密 码 学

第三讲　数据加密标准(DES)

王后珍

武汉大学国家网络安全学院

空天信息安全与可信计算教育部重点实验室

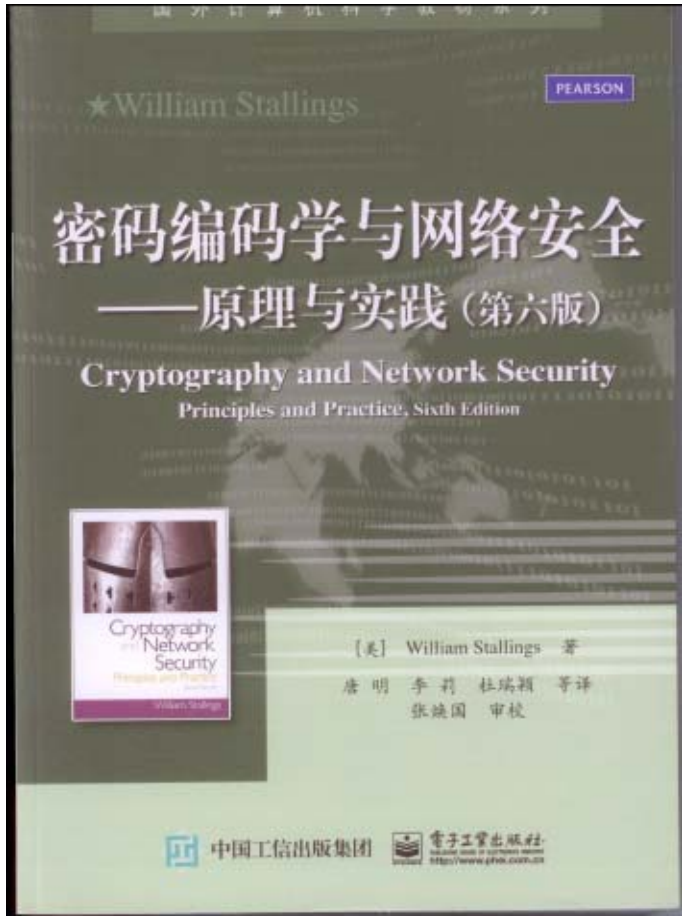
目 录

目 录

教材与主要参考书

教材

参考书



上节回顾——古典密码

- 代换（代替、替换）技术
  - 将明文字母替换成其它字母、数字或符号的方法。
- 置换（换位）技术
  - 保持明文的所有字母不变，只是打乱明文字母的位置和次序。
- 一次一密
  - **Vernam**代数密码，加解密算法都是模2加。

代数密码：

① **Vernam密码(1917年，AT&T Gilbert Vernam)**

明文、密文、密钥都表示为二进制位：

$$M=m_1,m_2,\ldots,m_n$$

$$K=k_1,k_2,\ldots,k_n$$

$$C=c_1,c_2,\ldots,c_n$$

② *加密*： $c_1=m_i \oplus k_i$,i=1,2,… ,n

解密： $m_1=c_i \oplus k_i$,i=1,2,… ,n

③因为加解密算法是模2加，所以称为代数密码。

④对合运算：$f=f^{-1}$，*模2加运算是对合运算。*

密码算法是对和运算，则加密算法＝解密算法，工程实现工作量减半。

⑤ **Vernam**密码经不起已知明文攻击。

代数密码：

⑥ 如果密钥序列有重复，则**Vernam**密码是不安全的。

⑦ *一种极端情况：一次一密*

- 密钥是随机序列。
- 密钥至少和明文一样长。
- 一个密钥只用一次。

⑧一次一密是绝对不可破译的，但它是不实用的。

⑨一次一密给密码设计指出一个方向，人们用序列密码逼近一次一密。

密码学的发展史

- 古代加密方法（手工阶段）
- 古典密码（机械阶段）
- 现代密码（计算机阶段）

现代密码

- 使用者：军队——>普通用户
- 现代密码经历了四个重要的发展时期
  - 1949年以前，现代密码技术的前夜时期
  - 1949年-1975年，密码学发展的神秘时期
  - 1976年-1996年，密码学发展的关键时期
  - 1997年-今，密码学发展的辉煌时期

现代密码

- 计算机的发展使得基于复杂计算的密码成为可能，密码学成为一门新的学科。
  - 1949年信息论之父C. E. Shannon发表了“The Communication Theory of Secret Systems”，密码学走上了科学与理性之路
  - 1967年David Kahn的《The Codebreakers》
  - 1971-73年IBM Watson实验室的Horst Feistel等的几篇技术报告

现代密码

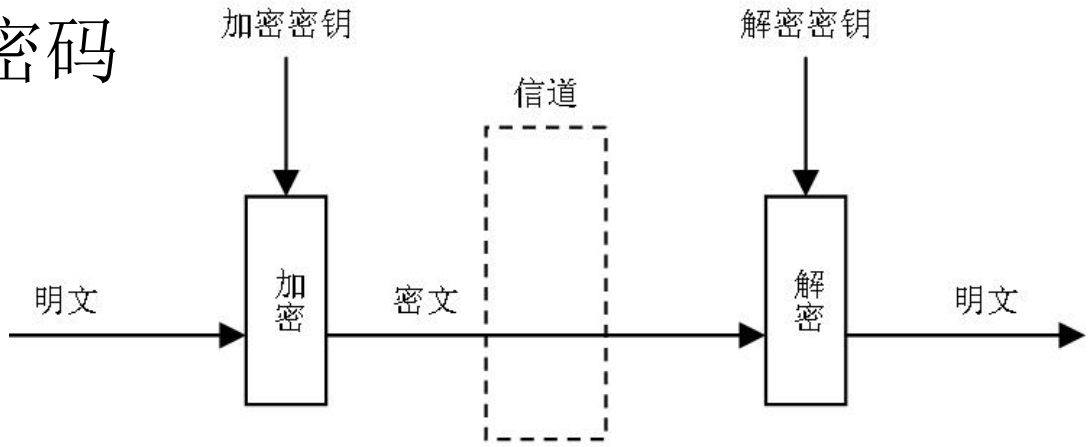
- 对称密钥密码算法进一步发展
  - 1977年DES正式成为标准
  - 80年代出现IDEA,RCx,CAST等
  - 90年代对称密钥密码进一步成熟：Rijndael, RC6, MARS, Twofish, Serpent等出现
  - 2001年Rijndael成为DES的替代者

现代密码

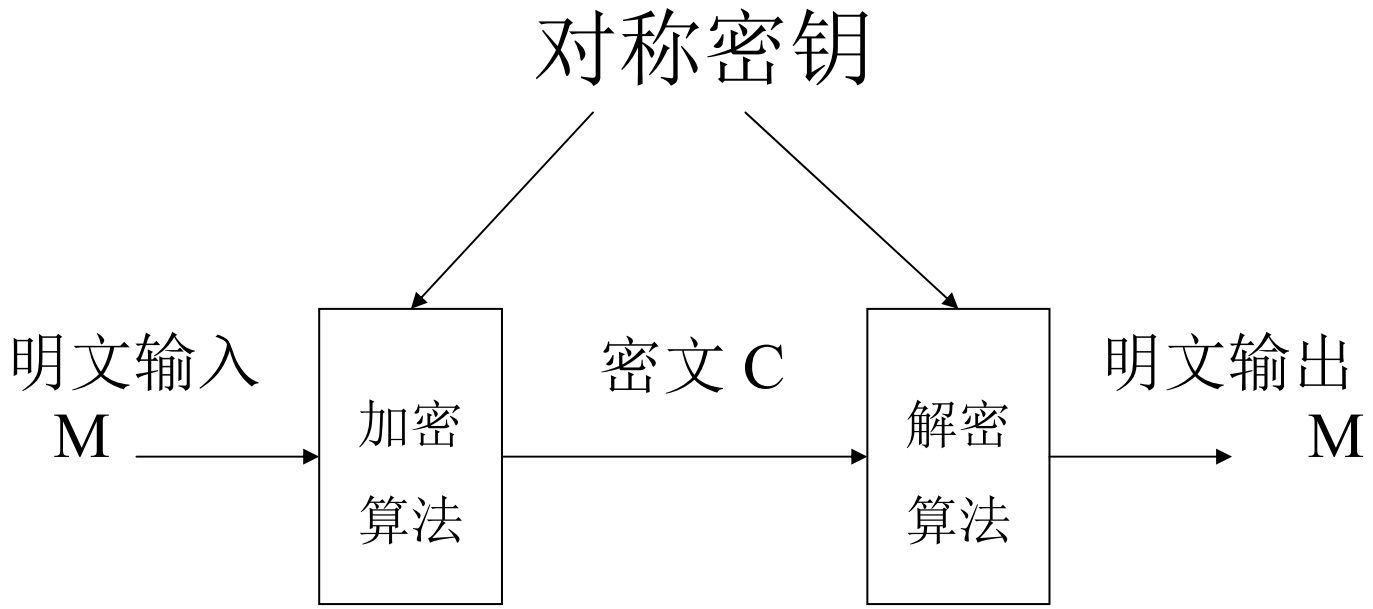
- 公钥密码的出现
  - 1976年Diffie & Hellman的“New Directions in Cryptography”提出了公钥密码思想。
  - 1977年Rivest,Shamir & Adleman提出了RSA公钥算法
  - 90年代逐步出现椭圆曲线等其他公钥算法
  - 一些新的密码技术，如，混沌密码、量子密码等

引言

- 概念
  - 对称密码
  - 分组密码
  - 对称分组密码

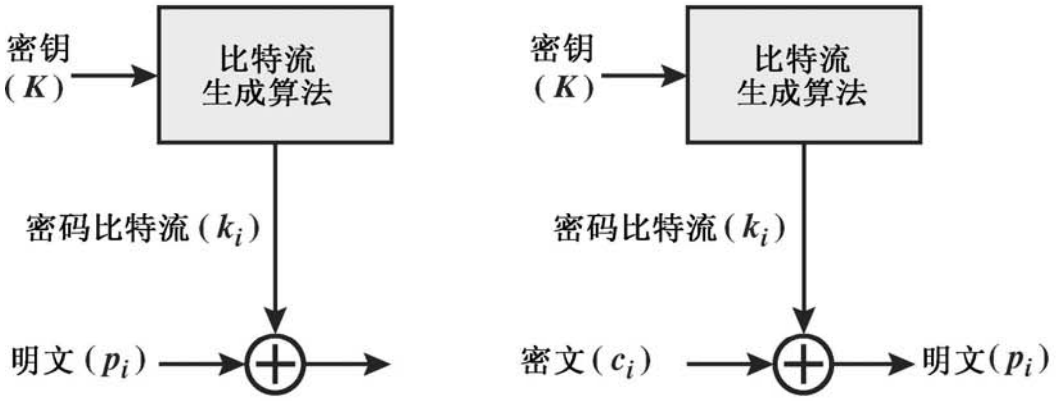


- 加密和解密过程都要使用密钥。如果加密密钥和解密密钥相同或相近，由其中一个很容易地得出另一个，这样的系统称为对称密钥系统，加密和解密密钥都是保密的；如果加密密钥与解密密钥不同，且由其中一个不容易得到另一个，则这种密码系统是非对称密钥系统，往往其中一个密钥是公开的，另一个是保密的。

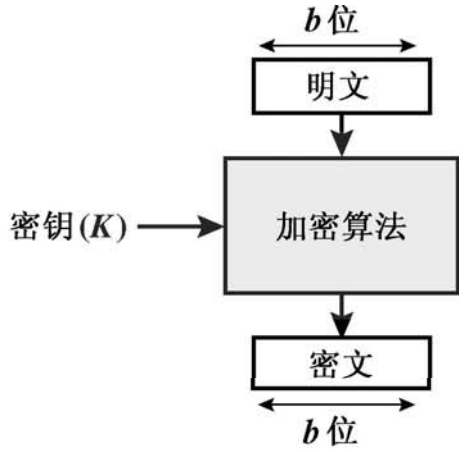


对称加密体制模型

流密码与分组密码的区别



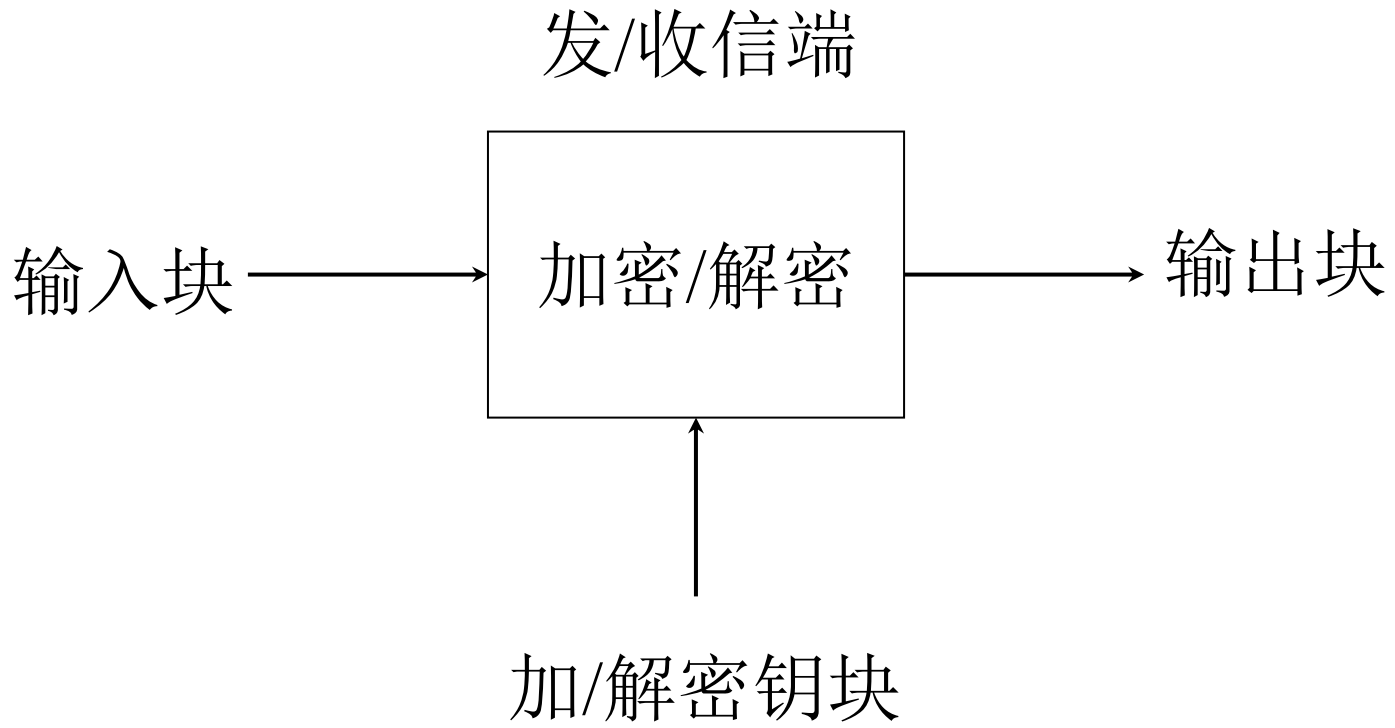
(a) 使用算法比特流发生器的流密码



(b) 分组密码

武漢大学

- 分组密码
  - ✓ 分组密码的加密方式是：首先将明文序列以固定长度进行分组，每组明文用相同的密钥和算法进行变换，得到一组密文。分组密码是以块为单位，在密钥的控制下进行一系列线性和非线性变换而得到密文的。



分组密码

- ✓ 分组密码的加/解密运算是：输出块中的每一位是由输入块的每一位和密钥的每一位共同决定。
- ✓ 加密算法中重复地使用代替(替代)和置换(移位)两种基本的加密变换，此即Shannon 1949年发现的隐藏信息的两种技术：混淆和扩散。

- 混淆(Confusion)：就是改变数据块，使输出位与输入位之间没有明显的统计关系(替代、XOR)；
- 扩散(Diffusion)：就是通过密钥位转移到密文的其它位上(移位)。

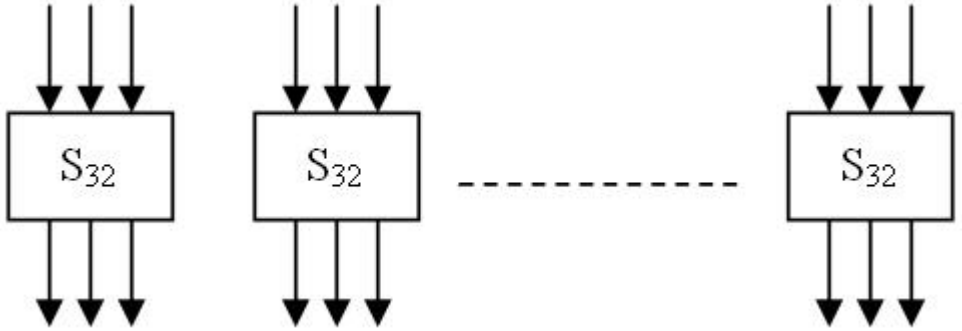
✓ 分组密码的特点：良好的扩散性；对插入信息的敏感性，较强的适应性；加/解密速度慢；差错的扩散和传播。

- 对称分组密码 与 序列密码

	对称分组密码	序列密码
相同点	可以进行加密/解密	
	加密/解密时通常都使用相同的密钥	
	明文与密文一样长	
	速度快	
不同点	对数据采取分段处理	能处理无结构的数据流
	被处理数据之间存在着相关性	被处理数据之间不存在相关性
	能在软件环境中高速实现	较适合于硬件电路实现
	通常应用于商业领域	通常应用于军事领域
	通过在密钥的控制下对明文进行替代和换位来保密	通过将明文与密钥产生的密钥流叠加来保密

原理

- 代替与换位
  - 代替Substitution
    - 在输入一组数据时，输出另一组数据



原理

- 代替与换位
  - 代替Substitution
    - 输入数据与输出数据
      - 未必一样长（压缩，等长，扩展）
      - 未必一一对应（一对一，多对一）

原理

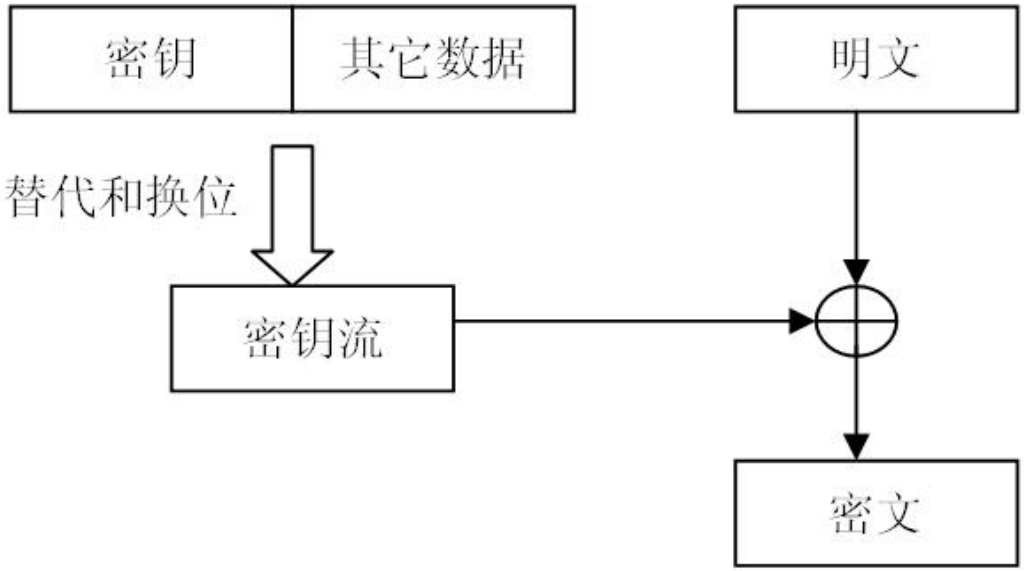
- 代替与换位
  - 代替Substitution
    - 混淆：不同的输入，导致相同的（或者部分相同的）输出
    - 扩散：输入数据中的1bit变化，将导致输出结果中的多bit变化

原理

- 代替与换位
  - 代替Substitution
    - 操作：算术/逻辑运算，非线性映射
    - 由于计算机字长和计算能力的限制，代替所处理的数据宽度很有限，所以在处理长明文块时，需要多个代替模块。
    - 各代替模块之间，没有关联

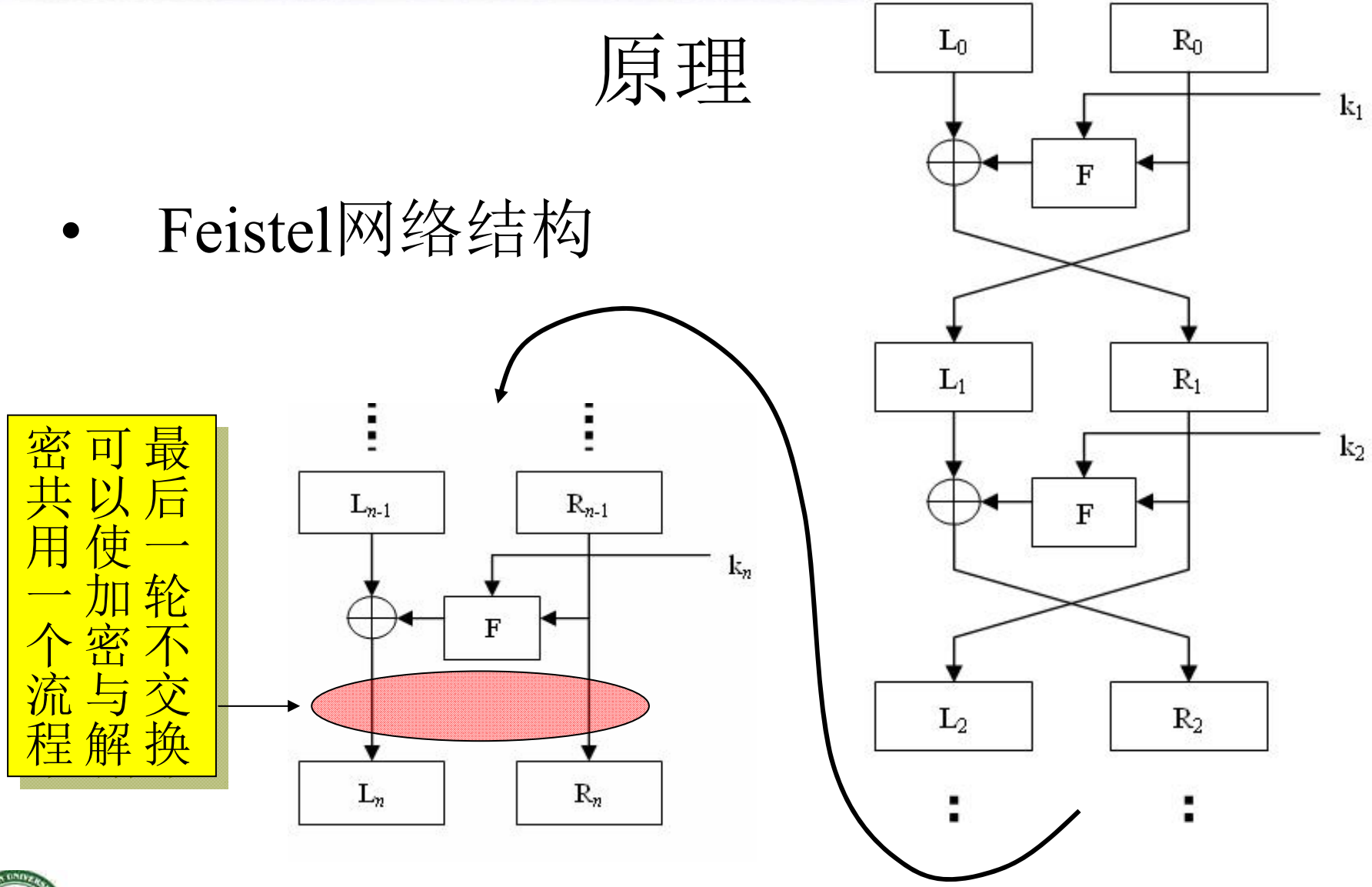
原理

- Feistel网络结构
  - 一次加密
    - 加密
    - 解密



原理

- Feistel网络结构



本讲内容

一、DES概况
二、DES加密过程
三、DES子密钥的产生
四、初始置换IP和IP^{-1}
五、加密函数f
六、 DES解密过程
七、DES的对合性和可逆性
八、DES的安全性
九、3重DES
十、DES的历史回顾

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）

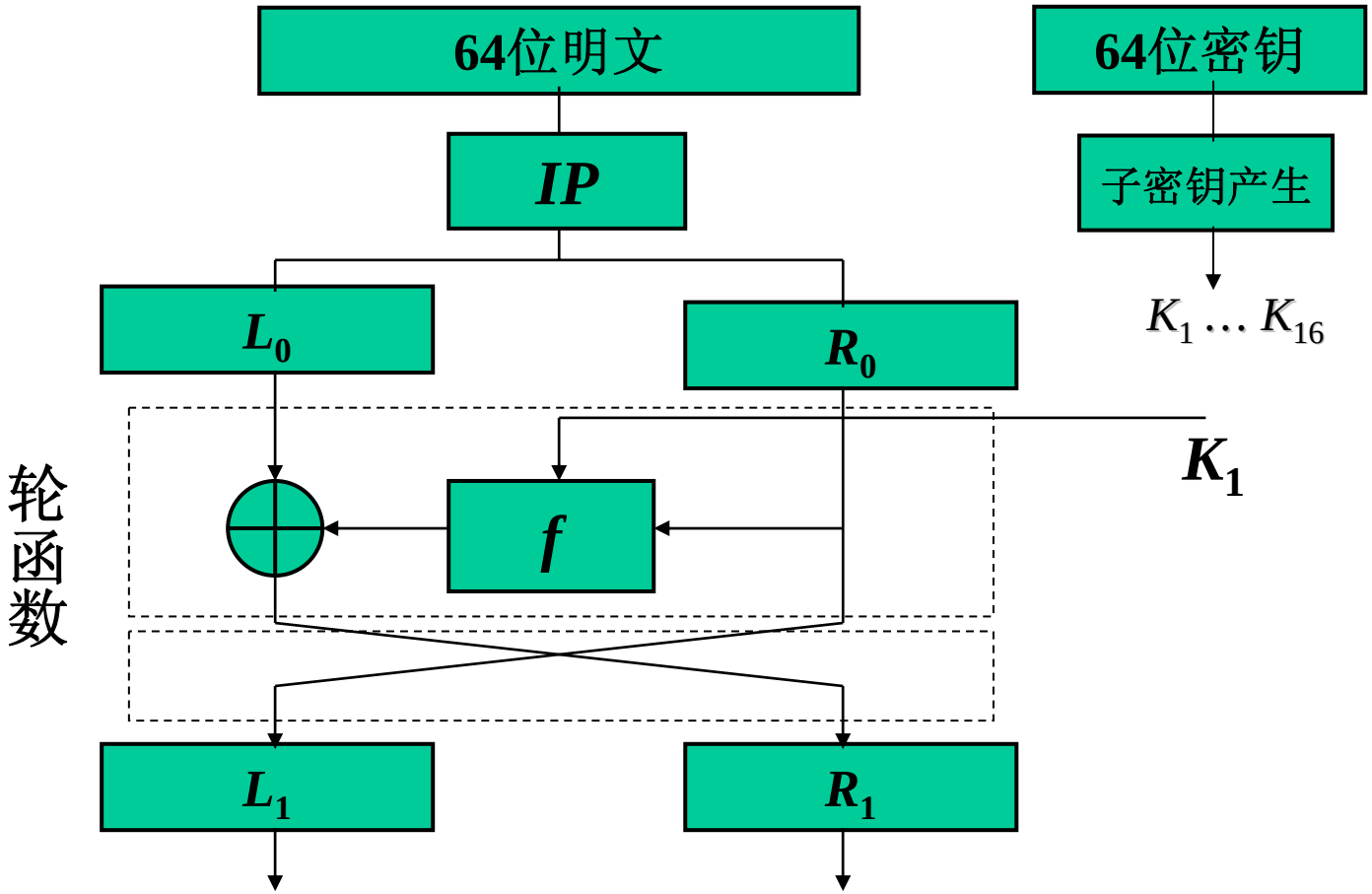
硬件（芯片，插卡，专门设备）

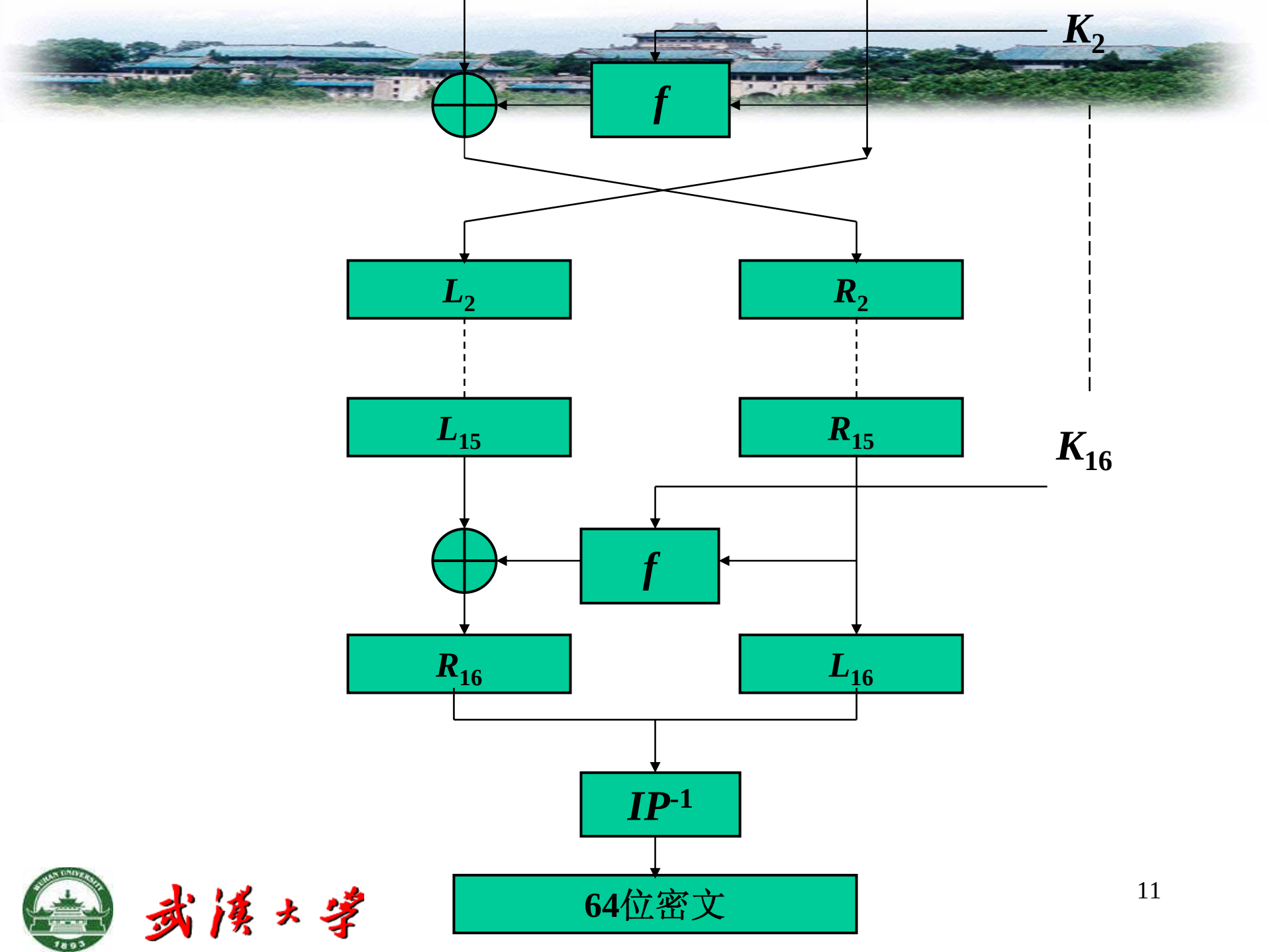
5、结论

- 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加密过程

1、DES算法框图




K_2
f
L_2
R_2
L_{15}
R_{15}
K_{16}
f
R_{16}
L_{16}
IP^{-1}
64位密文

二、DES加密过程

2、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，...，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，再与L_0模2项加：

$$L_0 \oplus f(R_0, K_1)$$

以此作为第二次加密迭代的R_1，以R_0作为L_1。

二、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：

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

三、DES子密钥的产生

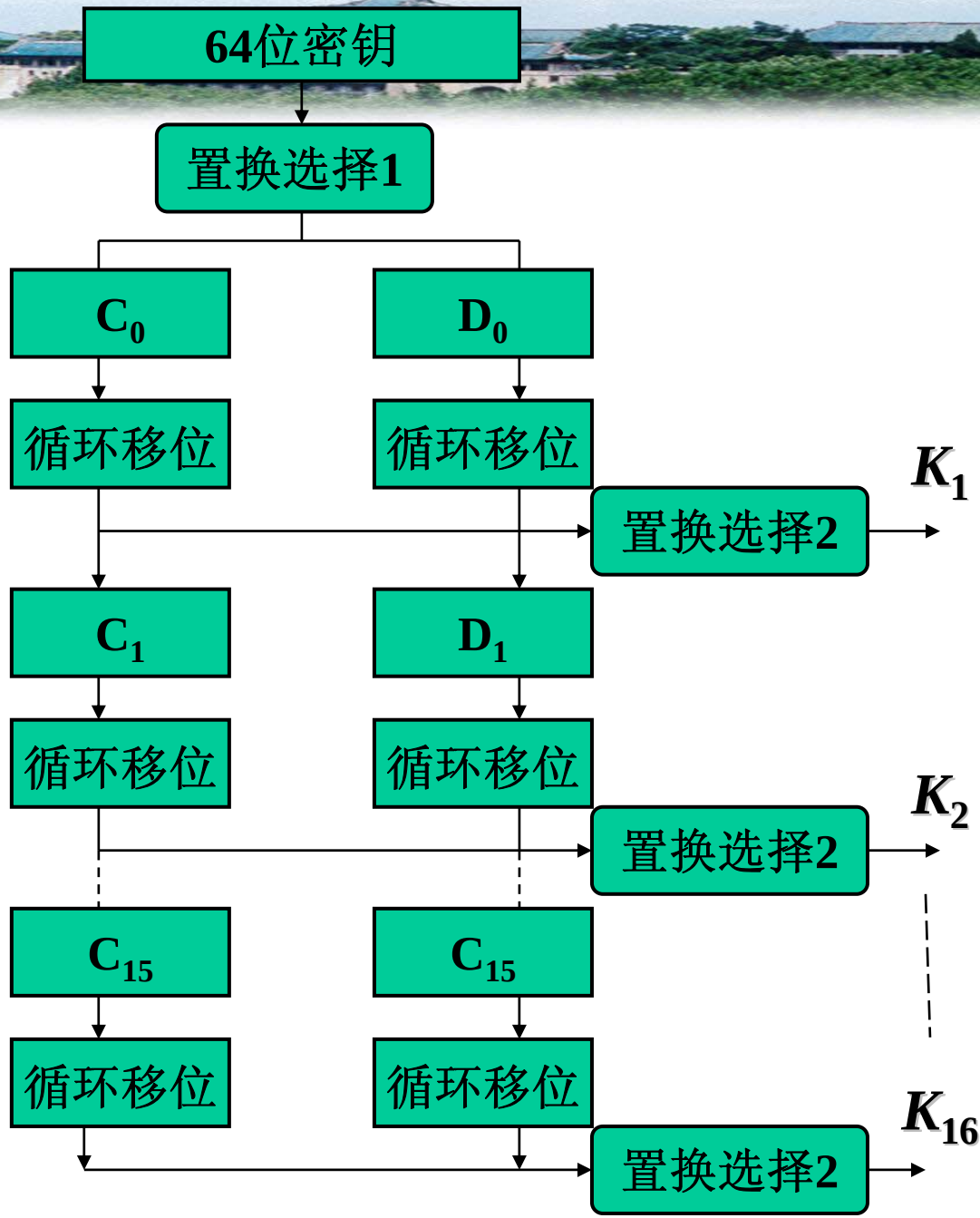
1、功能

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

$$K_1，K_2，\ldots K_{16}$$

分别供各次加密迭代使用。

2. 子密钥产生框图


64位密钥
置换选择1
C_0
D_0
循环移位
循环移位
置换选择2
K_1
C_1
D_1
循环移位
循环移位
置换选择2
K_2
C_{15}
C_{15}
循环移位
循环移位
置换选择2
K_{16}

三、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。

三、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

三、DES子密钥的产生

5、置换选择2：

①、作用

- 从C_i 和 D_i (56位)中选择出一个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	
41	52	31	37	47	55	30	40	51	45	33	48	D_i
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

四、初始置换IP和IP^{-1}

1、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。

四、初始置换IP和IP^{-1}

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

四、初始置换IP和IP^{-1}

2、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

四、初始置换IP和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：

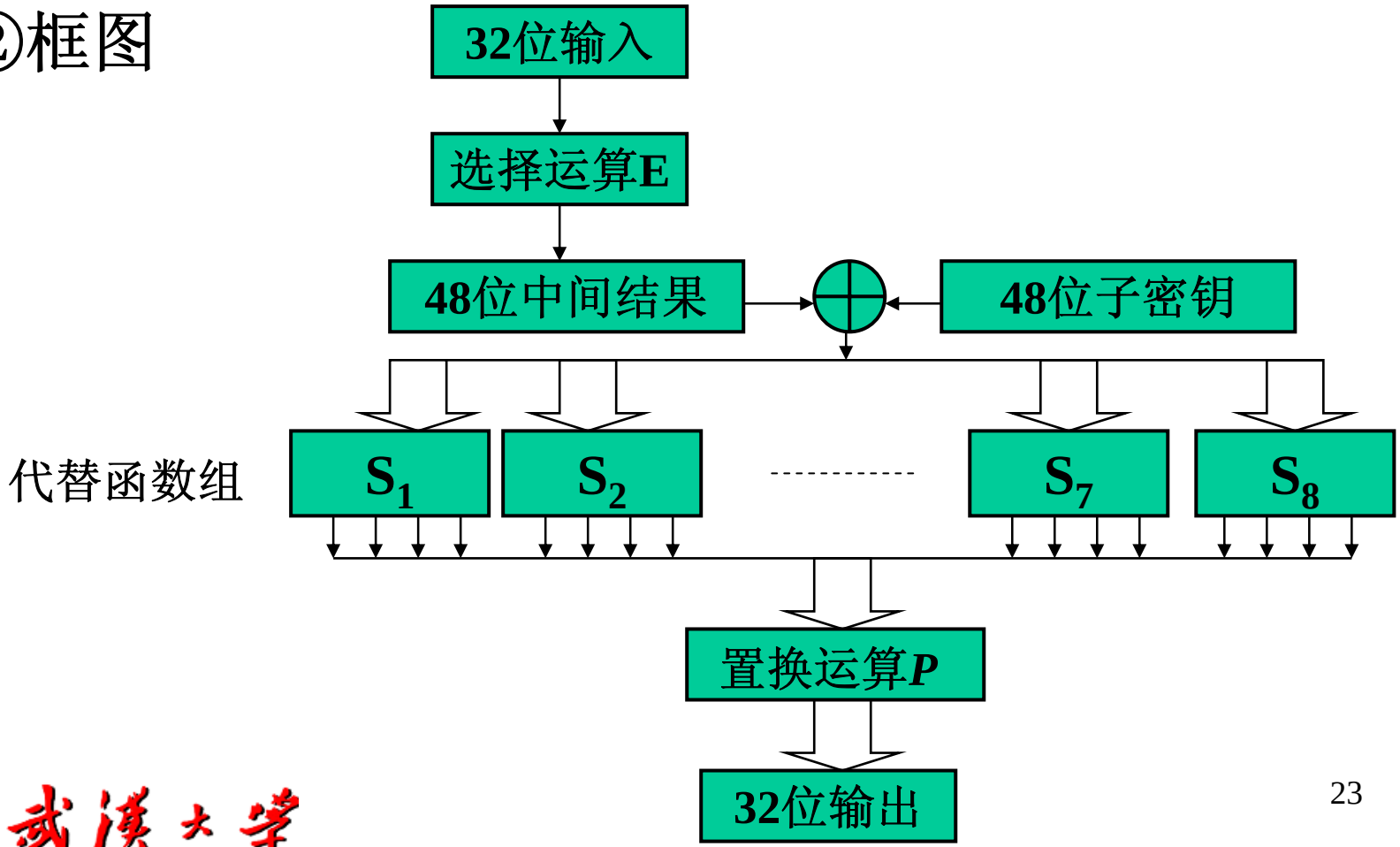
- 由于IP中的置换是规律的
- 所以IP^{-1}中的置换也是规律的
- 这对保密是不利的

五、加密函数 *f*

①作用

■ DES的轮函数，DES保密的核心。

②框图



五、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

五、加密函数 f

④代替函数组S（S盒）

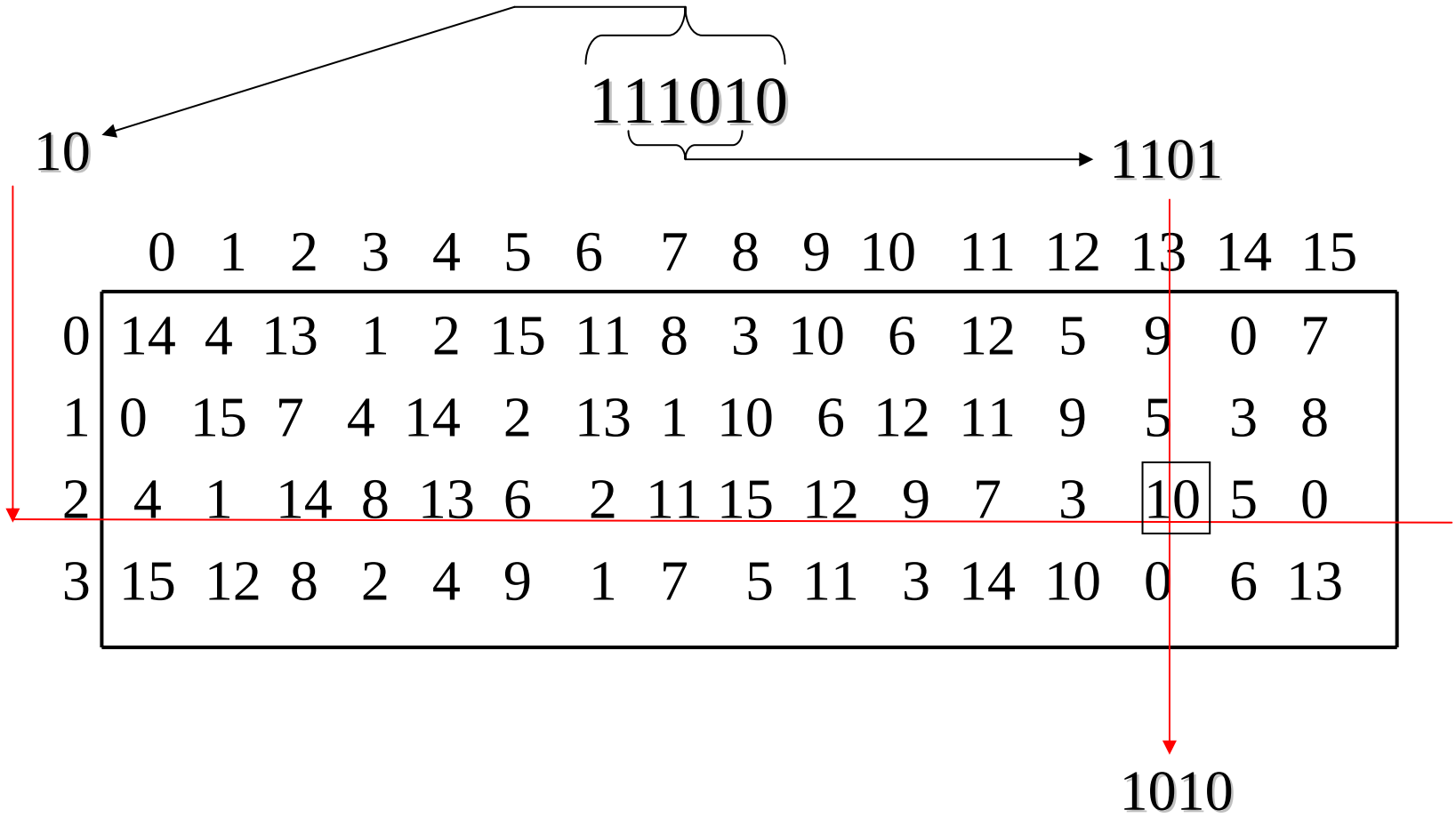
- S 盒的一般性质
  - ■S盒是DES中唯一的非线性变换，是DES安全的关键。
  - ■在保密性方面，起混淆作用。
  - ■共有8个S盒，并行作用。
  - ■每个S盒有6个输入，4个输出，是非线性压缩变换。
  - ■设输入为$b_1b_2b_3b_4b_5b_6$,则以b_1b_6组成的二进制数为行号，$b_2b_3b_4b_5$组成的二进制数为列号。行列交点处的数（二进制）为输出。

五、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

五、加密函数 f


111010
10
1101
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
1010

五、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⊕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∈{0,1},有 S(x)≠S(x⊕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。

五、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盒必须有足够的代线次数和项数，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！**

五、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

六、DES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：

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

七、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：

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

- 计算：$TT(L, R) = T^2(L, R) = (L, R) = I$，其中$I$为恒等变换。
- 因为$T^2 = I$，所以有

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

所以T变换是对合运算。

七、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

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

- $F_i^2 = F_i(L_{i-1} \oplus f(R_{i-1}, K_i), R_{i-1})$

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

$$= (L_{i-1}, R_{i-1})$$

$$= I$$

所以，$F_i = F_i^{-1}$ 。

- 所以 F_i 变换也是对合运算。

七、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（TT）F_i）= $F_i F_i = I$ ，
- 所以

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

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

七、DES的对合性和可逆性

1、可逆性证明

④加解密表示

(1) $DES(M) = (M)\,IP\,(F_1T)\,(F_2T)\ldots(F_{15}T)\,(F_{16})\,IP^{-1} = C$

(2) $DES^{-1}(C) = (C)\,IP\,(F_{16}T)\,(F_{15}T)\ldots(F_2T)\,(F_1)\,IP^{-1} = M$

- 把（1）式代入（2）式可证：

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

- 所以，DES是可逆的。

七、DES的对合性和可逆性

2、对合性证明

$$DES = IP\,(F_1T)\,(F_2T)\,\ldots\,(F_{15}\,T)\,(F_{16})\,IP^{-1}$$

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

- 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：

$$DES = IP\,(F)\,(TF)\,(TF)\ldots(TF)\,(TF)\,(TF)\,IP^{-1}$$

$$DES^{-1} = IP\,(F)\,(TF)\,(TF)\ldots(TF)\,(TF)\,(TF)\,IP^{-1}$$

- 显然：$DES = DES^{-1}$
- 所以DES的运算是对合运算。

八、DES的安全性

①攻击

- 穷举攻击。这是目前最有效的方法。
- 差分攻击。
- 线性攻击。

②安全弱点

- 密钥太短。这是最主要的弱点。
- 存在弱密钥。
- 存在互补对称性。

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

九、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。

九、3重DES

② 3DES的优势：

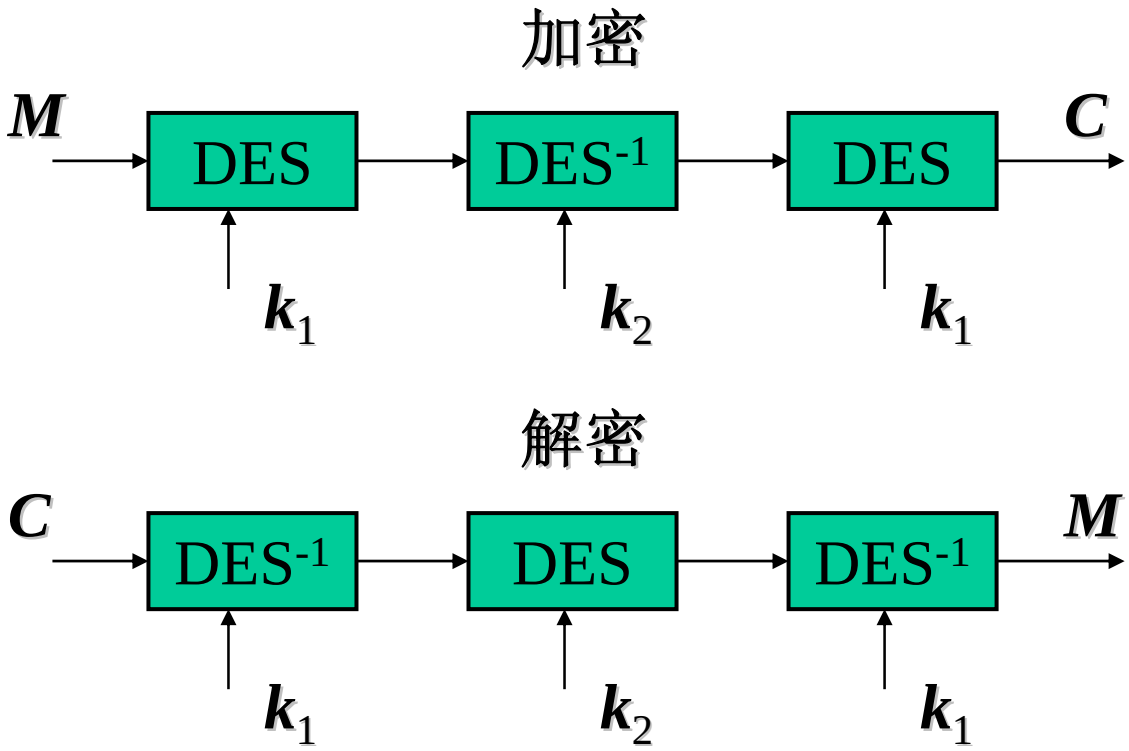
- 3密钥的3DES：密钥长度是168位。
- 2密钥的3DES：密钥长度是112位。
- 安全：密钥足够长；
  经过最充分的分析和实践检验。
- 兼容性好。

③ 3DES的弱势：

- 速度慢。

九、3重DES

④2密钥3DES框图



EES算法

- 密钥托管加密标准EES（Escrowed Encryption Stantard）
  - 1984年美国政府着手设计EES算法取代DES
  - DES作为世界标准，全世界的众矢之的
  - DES的密钥太短

- NSA密码政策的改变
  - 政府认为加密算法应当设计成“双刃剑”
  - 商界认为政府应当公布密码算法，否则侵犯公民的隐私权 。

武漢大学

EES算法

- **CLIPPER密码芯片的概况**
  - 密码算法称为SKIPJACK，属于分组密码，明文和密文分组长度为64位，密钥长度为80位。
  - 算法采用轮函数迭代结构，共迭代32圈。
- CLIPPER密码使用三个密钥参数：
  - *FK* 族密钥（Family Key），又称为法律监督密钥，80位，所有芯片均相同。
  - *SN* 芯片序列号(Serial Number)，30位，长度可变，对芯片来说是唯一的。
  - *UK* 单元密钥(Unit Key)，80位，它是芯片的有效密钥，各芯片不同

EES算法

- SKIPJACK算法的密钥长度为80位，比DES的56位多24位，其密钥空间为$2^{80} \approx 1 \cdot 2 \times 10^{24}$，根据目前的计算技术水平，可以抵抗穷举攻击。
- SKIPJACK算法抗差分攻击和线性攻击的能力也很强。
- SKIPJACK的子密钥生成算法过于简单，经过5轮加密迭代后将重复使用相同的子密钥，这显然是对安全不利的。
- 从加解密轮函数的结构可知，SKIPJACK适合16位CPU的软件实现，不太适合32位CPU实现。
- SKIPJACK算法不是对合运算，加解密要使用不同的运算，这对工程实现是不利的。
- 该算法由于安全性和公开性问题，已被AES/3-DES取代。

十、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代表当时商用密码的最高水平，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
  - 商用密码应当坚持公开设计原则；
  - 商用密码标准应当公布算法。

谢　谢！