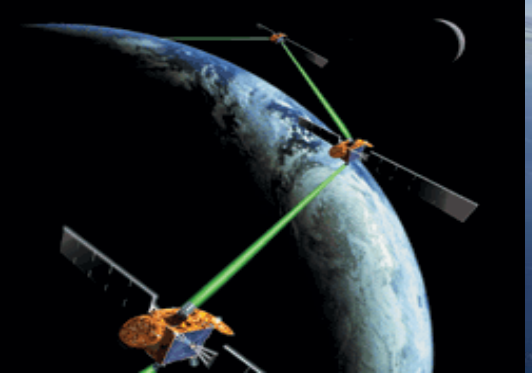
普通高等教育“十一五”国家级规划教材
教育部2011年精品教材

网络安全—技术与实践（第2版）

刘建伟 王育民 编著

清华大学出版社




课件制作人声明

- 本课件总共有17个文件，版权属于刘建伟所有，仅供选用此教材的教师和学生参考。
- 本课件严禁其他人员自行出版销售，或未经作者允许用作其他社会上的培训课程。
- 对于课件中出现的缺点和错误，欢迎读者提出宝贵意见，以便及时修订。

课件制作人：刘建伟

2016年04月05日

单钥加密体制（第1讲）

一 基本概念

二 密码分析

三 密码学历史

四 古典密码

五 传统密码学（对称算法）

六 DES数据加密标准

单钥加密体制（第1讲）

一 基本概念

二 密码分析

三 密码学历史

四 古典密码

五 传统密码学（对称算法）

六 DES数据加密标准

一、密码学基本概念

明文	需要秘密传送的消息。
密文	明文经过密码变换后的消息。
加密	由明文到密文的变换
解密	从密文恢复出明文的过程。
破译	对明文进行加密时采用的一组规则。
加密算法	对密文进行解密时采用的一组规则。
解密算法	从密文恢复出明文的过程。
密钥	加密和解密时使用的一组秘密信息。

一、密码学基本概念

1、密码系统组成

一个密码系统可以用以下数学符号描述：

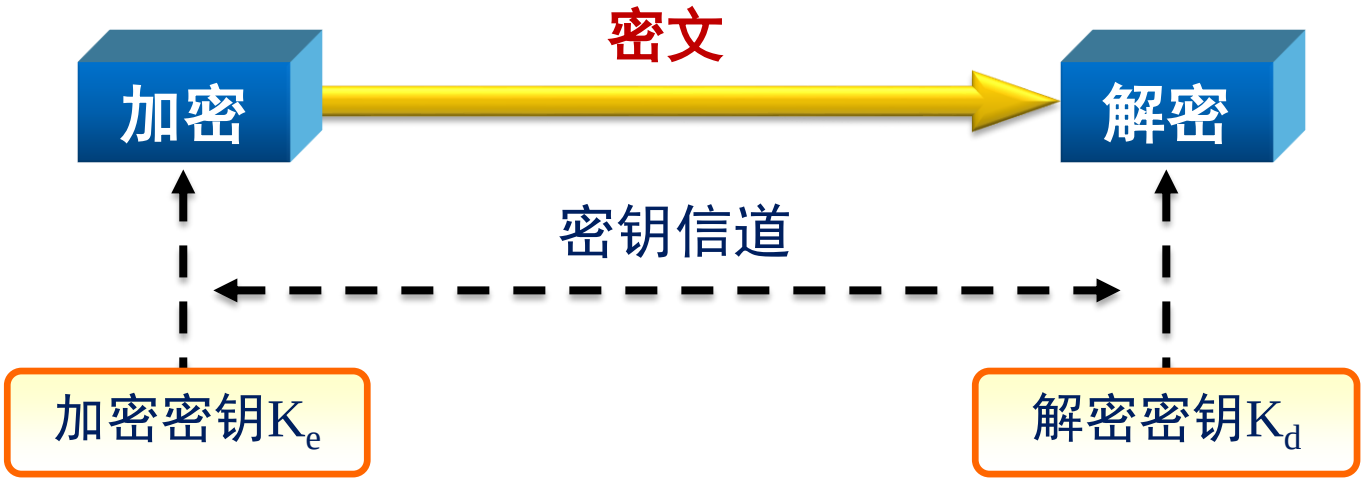
- $S = \{M, C, K, E, D\}$
- 明文消息空间M：由字母、数字组成的串集
- 密文消息空间C：可能的密文消息集
- 密钥生成算法ζ：$N \rightarrow K \times K'$
- 加密密钥空间K：可能的加密密钥集
- 解密密钥空间K'：可能的解密密钥集
- 加密算法E：$M \times K \rightarrow C$
- 解密算法D：$C \times K' \rightarrow M$
- $\forall$整数$1^l, \zeta(1^l)$输出长为l的密钥对$(k_e, k_d) \in K \times K'$
- $\forall m \in M, c \in C$

  $c = E_{ke}(m)$

  $m = D_{kd}(c) = D_{kd}(E_{ke}(m))$

一、密码学基本概念

2、密码体制的分类



- 若$k_e=k_d$，则加密算法称为：单钥体制（对称加密体制，或私钥加密体制）；
- 若$k_e \neq k_d$，则加密算法称为双钥体制（非对称加密体制，或公钥加密体制）。

一、密码学基本概念

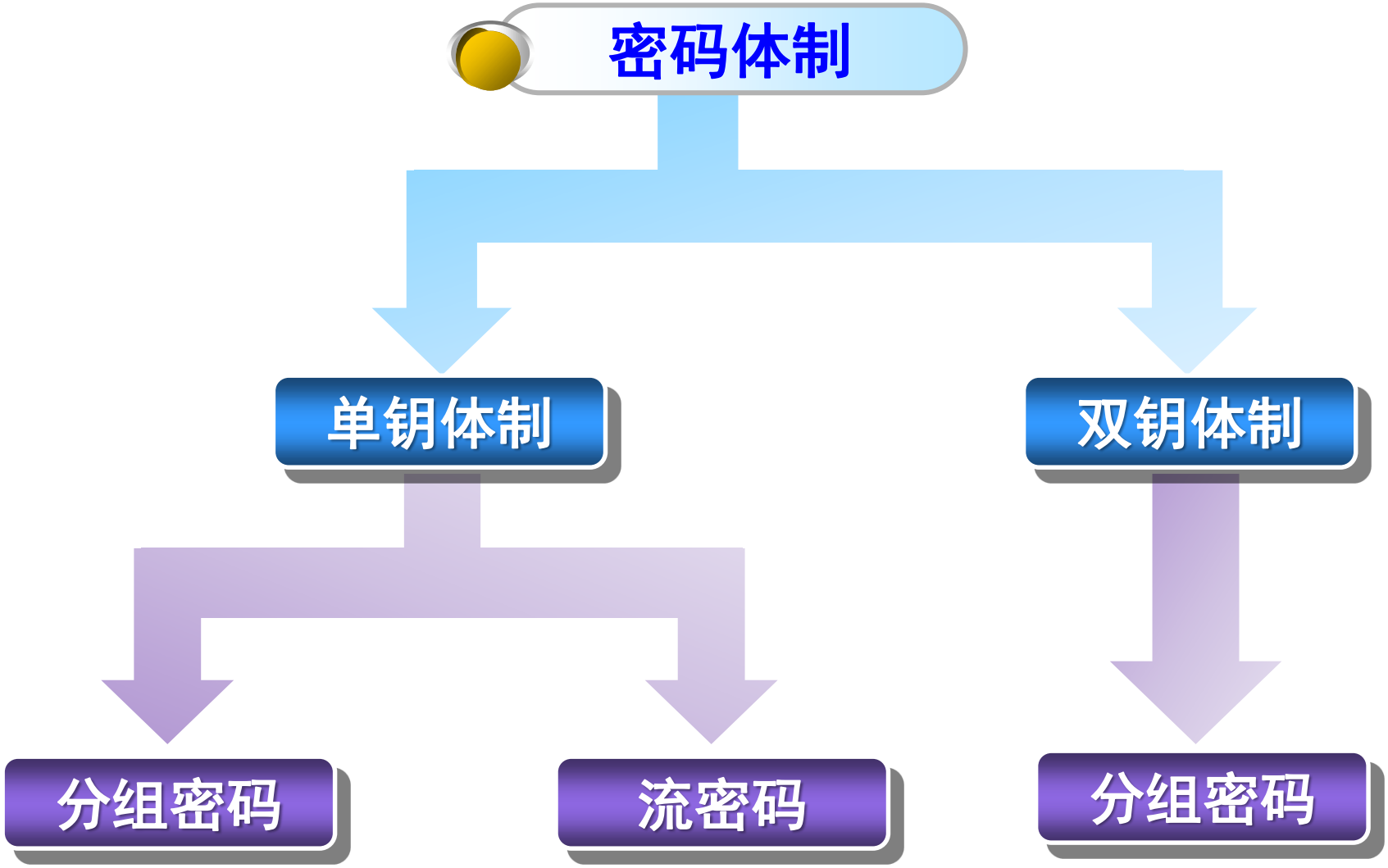
3、单钥体制的分类

- 对于单钥加密体制，可以按照其加密/解密运算的特点，分为流密码（Stream Cipher）和分组密码（Block Cipher）

流密码：数据逐比特加密，即数据流与密钥流逐比特进行异或（XOR）运算；

分组密码：对数据分组进行处理。

密码学基本概念小结



单钥加密体制（第1讲）

一 基本概念

二 密码分析

三 密码学历史

四 古典密码

五 传统密码学（对称算法）

六 DES数据加密标准

二、密码分析（破译）

- 试图破译单条消息
- 试图识别加密的消息格式，以便借助直接的解密算法破译后续的消息
- 试图找到加密算法中的普遍缺陷（无须截取任何消息）

二、密码分析（破译）

1、密码分析的条件与工具

- 已知加密算法
- 语言特性
- 计算机
- 截取到明文、密文中已知或推测的数据项
- 数学或统计工具和技术
- 技巧与运气

二、密码分析（破译）

2、密码分析类型

攻击类型	密码破译者已知的东西
唯密文	● 加密算法 ● 待破译的密文
已知明文	● 加密算法 ● 待破译的密文 ● 由密钥形成的一个或多个明文－密文对
选择明文	● 加密算法 ● 待破译的密文 ● 由破译者选择的明文消息，连同对应的由密钥生成的密文
选择密文	● 加密算法 ● 待破译的密文 ● 由破译者选择的猜测性密文，连同它对应的由密钥生成的已破译明文
选择文本	● 加密算法 ● 待破译的密文 ● 由破译者选择的明文消息，连同对应的由密钥生成的密文 ● 由破译者选择的猜测性密文，连同它对应的由密钥生成的已破译明文

二、密码分析（破译）

3、加密方案的安全性

- **无条件安全：**无论提供多少密文，若密文中所包含的信息不足以唯一地决定对应的明文，那么该密码体制就是无条件安全的。
- 除了一次一密(one-time padding)的方案外，没有无条件安全的其他算法。

安全性体现在

- 破译的成本超过加密信息的价值
- 破译的时间超过该信息有用的生命周期

二、密码分析（破译）

4、攻击的复杂性决定了密码算法的安全性

数据复杂性（data complexity）	用作攻击输入所需要的数据
处理复杂性（processing complexity）	完成攻击所需要的时间
存储需求（storage requirement）	进行攻击所需要的数据量

二、密码分析（破译）

5、密钥搜索所需平均时间

密钥长度 (bit)	密钥数量	每微秒加密1次所需时间	每微秒加密100万次所需时间
32	$2^{32}=4.3\times10^{9}$	2^{31}us=35.8 minutes	2.15ms
56	$2^{56}=7.2\times10^{16}$	2^{55}us=1142years	10.01 hours
128	$2^{128}=3.4\times10^{38}$	2^{127}us=5.4×10^{24} years	5.4×10^{18}years
26 characters (permutation)	$26!=4\times10^{26}$	2×10^{26}us=6.4×10^{12} years	6.4×10^{6}years

二、密码分析（破译）

6、常用对称加密算法

DES：第一代数据加密标准，因密钥长度太短已经弃用。

3DES：对数据用三个不同的密钥进行三次加密，强度更高。

AES：下一代的加密算法标准，速度快，安全级别高。

AES与3DES的比较

算法名称	算法类型	密钥长度	速度	解密时间（每秒尝试255个密钥）	资源消耗
AES	对称block密码	128、192、256位	高	1490000亿年	低
3DES	对称feistel密码	112位或168位	低	46亿年	中

二、密码分析（破译）

7、常用非对称加密算法

RSA：基于大整数因子分解问题的公钥密码算法

ECC：基于椭圆曲线上离散对数计算问题的公钥密码算法

RSA与ECC的安全性和速度比较

攻破时间（MIPS年）	RSA密钥长度	ECC密钥长度	RSA/ECC密钥长度比
10^4	512	106	5:1
10^8	768	132	6:1
10^{11}	1024	160	7:1
10^{20}	2048	210	10:1
10^{78}	21000	600	35:1

单钥加密体制（第1讲）

一 基本概念

二 密码分析

三 密码学历史

四 古典密码

五 传统密码学（对称算法）

六 DES数据加密标准

三、密码学的历史

- 密码学的演进

单表代替—>多表代替—>机械密(恩格玛)—>现代密码学(对称与非对称密码体制)—>量子密码学

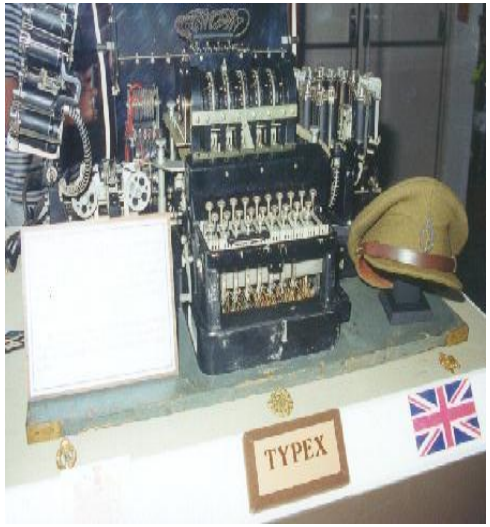
- 密码编码学和密码分析学
- 应用领域
- 军事、外交、商业、通信。

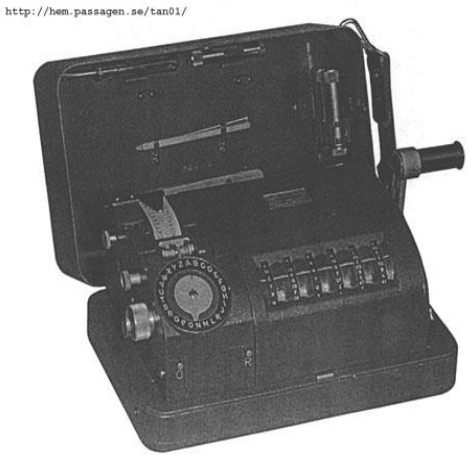
三、密码学的历史

Phaistos圆盘，一种直径约为160mm的Cretan-Mnoan粘土圆盘，始于公元前17世纪。表面有明显字间空格的字母，至今还没有破解。

三、密码学的历史

20世纪早期密码机





单钥加密体制（第一讲）

一 基本概念

二 密码分析

三 密码学历史

四 古典密码

五 传统密码学（对称算法）

六 DES数据加密标准

四、古典密码

1、古典密码学

- 已经成为历史，但被传统密码学所借鉴；
- 加解密都很简单，易被攻破；
- 属于对称密码体制；
- 包括置换密码、单表代换密码、多表代换密码等。

四、古典密码

2、古典密码的种类

- 置换密码
  - 用加密置换去对消息进行加密
- 代换密码
  - 明文中的字母用相应的密文字母进行替换
  - 单表代换密码
  - 多表代换密码
- 多表密码

四、古典密码

3、古典密码——代换密码

- 单表代换密码举例

明文：a b c d e f g h i j k l m n o p q r s t u v w x y z

密文：D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

- m = “Caser cipher is a shift substitution”
- c = “FDVHU FLSHU LV D VKLIW VXEVWLW XWLRO”

四、古典密码

4、古典密码——置换密码

- 用加密置换去对消息进行加密
- 举例：
  - E =（1，2，3，4）
  - D =（2，1，4，3）
  - M =“置换密码”
  - C = E(M) = “换置码密”

四、古典密码

5、古典密码——多表密码

维吉尼亚密码是多表密码中最知名的密码。令密钥串是gold，利用编码规则A=0, B=1, C=2, …, Z=25。这个密钥串的数字表示是: (6, 14, 11, 3)。设明文为：proceed meeting as agreed

15	17	14	2	4	4	3	12	4	4	19
6	14	11	3	6	14	11	3	6	14	11
21	5	25	5	10	18	14	15	10	18	4

8	13	6	0	18	0	6	17	4	4	3
3	6	14	11	3	6	14	11	3	6	14
11	19	20	11	21	6	20	2	7	10	17

密文为：vfzfkso pkseltu guchkr

注意：模数=26

单钥加密体制（第一讲）

一 基本概念

二 密码分析

三 密码学历史

四 古典密码

五 单钥密码体制（对称加密体制）

六 DES数据加密标准

五、单钥密码体制（对称加密体制）

1、对称加密体制

- 历史悠久，最古老与最现代的密码学
- 基本特点：加密和解密采用同一个密钥，所以又被称为对称密码体制。

let C = Cipher text, P = Plain text, k is key, E( )/D( ) is the encryption/decryption function, then

$$C=E(P, k),\ P=D(C, k)$$

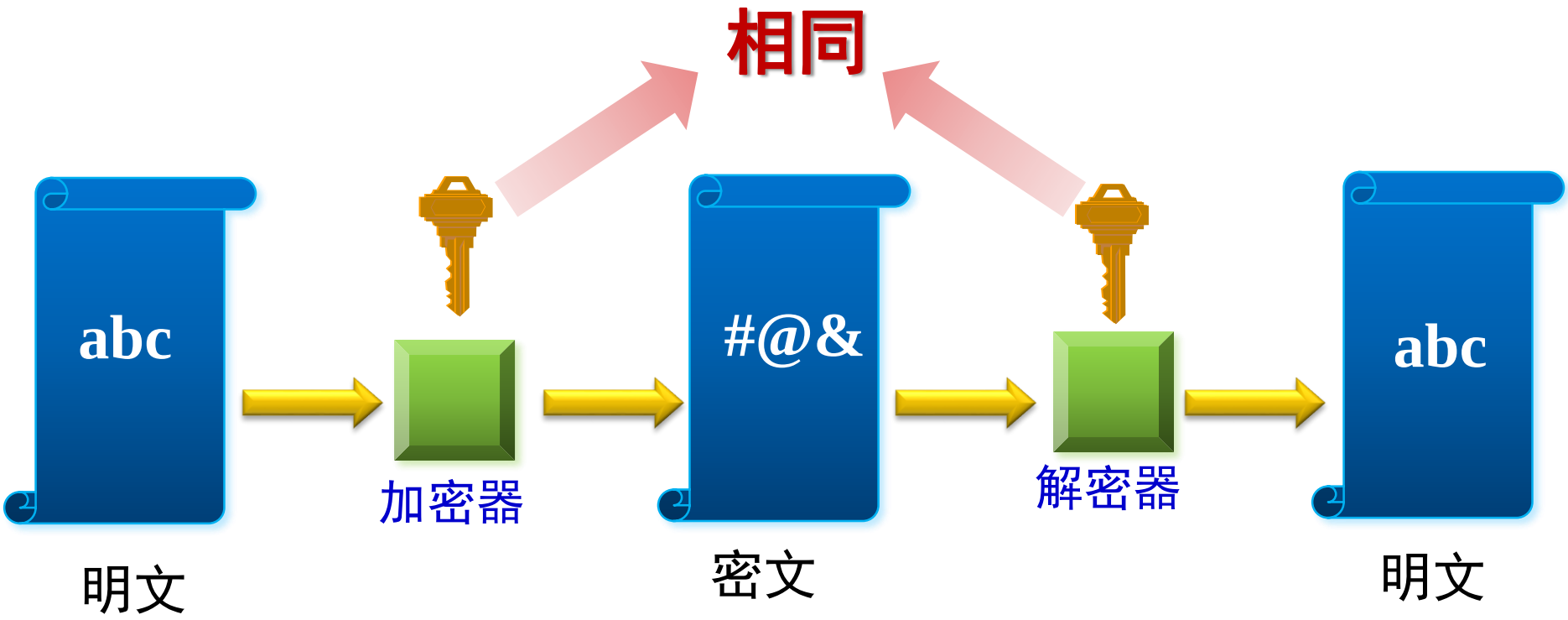
- 基本技术

  替换、置换和移位

五、单钥密码体制（对称加密体制）

2、对称密钥体制的加密过程

对称密码技术又称单钥密码技术，即同用一个密钥去加密和解密数据。



五、单钥密码体制（对称加密体制）

3、对称密钥体制中的密钥管理

单钥密码技术要求通信双方事先交换密钥。在实际应用中，商户需要与成千上万的购物者进行交易，若采用单钥密码技术，商户需要管理成千上万个不同对象通信的密钥。

双方如何交换密钥。通过传统手段，还是通过因特网，都会遇到密钥传送的安全性问题。

在现实环境中，密钥通常会经常更换，更为极端的是，每次传送都使用不同的密钥，单钥密码技术的密钥管理和发布都是远远无法满足使用要求的

五、单钥密码体制（对称加密体制）

4、对称算法设计标准

- 算法必须提供较高的安全性；
- 算法必须完全确定且易于理解；
- 算法的安全性必须依赖于密钥，而不应依赖于算法；
- 算法必须对所有用户都用效。

- 算法必须适用于各种应用；
- 用以实现算法的电子器件必须很经济；
- 算法必须能有效使用；
- 算法必须是可逆的运算。

单钥加密体制（第1讲）

一 基本概念

二 密码分析

三 密码学历史

四 古典密码

五 传统密码学（对称算法）

六 DES数据加密标准

六、DES数据加密标准

1、Shannon的密码设计思想

- 扩散(diffusion)

将明文及密钥的影响尽可能迅速地散布到较多个输出的密文中（将明文冗余度分散到密文中）。产生扩散的最简单方法是通过**“置换(Permutation)”**（比如：重新排列字符）。

- 混淆(confusion)

其目的在于使作用于明文的密钥和密文之间的关系复杂化，是明文和密文之间、密文和密钥之间的统计相关特性极小化，从而使统计分析攻击不能奏效。通常的方法是**“代换（Substitution)”**。

六、DES数据加密标准

2、分组密码的设计要求

1. 分组长度足够大（≥128~256比特）
2. 密钥量要足够大（≥128~192~256比特）
3. 算法足够复杂（包括子密钥产生算法）
4. 加密、解密算法简单，易软、硬件实现
5. 便于分析（破译是困难的，但算法却简洁清晰）

六、DES数据加密标准

3、分组密码——DES数据加密标准

- 数据加密标准（Data Encryption Standard），40年历史；
- DES是一种对称密码算法，源自IBM公司于1970年开发的Lucifer算法， 1976年11月23日DES被采纳为美国联邦标准；
- DES是第一个得到广泛应用的密码算法，满足对合特性；
- DES是一种分组加密算法，输入的明文分组长度为64位，密钥为56位，生成的密文分组长度为64位；

六、DES数据加密标准

DES的运算共有3个

1、对输入分组进行固定的“初始置换”IP运算，可以将这个置换表示为：$(L_0, R_0) \leftarrow IP(InputBlock)$

注意：这里L_0和R_0称为左、右半分组，各为32比特。IP是固定的、公开的函数。上述这个过程实际上为“扩散（ Diffusion ）”。

2、迭代运算，即将下面的运算迭代16轮：

$$L_i \leftarrow R_{i-1}$$
$$R_i \leftarrow L_{i-1} \oplus f(R_{i-1}, k_i)$$

注意：这个过程就是香农信息论中的“混淆（Confusion）”。

六、DES数据加密标准

3、将16轮迭代后得到的结果（L16, R16）输入到IP的逆置换IP^{-1}中：

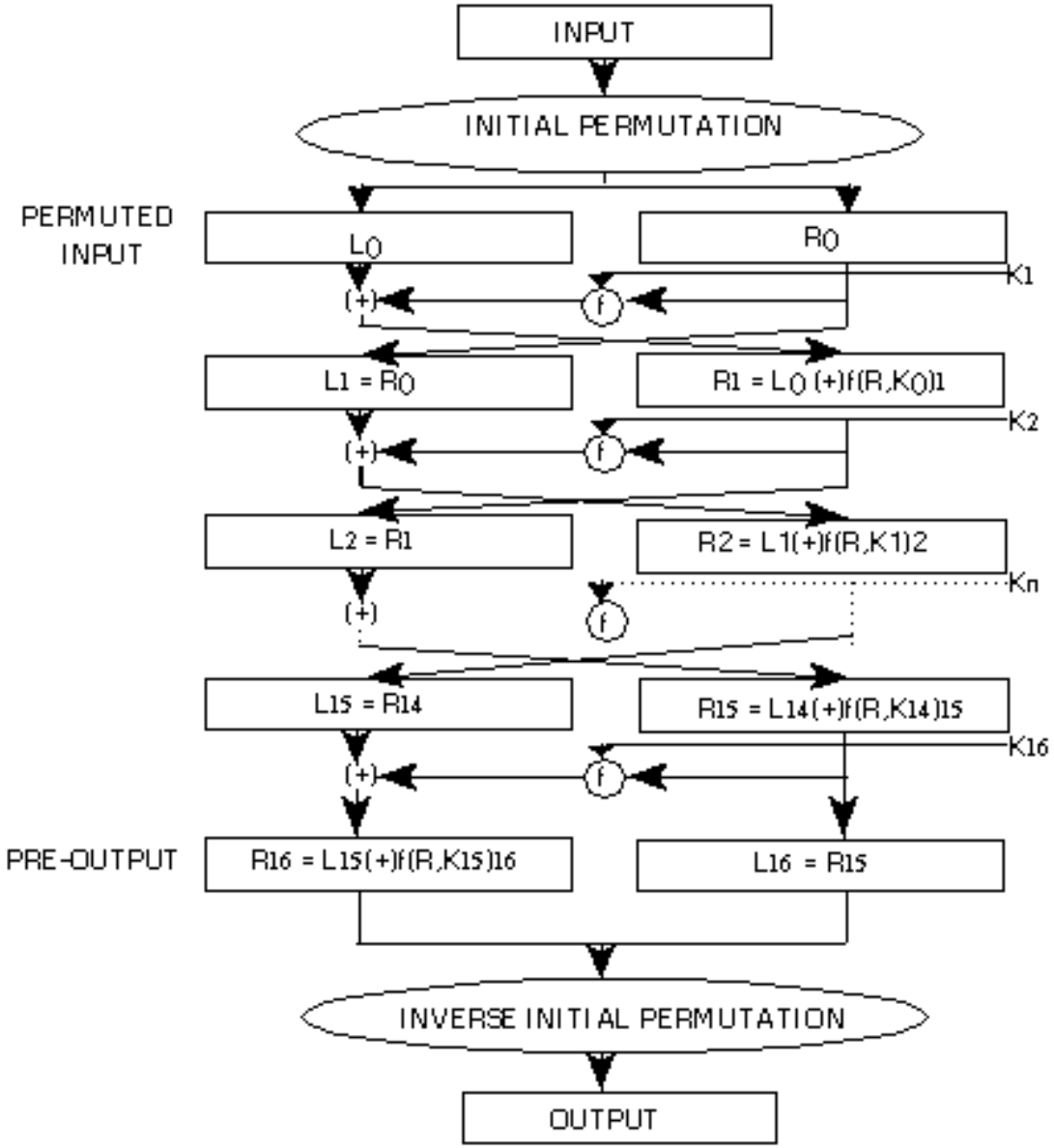
$$OutputBlock \leftarrow IP^{-1}(R_{16}, L_{16})$$

注意：

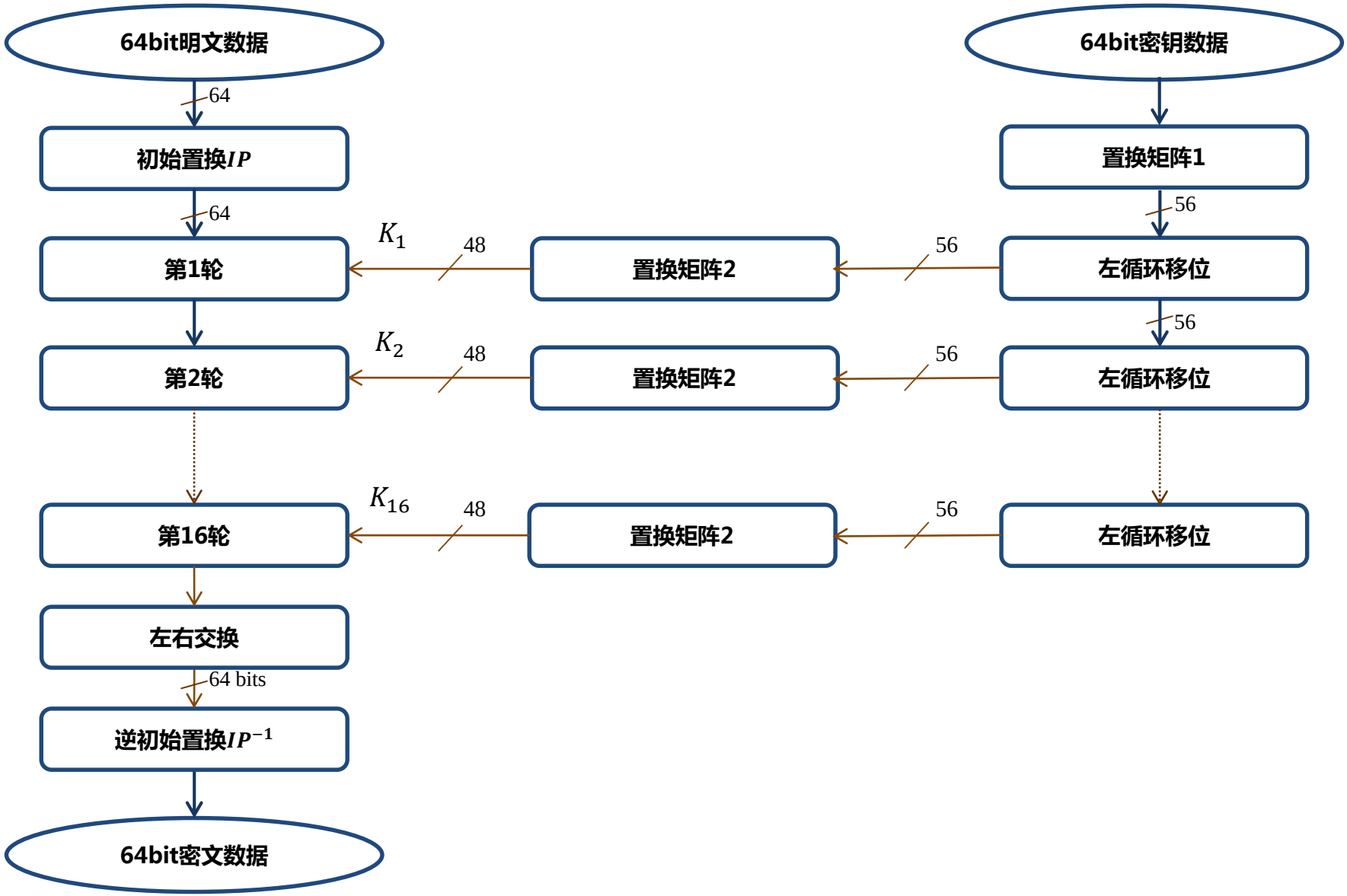
- DES算法的加密和解密运算均采用这3个步骤。
- 如果加密时使用的轮密钥次序为k1, k2, …, k16，那么当解密时使用的密钥次序为：k16, k15, …, k1。
- DES采用Feistel网络结构。Feistel 密码结构是一种对称结构，满足对合性。采用此结构的密码，其好处是加解密可以使用同一个芯片。

六、DES数据加密标准

DES算法流程图



DES数据加密标准——基本算法



六、DES数据加密标准

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

六、DES数据加密标准

设明文64bits数据为下表

M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8
M_9	M_{10}	M_{11}	M_{12}	M_{13}	M_{14}	M_{15}	M_{16}
M_{17}	M_{18}	M_{19}	M_{20}	M_{21}	M_{22}	M_{23}	M_{24}
M_{25}	M_{26}	M_{27}	M_{28}	M_{29}	M_{30}	M_{31}	M_{32}
M_{33}	M_{34}	M_{35}	M_{36}	M_{37}	M_{38}	M_{39}	M_{40}
M_{41}	M_{42}	M_{43}	M_{44}	M_{45}	M_{46}	M_{47}	M_{48}
M_{49}	M_{50}	M_{51}	M_{52}	M_{53}	M_{54}	M_{55}	M_{56}
M_{57}	M_{58}	M_{59}	M_{60}	M_{61}	M_{62}	M_{63}	M_{64}

六、DES数据加密标准

经过初始置换IP后变为

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

六、DES数据加密标准

逆初始置换IP^{-1}

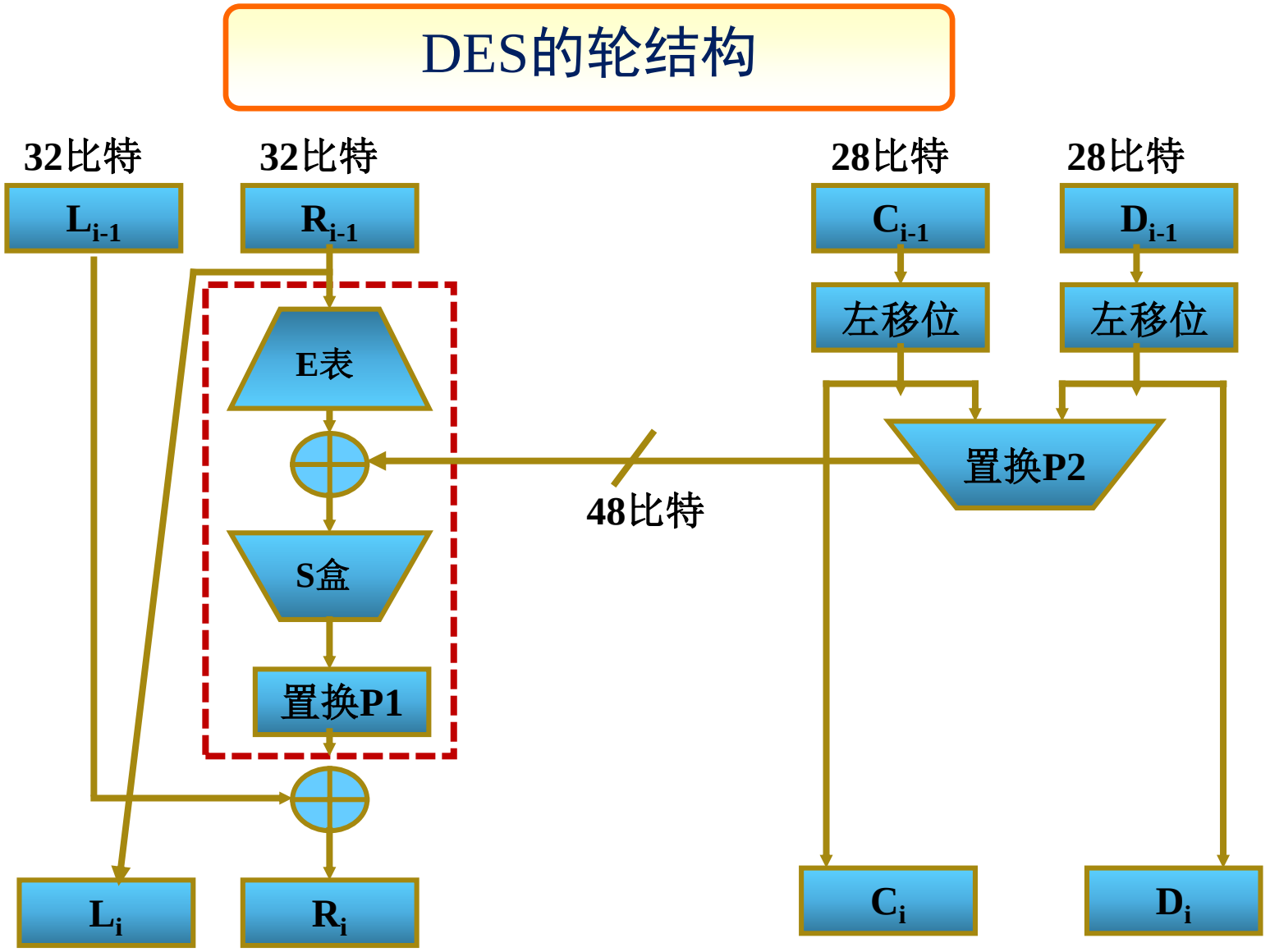
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

六、DES数据加密标准

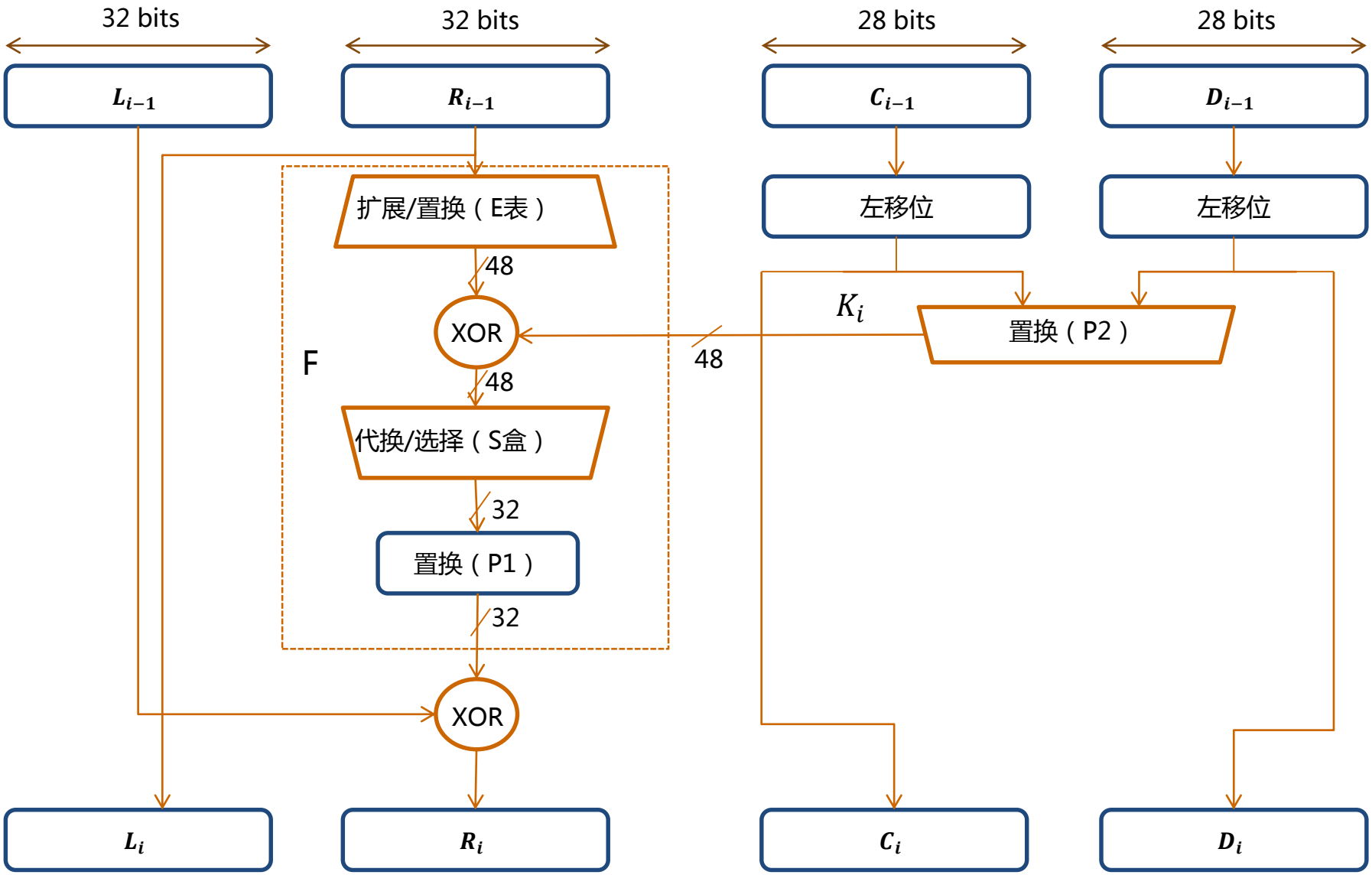
经过逆初始置换IP^{-1}后变为

M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8
M_9	M_{10}	M_{11}	M_{12}	M_{13}	M_{14}	M_{15}	M_{16}
M_{17}	M_{18}	M_{19}	M_{20}	M_{21}	M_{22}	M_{23}	M_{24}
M_{25}	M_{26}	M_{27}	M_{28}	M_{29}	M_{30}	M_{31}	M_{32}
M_{33}	M_{34}	M_{35}	M_{36}	M_{37}	M_{38}	M_{39}	M_{40}
M_{41}	M_{42}	M_{43}	M_{44}	M_{45}	M_{46}	M_{47}	M_{48}
M_{49}	M_{50}	M_{51}	M_{52}	M_{53}	M_{54}	M_{55}	M_{56}
M_{57}	M_{58}	M_{59}	M_{60}	M_{61}	M_{62}	M_{63}	M_{64}

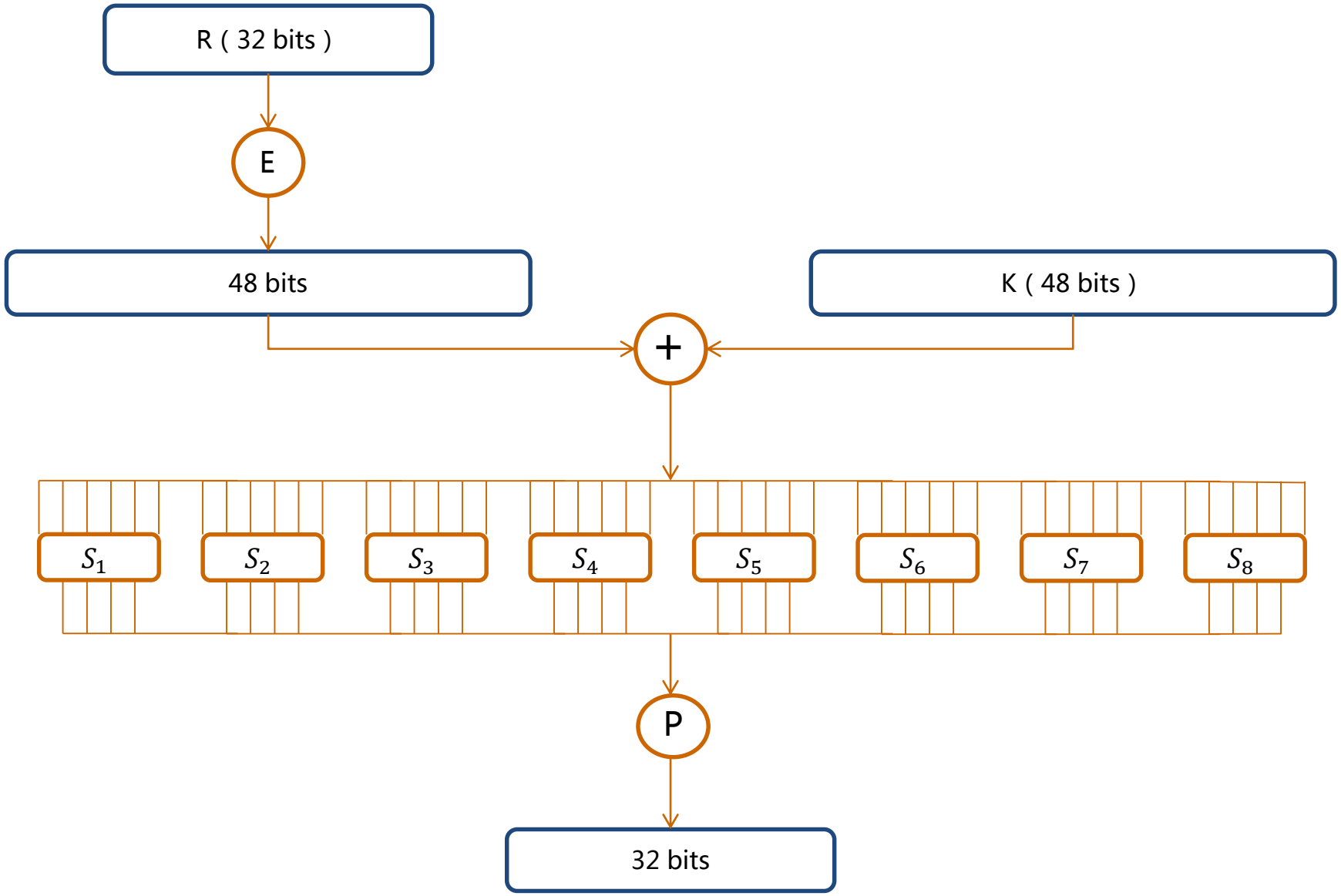
六、DES数据加密标准


DES的轮结构
32比特
32比特
28比特
28比特
L_{i-1}
R_{i-1}
C_{i-1}
D_{i-1}
左移位
左移位
E表
置换P2
48比特
S盒
置换P1
L_i
R_i
C_i
D_i

DES数据加密标准——1轮的加密过程



DES数据加密标准——S盒和P盒



DES数据加密标准——8个S盒

S_1

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

S_2

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

S_3

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

DES数据加密标准——8个S盒

S_4

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

S_5

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

S_6

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

DES数据加密标准——8个S盒

S_7

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

S_8

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

DES数据加密标准——P盒与S盒的密码学意义

S盒的作用是混淆（Confusion），主要增加明文和密文之间的复杂度（包括非线性度等）。DES的安全性直接取决于S盒的安全性。

P盒的作用是扩散（Diffusion），目的是让明文和密钥的影响迅速扩散到整个密文中。即一位的明文或密钥的改变会影响到密文的多个比特。

S盒和P盒的作用体现了Shannon的扩散和混淆的密码设计思想。

DES数据加密标准——安全性分析

1997年1月28日，美国RSA公司悬赏10000美元破译DES。美国程序员RockeVerser用140天破译成功。从此宣布了 DES时代的终结。

2008年SciEngines公司的Rivyera将破解DES的时间缩减到1天以内，并一直保持着暴力破解DES的记录。

因此必须设计新一代的数据加密标准来替代DES。

推出新的更安全的数据加密标准

六、DES数据加密标准

DES加密的一个例子

- 取16进制明文X：0123456789ABCDEF
- 密钥K为：133457799BBCDFF1
  去掉奇偶校验位以二进制形式表示的密钥是000100100110
  100101011011110010011011011110110111111111000
- 应用IP，我们得到：
  L_0= 11001100000000001100110011111111
  $R_0=L_1$=11110000101010101111000010101010
- 然后进行16轮加密。
  最后对L_{16}, R_{16}使用IP^{-1}
- 加密输出得到密文：85E813540F0AB405

思考题

- 什么是对称加密体制?
- 什么是非对称加密体制？
- 根据对明文数据的处理方式不同，对称加密体制又可以分为哪两类算法？
- 非对称密码体制是分组加密算法吗？
- DES算法中的IP置换的作用是什么？
- DES算法中16轮迭代运算的作用是什么？
- 什么是算法的对合性？DES为什么要满足对和的性质?
- 数据的安全性是否取决于密码算法的保密？

谢谢！