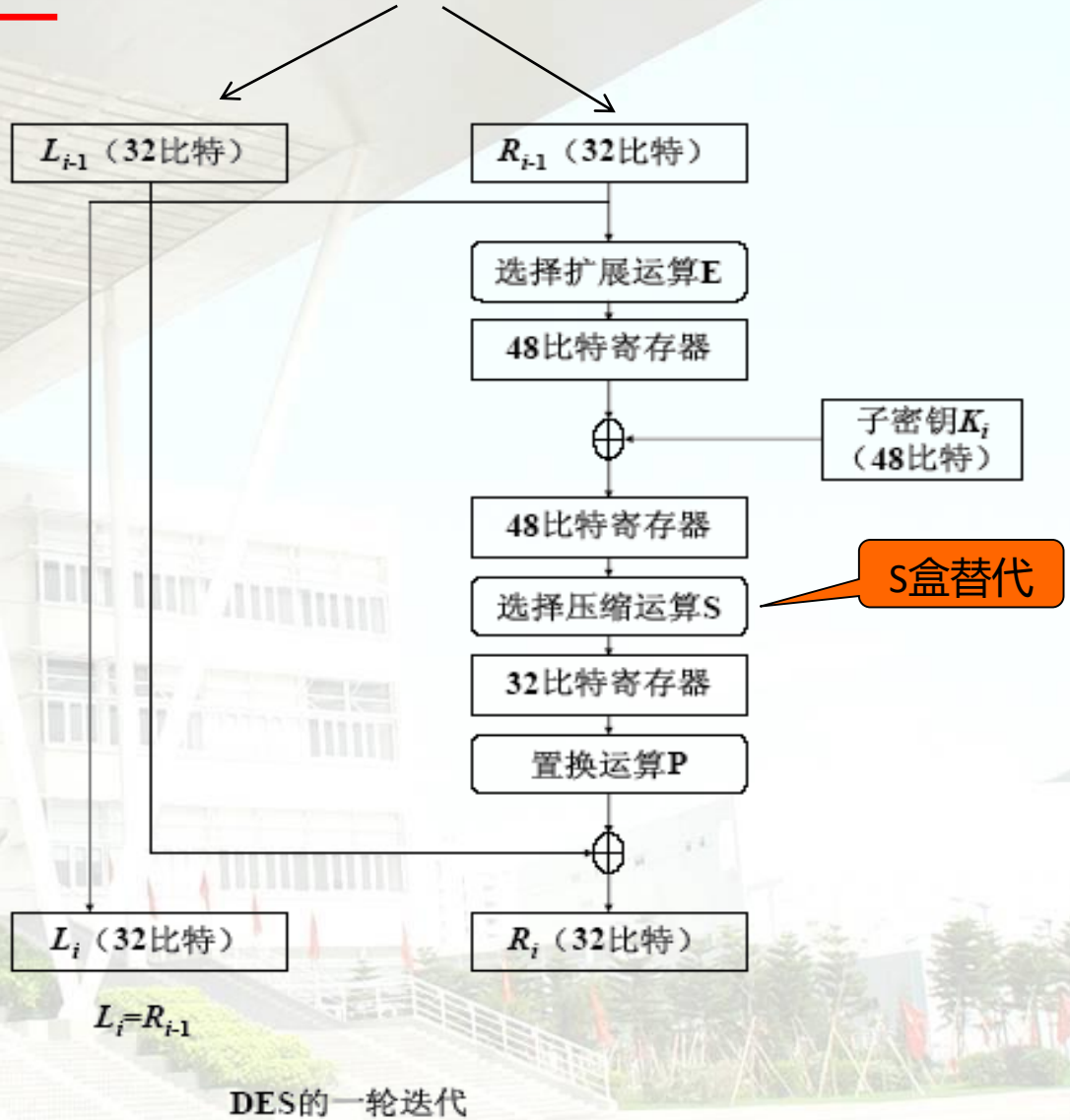


DES的一轮迭代

将64位的置换结果分为：左右两部分

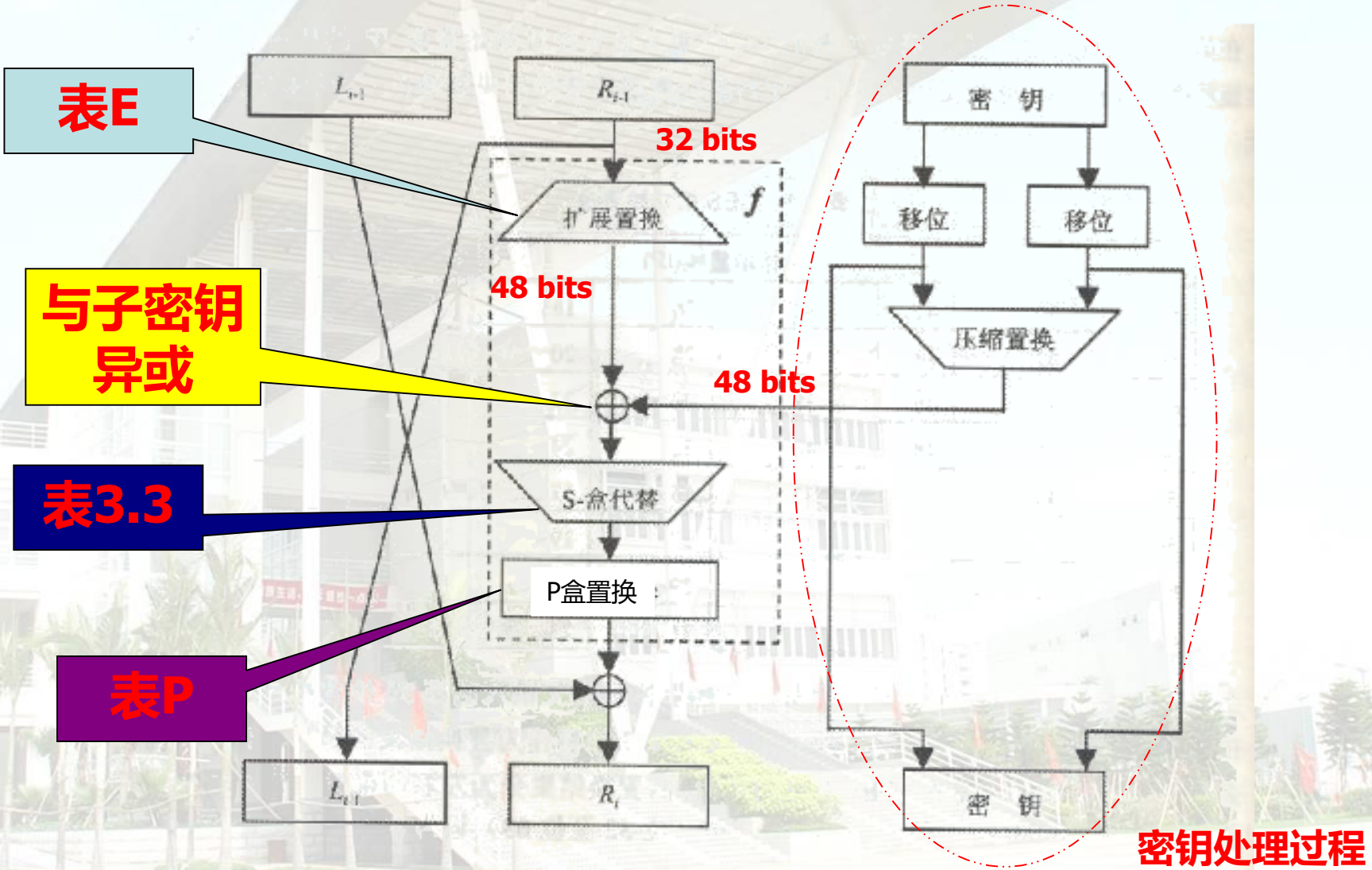
$L_i = R_{i-1}$

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

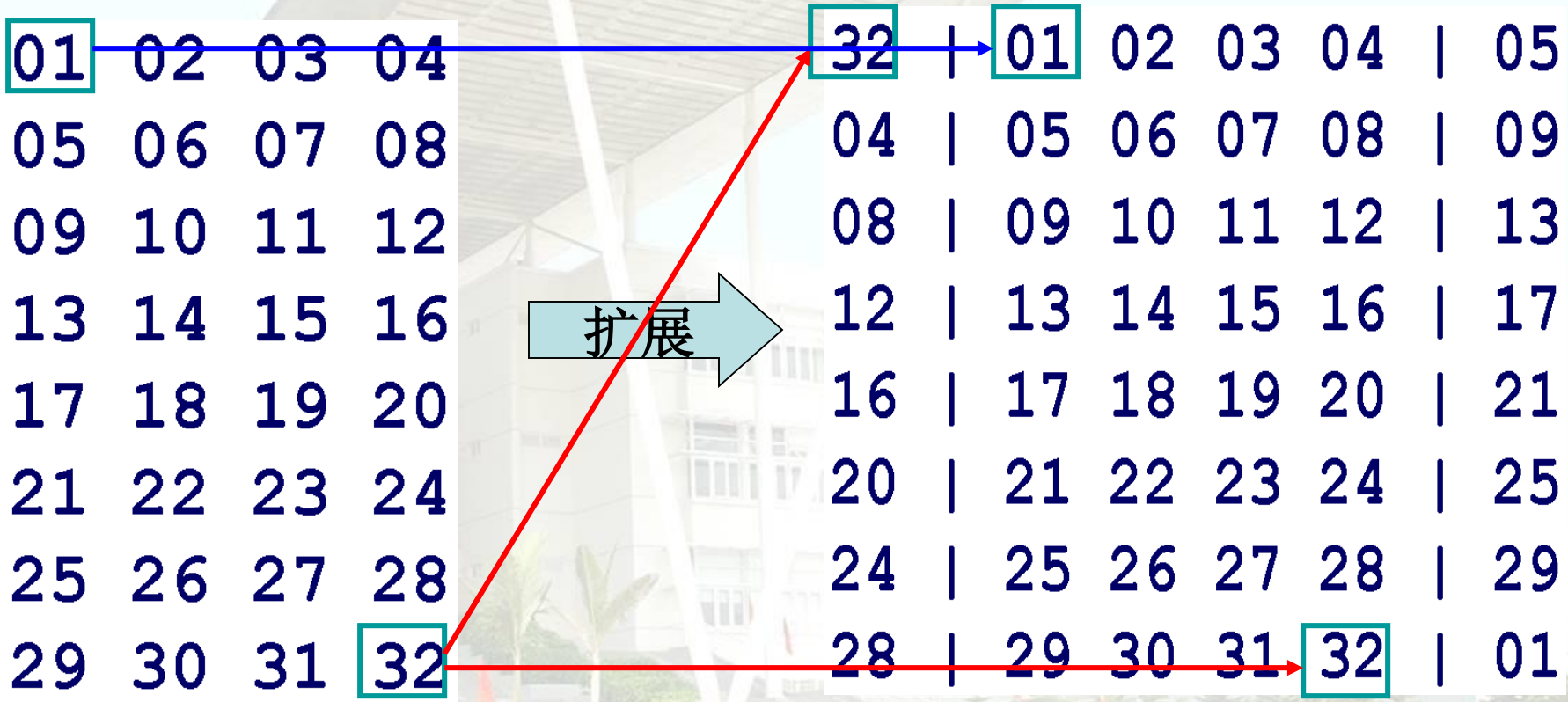


DES的一轮迭代

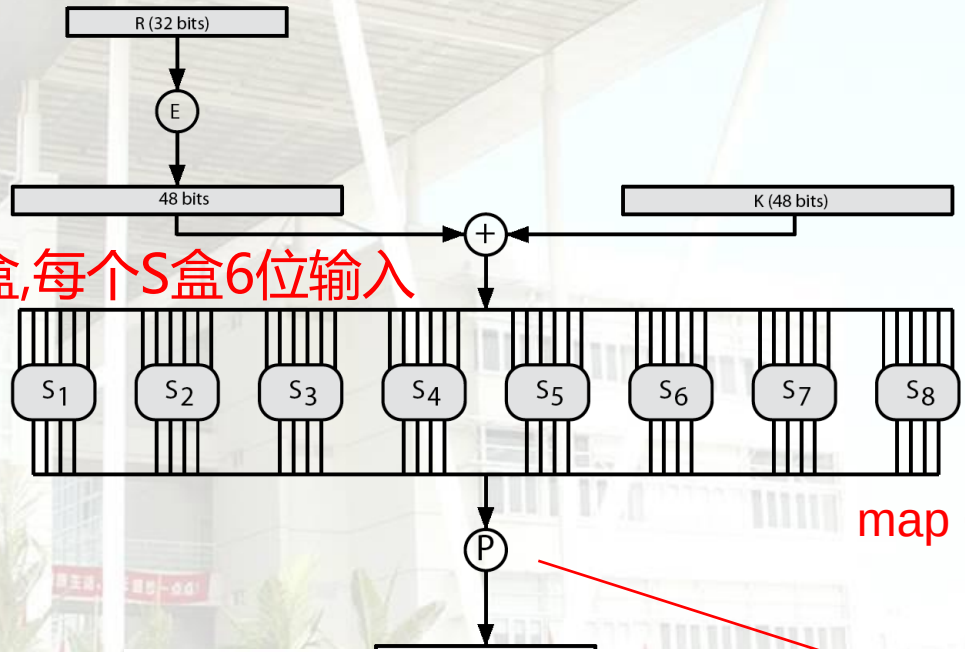
DES的轮迭代


表E
与子密钥异或
表3.3
表P
L_{i-1}
R_{i-1}
32 bits
扩展置换
f
48 bits
48 bits
S-盒代替
P盒置换
L_i
R_i
密 钥
移位
移位
压缩置换
密 钥
密钥处理过程

扩展置换 E -盒 - 32位扩展到48位



DES Round Structure



8个S盒,每个S盒6位输入

map 6 to 4 bits

P-盒置换

P-盒置换是对 S-盒的 32 位输出进行一次换位。 每位输入将要换到的新位置。

Substitution Boxes S

- have eight S-boxes which map 6 to 4 bits
- each S-box
  - outer bits 1 & 6 (**row** bits) select one row of 4

    011001 ->01 选01行（Table 3.2）
  - inner bits 2-5 (**col** bits) select one col of 16

    011001 ->1100 $(12)_{10}$ 选12列（Table 3.2）
  - result is 8 lots of 4 bits, or 32 bits
- selection depends on both data & key

DES Key Schedule

- forms subkeys used in each round
  - initial permutation of the key (PC1) which selects 56-bits in two 28-bit halves
  - 16 stages consisting of:
    - rotating **each half** separately either 1 or 2 places depending on the **key rotation schedule** K
    - selecting 24-bits from each half & permuting them by PC2 for use in round function F
- practical use issues in h/w vs s/w

DES Decryption 解密

- do encryption steps again
- But using subkeys in reverse order (SK16 … SK1)

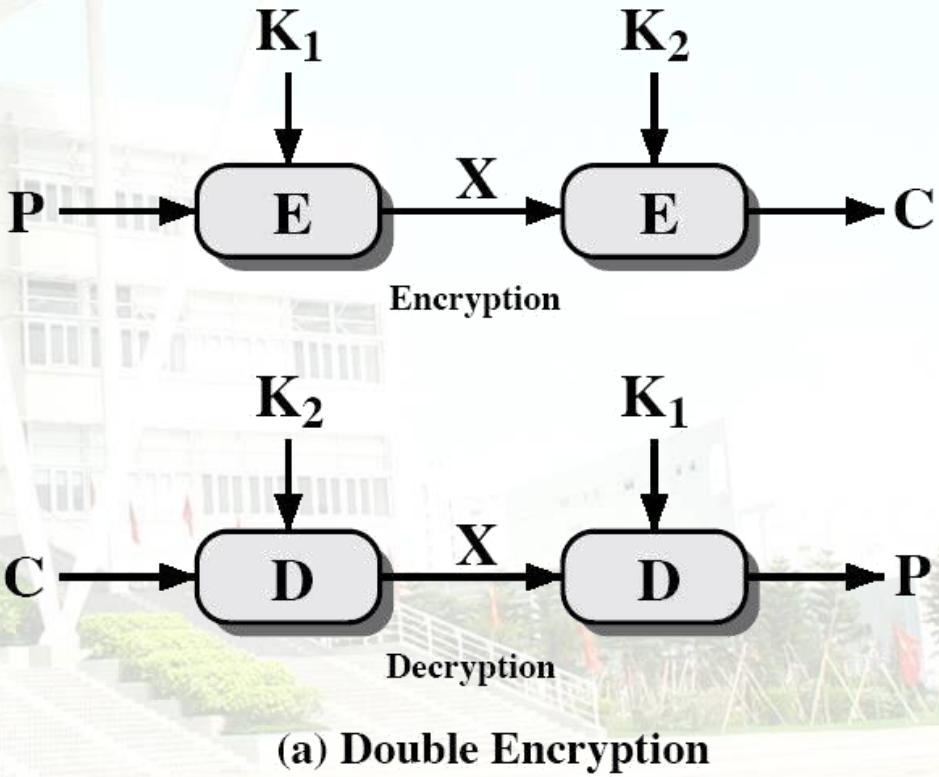
改进算法-2DES

2DES 加密形式有两个阶段和两个密钥。

$$C = E_{k2}\ (E_{k1}\ (P))$$

$$P = D_{k1}\ (D_{k2}\ (C))$$

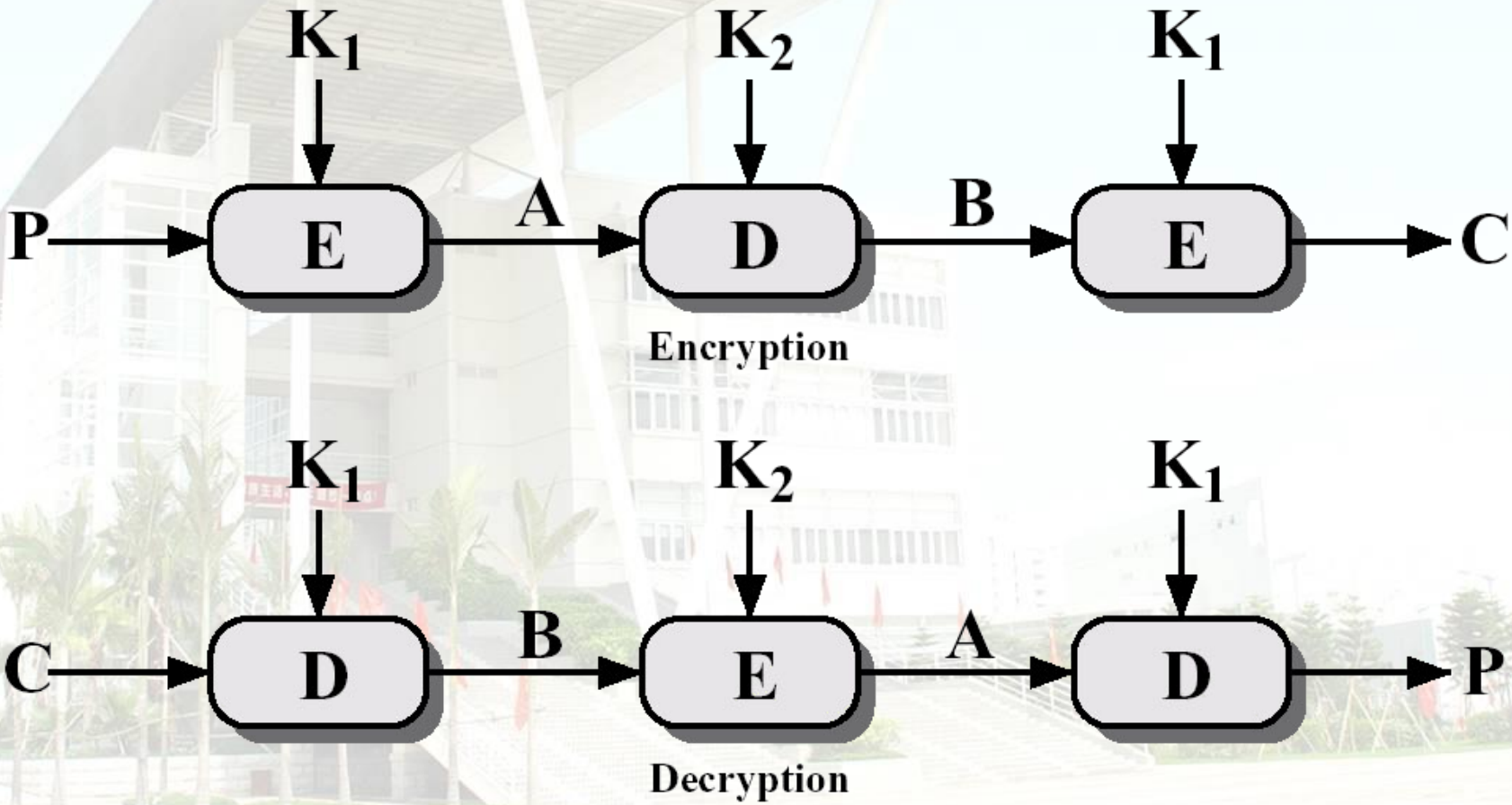
密钥长度= 56 X 2 =112



(a) Double Encryption

3-DES

$$C=E_{K3}(D_{K2}(E_{K1}(P))) \Leftrightarrow P=D_{K1}(E_{K2}(D_{K3}(C)))$$



改进算法-3DES

两个密钥的3DES：

$C = E_{k1}(D_{k2}(E_{k1}(P)))$

三个密钥的3DES：

$C = E_{k3}(D_{k2}(E_{k1}(P)))$

168-bit　　196-bit

密钥长度= 56 X 3 =168