§3.3 数据加密标准DES

DES（Data Encryption Standard）

发明人：美国IBM公司W. Tuchman 和 C. Meyer 1971-1972年研制成功。

基础：1967年美国Horst Feistel提出的理论

标准化：DES算法1975年3月公开发表，1977年1月15日由美国国家标准局颁布为数据加密标准（Data Encryption Standard），于1977年7月15日生效。

1979年，美国银行协会批准使用DES。

1980年，DES成为美国标准化协会(ANSI)标准。

1984年2月，ISO成立的数据加密技术委员会(SC20)在DES基础上制定数据加密的国际标准工作。

§3.3 数据加密标准DES

DES（Data Encryption Standard）

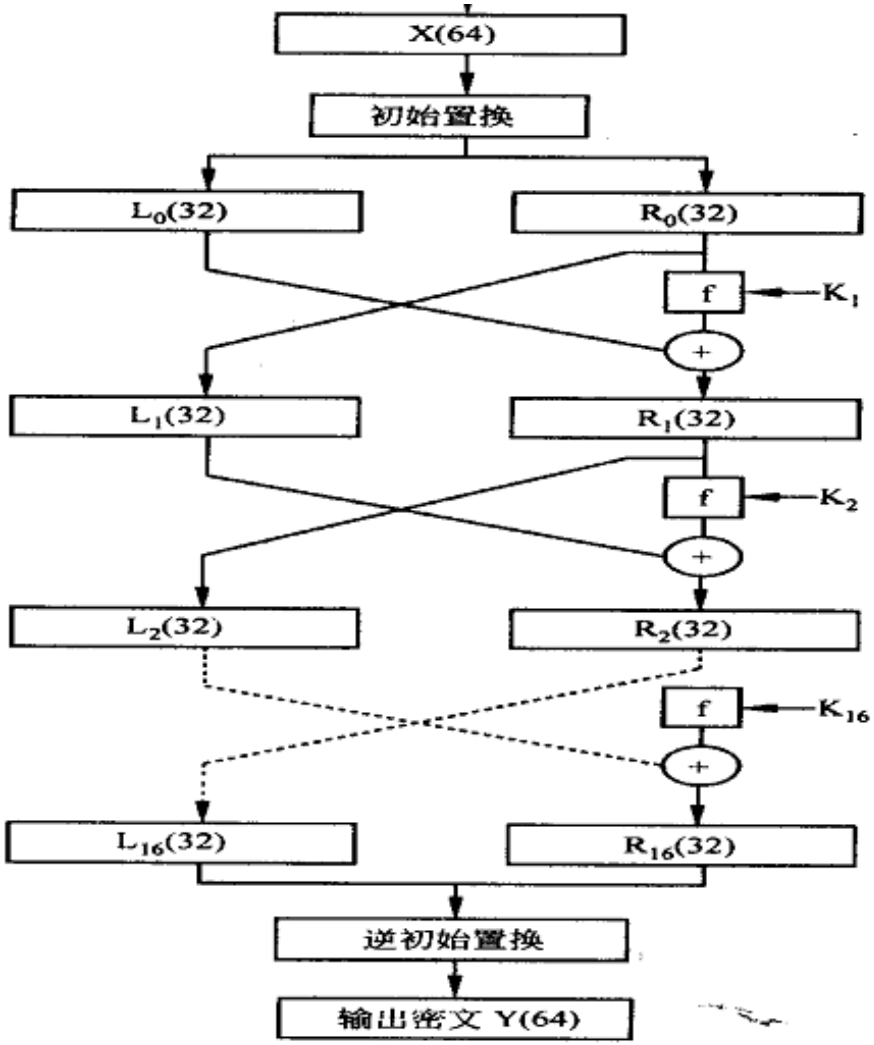
- **DES的基本原理**

DES为二进制编码数据设计的，可以对计算机数据进行密码保护的数学运算。

DES算法是对称的，既可用于加密又可用于解密。密钥的长度为56位。（密钥通常表示为64位的数，但每个第8位都用作奇偶校验）密钥可以是任意的56位的数，且可在任意的时候改变。其中极少量的数被认为是弱密钥，但能容易地避开它们。所有的保密性依赖于密钥。

DES加密算法过程：初始置换IP、16次迭代过程、逆置换。

§3.3 数据加密标准DES



§3.3 数据加密标准DES

DES的算法描述

利用传统的换位和置换加密。假定信息空间由{0,1}组成的字符串，信息被分成64比特的块，密钥是56比特。经过DES加密的密文也是64比特的块。

明文：$m=m_1m_2\ldots m_{64}$　$m_i = 0, 1$，$i = 1, 2, \ldots, 64$

密钥：$k=k_1k_2\ldots k_{64}$　　$k_i = 0, 1$，$i = 1, 2, \ldots, 64$

其中k_8，k_{16}，…，k_{64}是奇偶校验位，起作用的仅为56位。

加密算法：　$E_k(m) = IP^{-1}\cdot T_{16}\cdot T_{15}\cdots\cdots T_1\cdot IP(m)$

其中IP为初始置换，IP^{-1}是IP的逆，T_i (i = 1,2,…16)是一系列的变换。

解密算法：　$E_k^{-1}(c) = IP^{-1}\cdot T_1\cdot T_2\cdots\cdots T_{16}\cdot IP(c)$

§3.3 数据加密标准DES



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

§3.3 数据加密标准DES

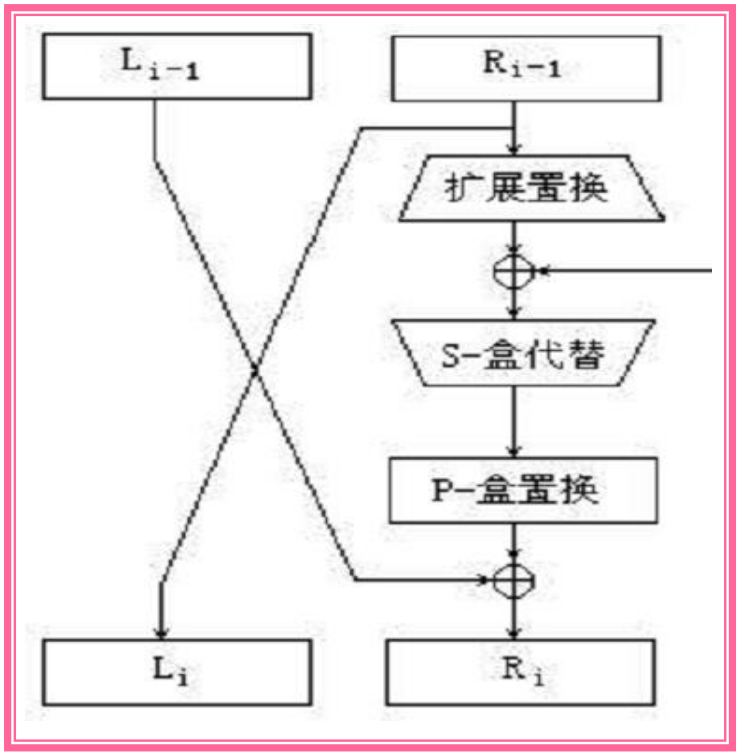




§3.3 数据加密标准DES

DES迭代过程的核心是非线性F函数的功能，它是每轮实现加密混淆和扩散的主要途径。

每一轮迭代过程都必须经过三个子过程：扩展置换、压缩替换（S盒选择）、P盒排列。

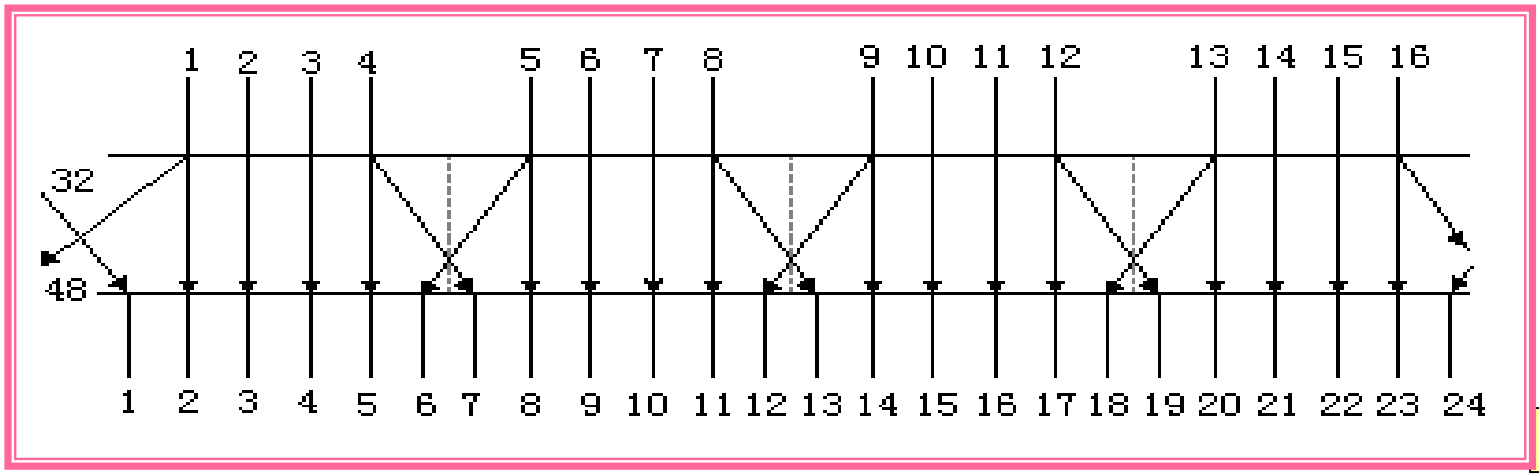


§3.3 数据加密标准DES

扩展置换：

这个运算将数据的右半部分R_i从32位扩展到了48位。由于这个运算改变了位的次序，重复了某些位，故被称为扩展置换。

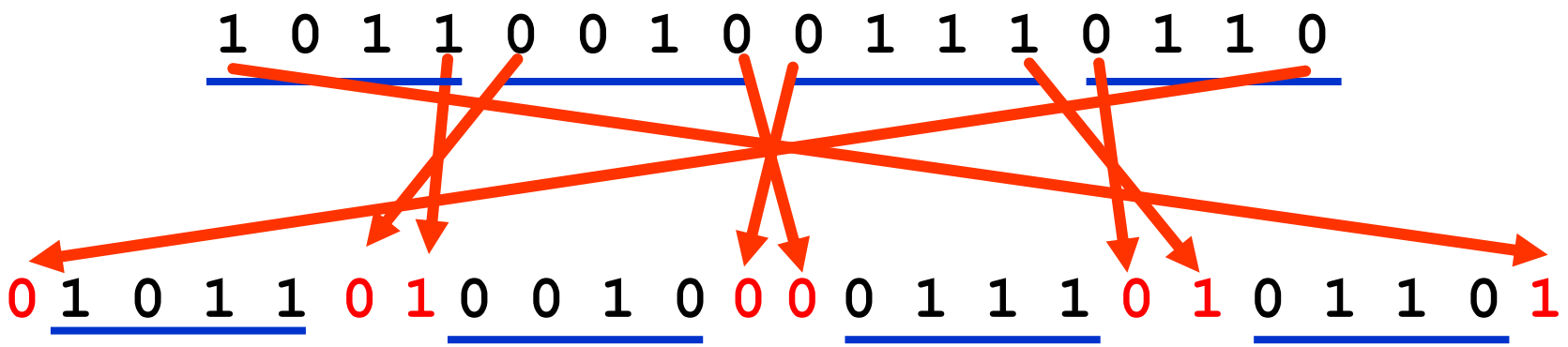
这个操作有两个方面的目的：它产生了与密钥同长度的数据以进行异或运算，它提供了更长的结果，使得在替代运算时能进行压缩。下图显示了扩展置换，有时它也叫做E盒。



§3.3 数据加密标准DES

扩展置换的例子

输入16位



0 1 0 1 1 0 1 0 0 1 0 0 0 1 1 1 0 1 0 1 1 0 1

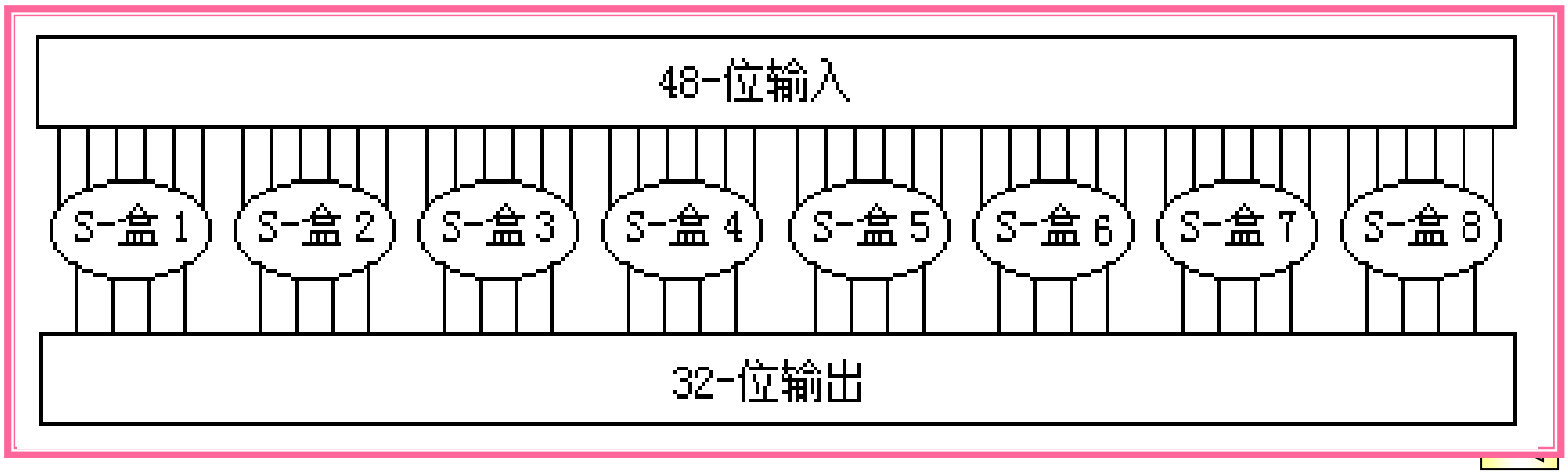
输出24位

§3.3 数据加密标准DES

压缩替换（S盒选择）

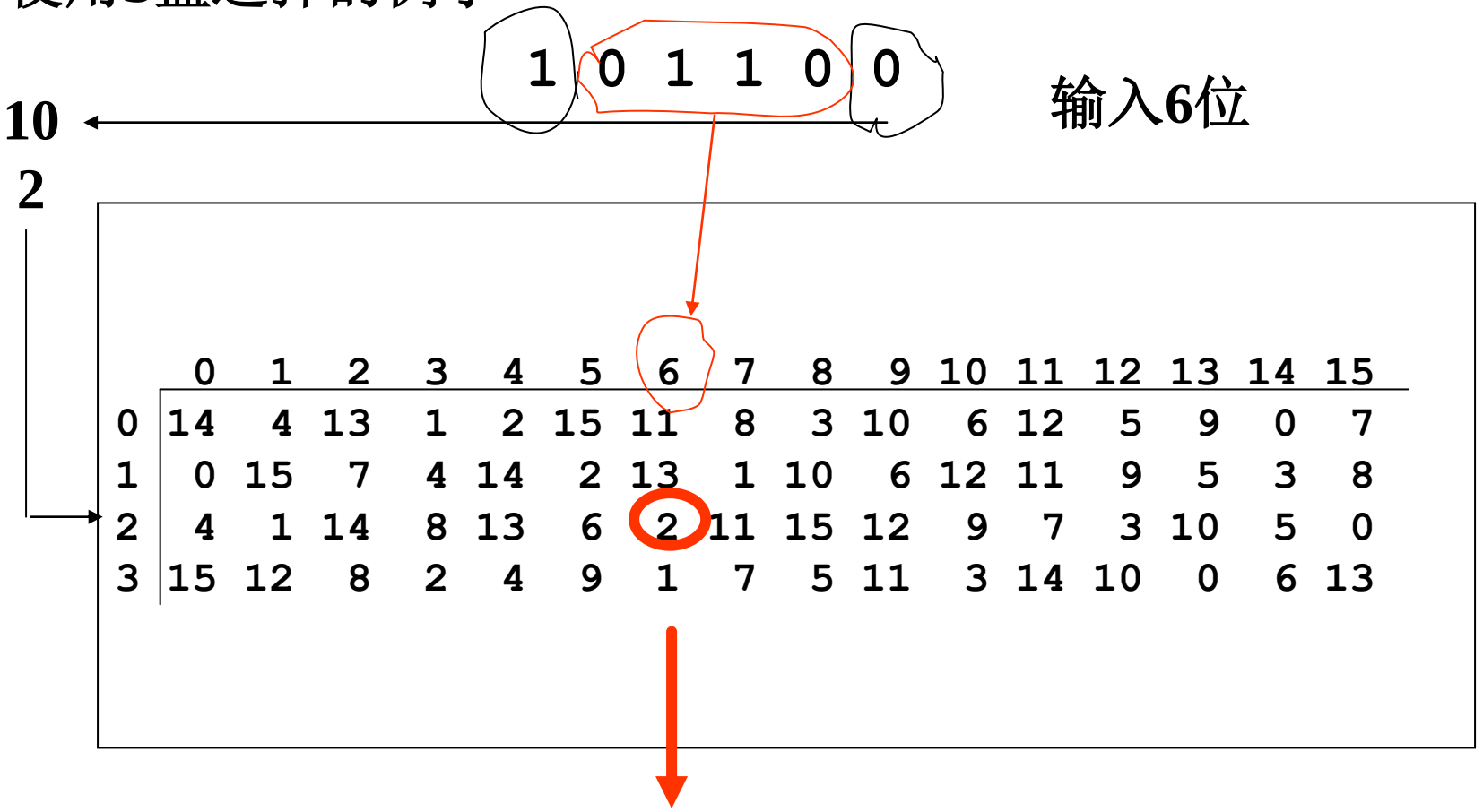
压缩后的密钥与扩展分组异或以后，将48位的结果送入，进行替换运算。替换由8个替换盒（ S盒）完成。每一个S盒都有6位输入，4位输出，且这8个S盒是不同的。48位的输入被分为8个6位的分组，每一分组对应一个S盒替换操作：

分组1由S-盒1操作，分组2由S-盒2操作，依次类推。



§3.3 数据加密标准DES

使用S盒选择的例子



§3.3 数据加密标准DES

P盒置换

S盒代替运算后的32位输出依照P盒进行置换。该置换把每输入位映射到输出位，任意一位不能被映射两次，也不能被略去，这个置换叫做直接置换。

下表给出了每位移到的位置。例如第21位移到了第4位处，同时第4位移到了第31位处。最后，将P盒置换的结果与最初的64位分组的左半部分异或，然后左、右半部分交换，接着开始另一轮。

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

§3.3 数据加密标准DES

DES解密过程

在经过所有的代替、置换、异或和循环移动之后，获得了这样一个非常有用的性质：加密和解密可使用相同的算法。

DES使得用相同的函数来加密或解密每个分组成为可能，二者的唯一不同之处是密钥的次序相反。这就是说，如果各轮的加密密钥分别是K_1，K_2，K_3，…，K_{16}，那么解密密钥就是K_{16}，K_{15}，K_{14}，……，K_1。

§3.3 数据加密标准DES

子密钥的生成

一开始，由于不考虑每个字节的第8位，DES的密钥由64位减至56位，如下表所示进行密钥置换。

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

§3.3 数据加密标准DES

在DES的每一轮中，从56位密钥产生出不同的48位子密钥，这些子密钥K_i由下面的方式确定。

首先，56位密钥被分成两部分，每部分28位。然后，根据轮数，这两部分分别循环左移l位或2位。下表给出了每轮移动的位数。

轮	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
位数	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

§3.3 数据加密标准DES

移动后，就从56位中选出48位。因为这个运算不仅置换了每位的顺序，同时也选择子密钥，因而被称作选择置换。这个运算提供了一组48位的集。下表给出了选择置换后的输出。例如处在第33位位置的那一位在输出时移到了第35位的位置，而处在第18位位置的那一位被略去了。

删除的8位分别是第9、18、22、25、35、38、43、54位。

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

§3.3 数据加密标准DES

DES解密过程

在经过所有的代替、置换、异或和循环移动之后，获得了这样一个非常有用的性质：加密和解密可使用相同的算法。

DES使得用相同的函数来加密或解密每个分组成为可能，二者的唯一不同之处是密钥的次序相反。这就是说，如果各轮的加密密钥分别是K_1，K_2，K_3，…，K_{16}，那么解密密钥就是K_{16}，K_{15}，K_{14}，……，K_1。

§3.3 数据加密标准DES

DES的安全性

DES的唯一密码学缺点就是密钥长度较短。解决密钥长度的问题的办法之一是采用多重DES。

双重DES使用两个长度为56位DES密钥，先用密钥K_1进行DES加密，对加密后的密文再使用密钥K_2进行DES加密，得到最终密文。双重DES很难抵抗中间相遇攻击。

三重DES使用三个长度为56位DES密钥，先用密钥K_1进行DES加密，对加密后的密文再使用密钥K_2进行DES解密，最后用密钥K_3进行DES加密，得到最终密文。但最常用的三重DES算法中选取$K_1 = K_3$。