

密码学

第三讲 数据加密标准(DES)

张焕国

武汉大学计算机学院

空天信息安全与可信计算教育部重点实验室





内容简介

第一讲 信息安全概论

第二讲 密码学的基本概念

第三讲 数据加密标准 (DES)

第四讲 高级数据加密标准 (AES)

第五讲 中国商用密码 (SMS4)

第六讲 分组密码的应用技术

第七讲 序列密码

第八讲 复习

第九讲 公钥密码 (1)





内容简介

第十讲 公钥密码 (2)

第十一讲 数字签名 (1)

第十二讲 数字签名 (2)

第十三讲 **HASH**函数

第十四讲 认证

第十五讲 密码协议

第十六讲 密钥管理 (1)

第十七讲 密钥管理 (2)

第十八讲 复习

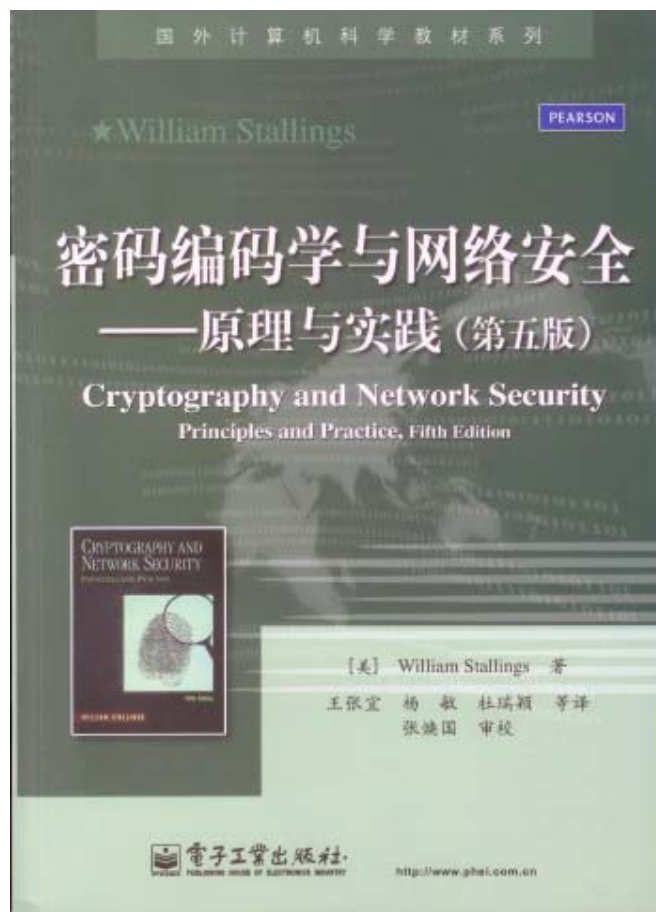


教材与主要参考书

教材



参考书



武汉大学



一、DES概况

1、几个重要的历史时间

- 1973年美国国家标准局（NBS）向社会公开征集加密算法，以制定加密算法标准；
- 1974年第二次征集；
- 1975年选中IBM的算法，并公布征求意见；
- 1977年1月15日正式颁布；
- 1998年底以后停用；
- 1999年颁布3DES为新标准。





一、DES概况

2、标准加密算法的目标

- 用于加密保护政府机构和商业部门的**非机密的敏感数据**。
- 用于加密保护**静态存储**和**传输信道**中的数据。
- 安全使用**10 ~15年**。





一、DES概况

3、密码的整体特点

①分组密码

■ 明文、密文和密钥的分组长度都是**64**位。

②面向二进制数据的密码算法

■ 因而能够加解密任何形式的计算机数据。

③对合运算：

■ $f = f^{-1}$

■ 加密和解密共用同一算法，使工程实现的工作量减半。

④综合运用了置换、代替、代数等基本密码技术。

⑤基本结构属于Feistel结构。





一、DES概况

4、应用

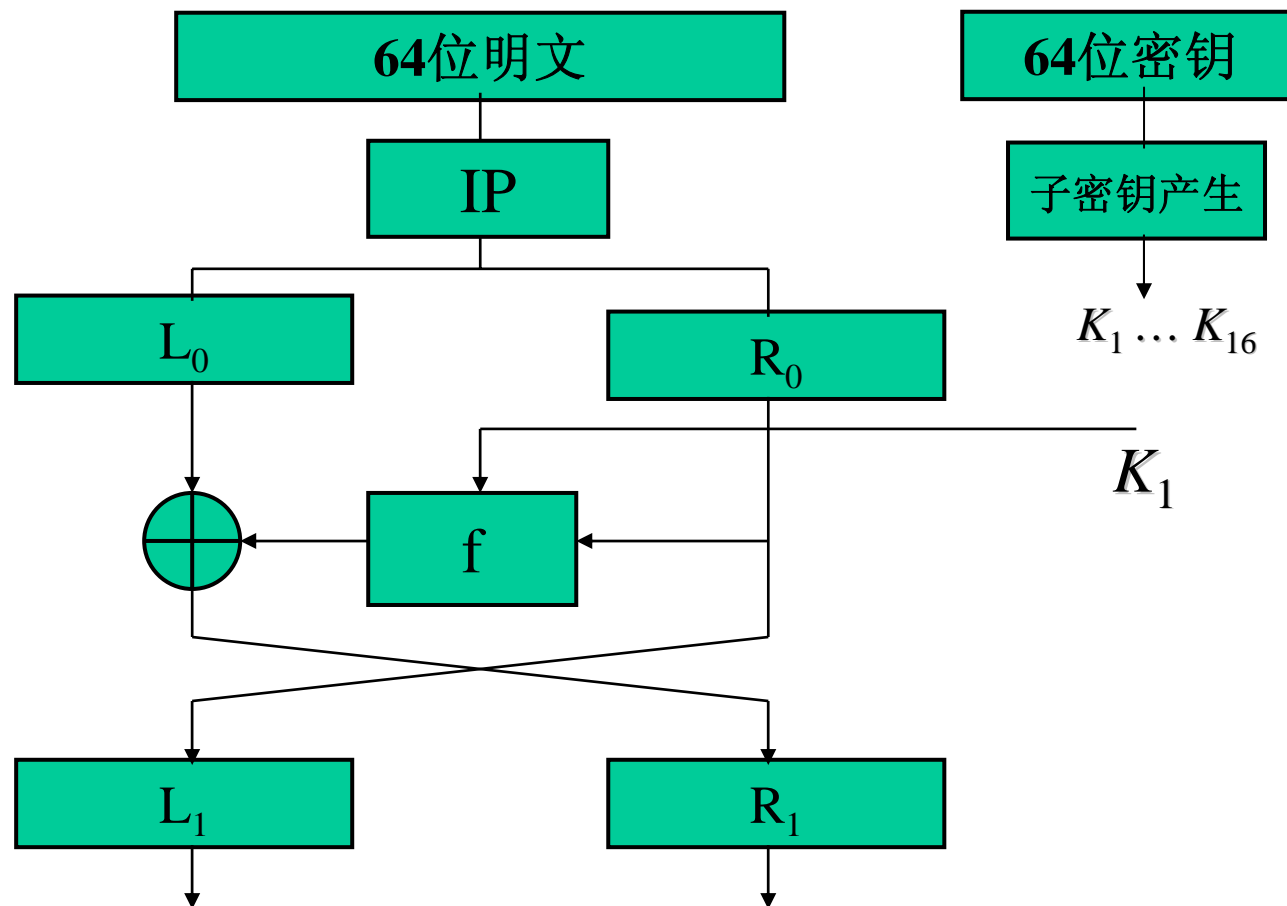
- ①在全世界范围得到广泛应用。
- ②许多国际组织采用为标准。
- ③产品形式：软件（嵌入式软件，应用软件）
硬件（芯片，插卡，专用设备）

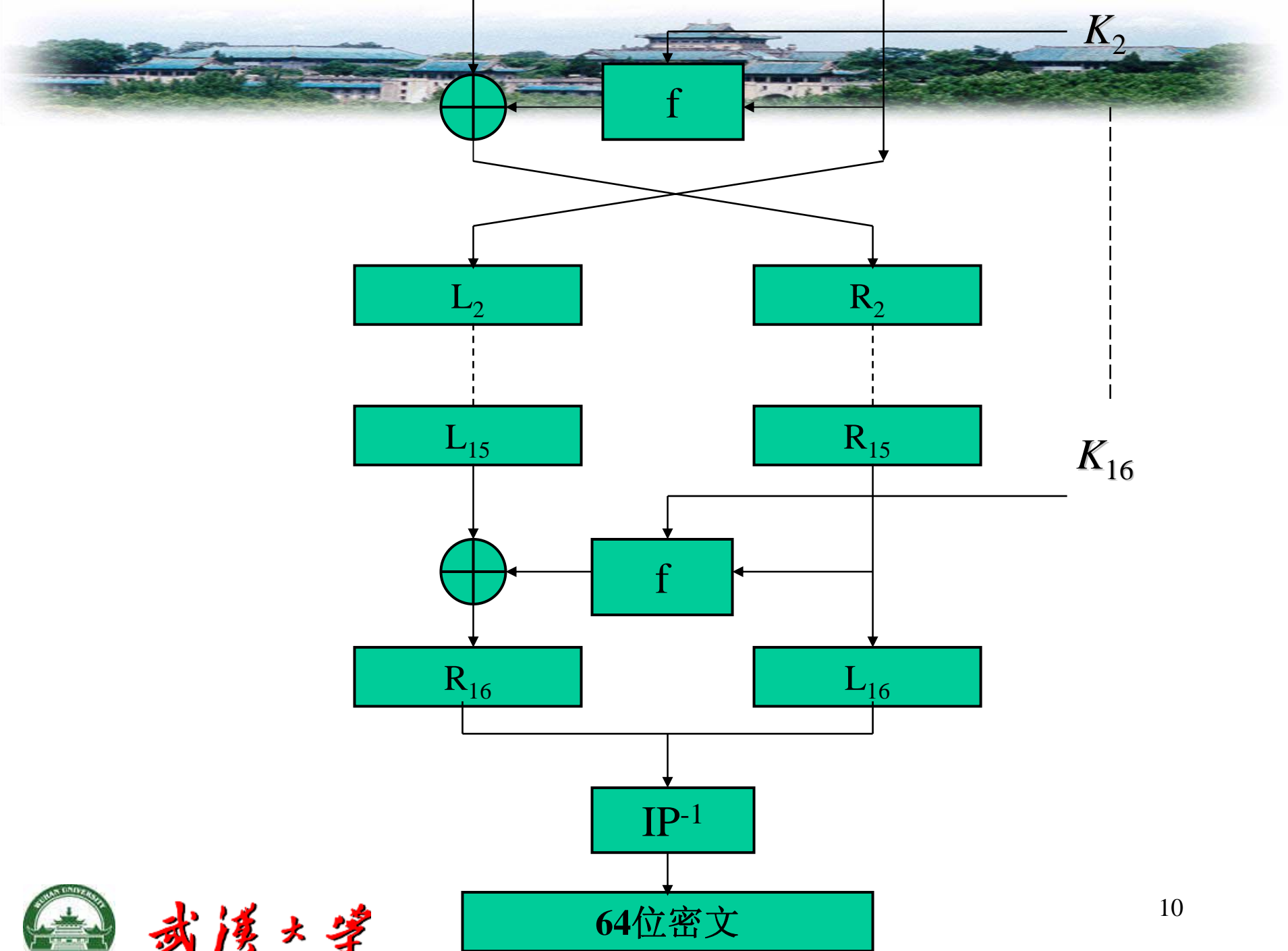
5、结论

- 用于其设计目标是安全的。
- 设计精巧、实现容易、使用方便，堪称典范。
- 为国际信息安全发挥了重要作用。



二、DES算法框图







三、DES加密过程

- 1、64位密钥经子密钥产生算法产生出16个子密钥： K_1, K_2, \dots, K_{16} ，分别供第一次，第二次，...，第十六次加密迭代使用。
- 2、64位明文经初始置换IP，将数据打乱重排并分成左右两半。左边为 L_0 ，右边为 R_0 。
- 3、第一次加密迭代：
在子密钥 K_1 的控制下，由加密函数 f 对 R_0 加密：
$$L_0 \oplus f(R_0, K_1)$$

以此作为第二次加密迭代的 R_1 ，以 R_0 作为第二次加密迭代的 L_1 。





三、DES加密过程

4、第二次加密迭代至第十六次加密迭代分别用子密钥 K_2 ，...， K_{16} 进行，其过程与第一次加密迭代相同。

5、第十六次加密迭代结束后，产生一个64位的数据组。以其左边32位作为 R_{16} ，以其右边32位作为 L_{16} 。

6、 R_{16} 与 L_{16} 合并，再经过逆初始置换 IP^{-1} ，将数据重新排列，便得到64位密文。

7、DES加密过程的数学描述：

$$\begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \\ i = 1, 2, \dots, 16 \end{cases}$$





四、DES子密钥的产生

1、功能

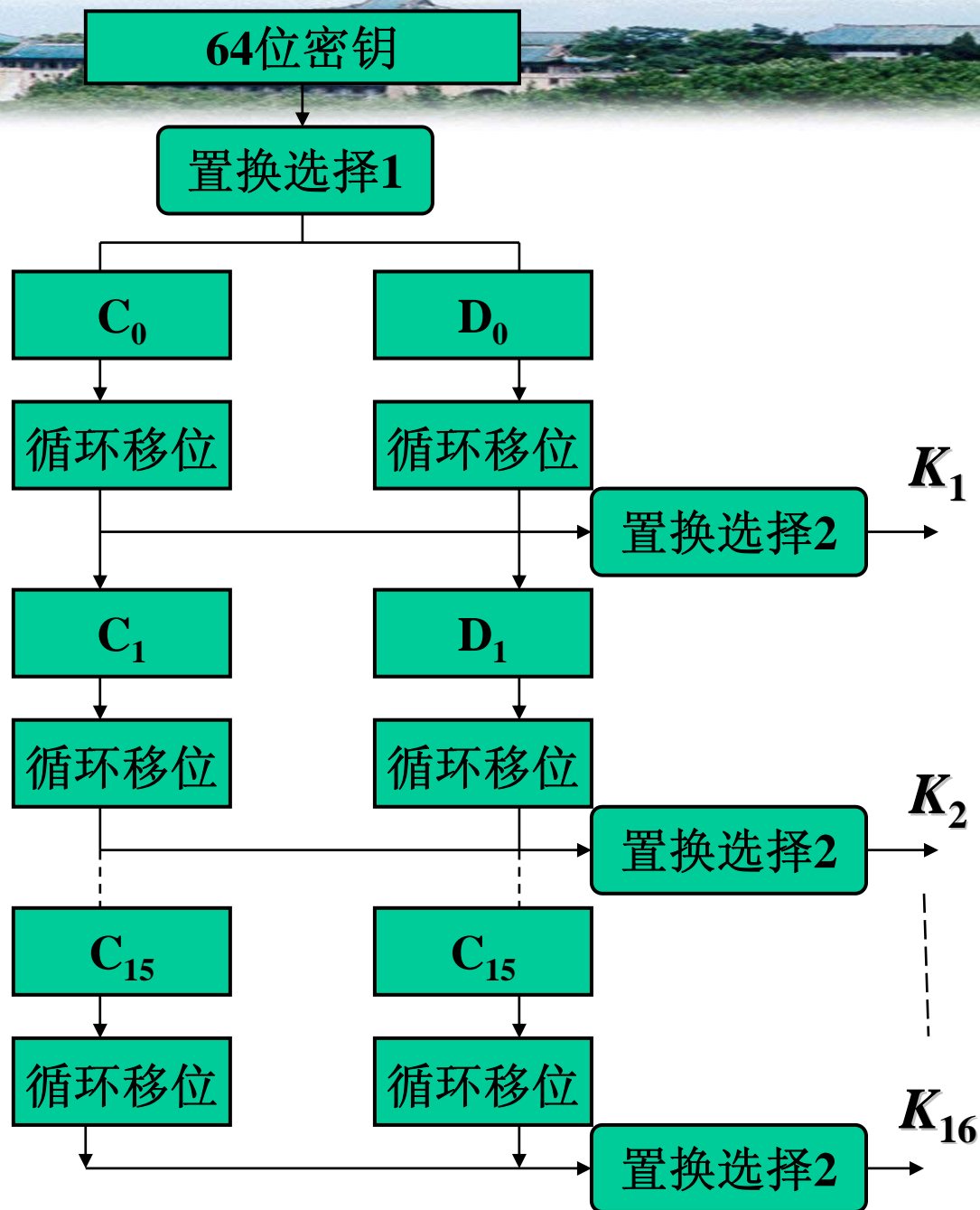
64位密钥经过置换选择1、循环左移、置换选择2等变换，产生16个子密钥

$$K_1, K_2, \dots, K_{16}$$

分别供各次加密迭代使用。



2. 子密钥 产生框图





四、DES子密钥的产生

3、置换选择1

①、作用

- 去掉密钥中的8个奇偶校验位。
- 打乱重排，形成 C_0 (左28位)， D_0 (右28位)。

②、矩阵

 C_0 D_0

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

- #### ③说明：
- 矩阵中第一个数字47，表明原密钥中的第47位移到 C_0 中的第一位。





四、DES子密钥的产生

4、循环移位

①、作用

- 对 C_0 ， D_0 分别循环左移位。

②、循环移位表

迭代次数	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
移位次数	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1





四、DES子密钥的产生

5、置换选择2:

①、作用

- 从 C_i 和 D_i (56位) 中选择一个48位的子密钥 K_i

②、矩阵

K_i

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

- #### ③、说明：从 C_i 中取出24位，从 D_i 中取出24位，形成48位的子密钥 K_i





五、初始置换IP

①、作用

- 把64位明文打乱重排
- 左一半为 L_0 (左32位)，右一半为 R_0 (右32位)。
 - 例如：把输入的第1位置换到第40位，把输入的第58位置换到第1位。





五、初始置换IP

②、矩阵

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

注意：

- IP中的置换是规律的
- 这对保密是不利的





六、逆初始置换 IP^{-1}

①、作用

- 把64位中间密文打乱重排。
- 形成最终的64位密文。

②、相逆性

- IP 与 IP^{-1} 互逆。
- 例：在 IP 中把输入的第1位置换到第40位，而在 IP^{-1} 中把输入的第40位置换到第1位。

③、保密作用不大

- 由于没有密钥参与，在 IP 和 IP^{-1} 公开的条件下，其保密意义不大





六、逆初始置换IP⁻¹

④、矩阵

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

注意：

- 由于IP中的置换是规律的

- 所以IP⁻¹中的置换也是规律的

- 这对保密是不利的

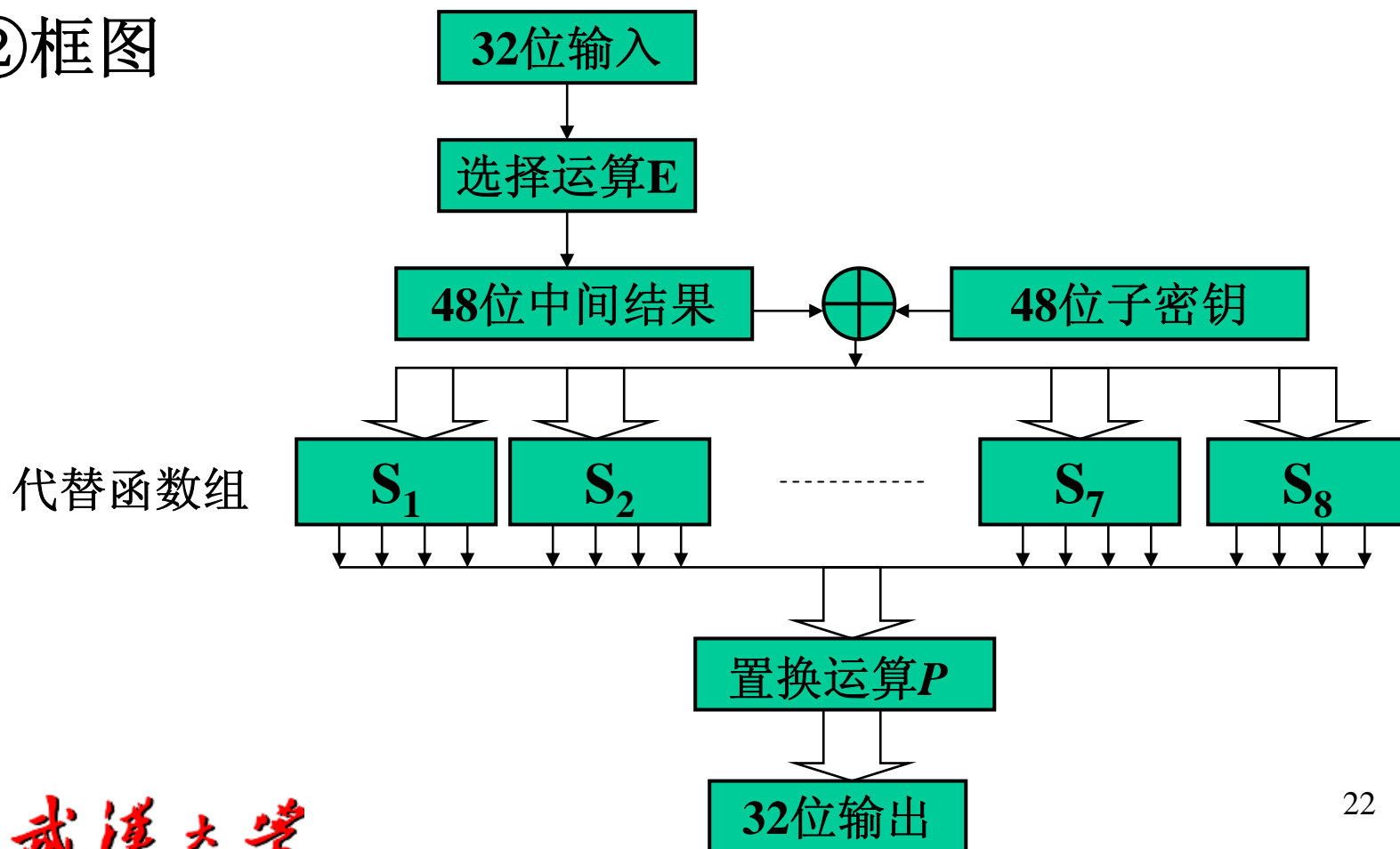


七、加密函数 f

①作用

■ DES的轮函数，DES保密的核心。

②框图





七、加密函数 f

③选择运算E

- 把32位输入扩充为48位中间数据;
- 通过重复使用数据, 实现数据扩充。
- 矩阵:

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





七、加密函数 f

④代替函数组S (S盒)

● S 盒的一般性质

- S盒是DES中唯一的非线性变换，是DES安全的关键。
- 在保密性方面，起混淆作用。
- 共有8个S盒，并行作用。
- 每个S盒有6个输入，4个输出，是非线性压缩变换。
- 设输入为 $b_1b_2b_3b_4b_5b_6$ ，则以 b_1b_6 组成的二进制数为行号， $b_2b_3b_4b_5$ 组成的二进制数为列号。行列交点处的数（二进制）为输出。





七、加密函数 f

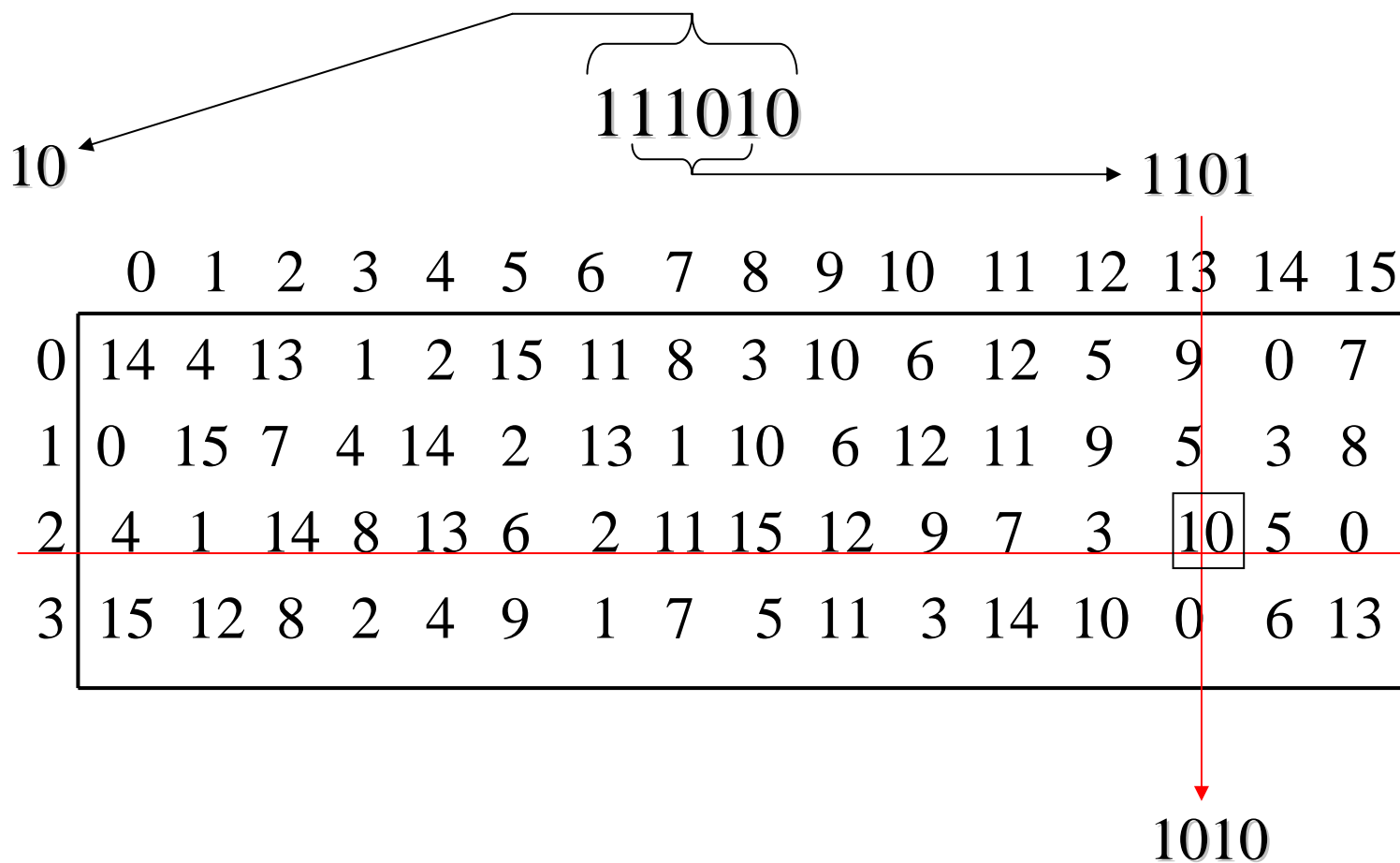
举例：

S_1

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



七、加密函数 f





七、加密函数 f

● S盒的设计准则

1976年，NSA公布的DES的S盒设计准则：

- P0: 每个S盒的每一行都是整数0到15的一个置换；
- P1: 每个S盒的输出不是它的输入的线性或仿射函数；
- P2: 改变S盒的任一输入比特，其输出至少有两比特发生改变；
- P3: 对任一S盒和任一输入 x ， $S(x)$ 和 $S(x \oplus 001100)$ 至少有两位发生变化（这里 x 是一个长度为6的比特串）；
- P4: 对任何S盒和任一输入 x ，以及 $e, f \in \{0, 1\}$ ，有 $S(x) \neq S(x \oplus 11ef00)$ ，其中 x 是一个长度为6的比特串；
- P5: 对任何S盒，当它的任一输入比特位保持不变，其它5位改变时，输出数字中0和1的数目大致相等。





七、加密函数 f

● 其它准则

美国NSA至今没有完全公布S盒的设计细节。研究表明，除了上述准则外，还有一些其它准则。

- 非线性度准则：S盒必须有足够的非线性度，否则不能抵抗线性攻击；
- 差分均匀性准则：S盒的差分性应均匀，否则不能抵抗差分攻击；
- 代数次数及项数分布准则：S盒必须有足够的代数次数和项数，否则不能抵抗插值攻击和高阶差分攻击；

● 结论：S盒的密码学特性确保了DES的安全！





七、加密函数 f

⑤ 置换运算 P

- 把数据打乱重排。
- 在保密性方面，起扩散作用：
 - 因为S盒是6位输入，4位输出，其非线性作用是局部的
 - 因此，需要把S盒的混淆作用扩散开来
- S盒与P置换的互相配合，共同确保DES的安全。
- 矩阵：

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





八、DES的解密过程

- DES的加密算法是对合运算，因此解密和加密可共用同一个算法。
- 不同点：子密钥使用的顺序不同。
- 第一次解密迭代使用子密钥 K_{16} ，第二次解密迭代使用子密钥 K_{15} ，第十六次解密迭代使用子密钥 K_1 。
- DES解密过程的数学描述：

$$\begin{cases} R_{i-1} = L_i \\ L_{i-1} = R_i \oplus f(L_i, K_i) \\ i = 16, 15, 14, \dots, 1 \end{cases}$$





九、DES的对合性和可逆性

1、可逆性证明

① 定义 变换 T 是把64位数据的左右两半交换位置：

$$T(L, R) = (R, L)$$

● 因为， $TT(L, R) = (L, R) = I$ ，其中 I 为恒等变换。

又显然 $TT^{-1}=I$ ，于是， $TT^{-1}=TT$ ，所以有

$$T=T^{-1}.$$

所以 T 变换是对合运算。





九、DES的对合性和可逆性

1、可逆性证明

②记 DES第 i 轮中的主要运算为，即

$$F_i(L_{i-1}, R_{i-1}) = (L_{i-1} \oplus f(R_{i-1}, K_i), R_{i-1})$$

$$\begin{aligned} \bullet F_i^2 &= F_i(L_{i-1} \oplus f(R_{i-1}, K_i), R_{i-1}) \\ &= (L_{i-1} \oplus f(R_{i-1}, K_i) \oplus f(R_{i-1}, K_i), R_{i-1}) \\ &= (L_{i-1}, R_{i-1}) \\ &= I \end{aligned}$$

所以， $F_i = F_i^{-1}$ 。

● 所以 F_i 变换也是对合运算。





九、DES的对合性和可逆性

1、可逆性证明

③ 结合①、②，便构成DES的轮运算

$$H_i = F_i T$$

● 因为 $(F_i T) (T F_i) = (F_i (T T) F_i) = F_i F_i = I$,

● 所以

$$(F_i T)^{-1} = (T F_i)$$

$$(F_i T) = (T F_i)^{-1}$$





九、DES的对合性和可逆性

1、可逆性证明

④加解密表示

$$(1) \text{ DES}(M) = (M) \text{ IP } (F_1 T) (F_2 T) \dots (F_{15} T) (F_{16}) \text{ IP}^{-1} = C$$

$$(2) \text{ DES}^{-1}(C) = (C) \text{ IP } (F_{16} T) (F_{15} T) \dots (F_2 T) (F_1) \text{ IP}^{-1} = M$$

● 把 (1) 式代入 (2) 式可证：

$$\text{DES}^{-1}(\text{DES}(M)) = M$$

● 所以，**DES是可逆的。**





九、DES的对合性和可逆性

2、对合性证明

$$\text{DES} = IP (F_1 T) (F_2 T) \dots (F_{15} T) (F_{16}) IP^{-1}$$

$$\text{DES}^{-1} = IP (F_{16} T) (F_{15} T) \dots (F_2 T) (F_1) IP^{-1}$$

● DES和DES⁻¹ 除了子密钥的使用顺序相反之外是相同的。

● 不考虑子密钥的使用顺序：

$$\text{DES} = IP (F) (TF) (TF) \dots (TF) (TF) (TF) IP^{-1}$$

$$\text{DES}^{-1} = IP (F) (TF) (TF) \dots (TF) (TF) (TF) IP^{-1}$$

● 显然：DES = DES⁻¹

● 所以DES的运算是**对合运算**。





十、DES的安全性

①攻击

- 穷举攻击。目前最有效的方法。
- 差分攻击。
- 线性攻击。

②安全弱点

- 密钥太短。
- 存在弱密钥。
- 存在互补对称性。

设 $C=DES(M, K)$ ，则有 $\overline{C}=DES(\overline{M}, \overline{K})$ 。





十、3重DES

①美国NIST在1999年发布了一个新版本的DES标准（FIPS PUB46-3）：

- DES只用于遗留系统。
- 3DES将取代DES成为新的标准。
- 国际组织和我国银行都接受3DES。





十、3重DES

② 3DES的优势:

- 3密钥的3DES: 密钥长度是168位。

- 2密钥的3DES: 密钥长度是112位。

- 安全: 密钥足够长;

经过最充分的分析和实践检验。

- 兼容性好。

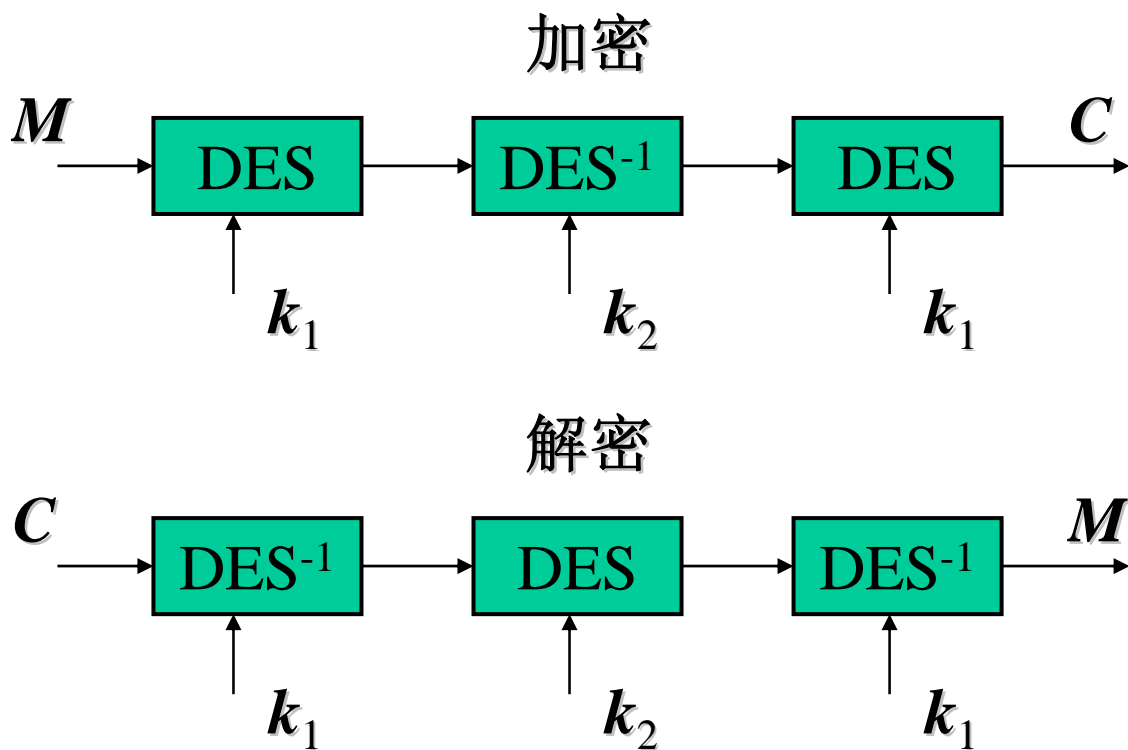
③ 3DES的弱势:

- 速度慢。



十、3重DES

④2密钥3DES框图





十一、DES的历史回顾

● DES的贡献

- DES很好地体现了商农的密码设计理论。
- DES体现了密码公开设计原则，开创了公开密码算法的先例。
- DES代表当时商业密码的最高水平，是商用密码的典范。
- DES对确保国际信息安全和提高国际密码设计水平都发挥了重要作用。

● DES给我们的启示

- 商业密码应当坚持公开设计原则；
- 商业密码标准应当公布算法。





作业题

- 1、p113第4题。
- 2、p113第7题。

自选实践题

- 1、p113第8题。





谢 谢！



武汉大学