《密码学》

期末速成课

课时三　对称密码体制

高数帮

考点	重要程度	占分	题型
1. 分组密码代表	★★★	3 - 5	选择/填空
2. 分组密码长度、密钥长度、输出长度	★★★	0 - 3	大题
3. 分组密码运行模式	★★★★	0 - 3	选择/填空
4. DES/AES	★★★★★	6 - 10	选择/大题
5. RC4	★★★★★	3 - 8	选择/大题
6. 反馈移位寄存器	★★★★	0 - 4	选择/填空

3.1 对称密码体制

一、对称密码体制

1、对称密码体制分为分组密码和流密码

分组密码有DES、AES、IDEA、RC6...

流密码有RC4、A5、SEAL...

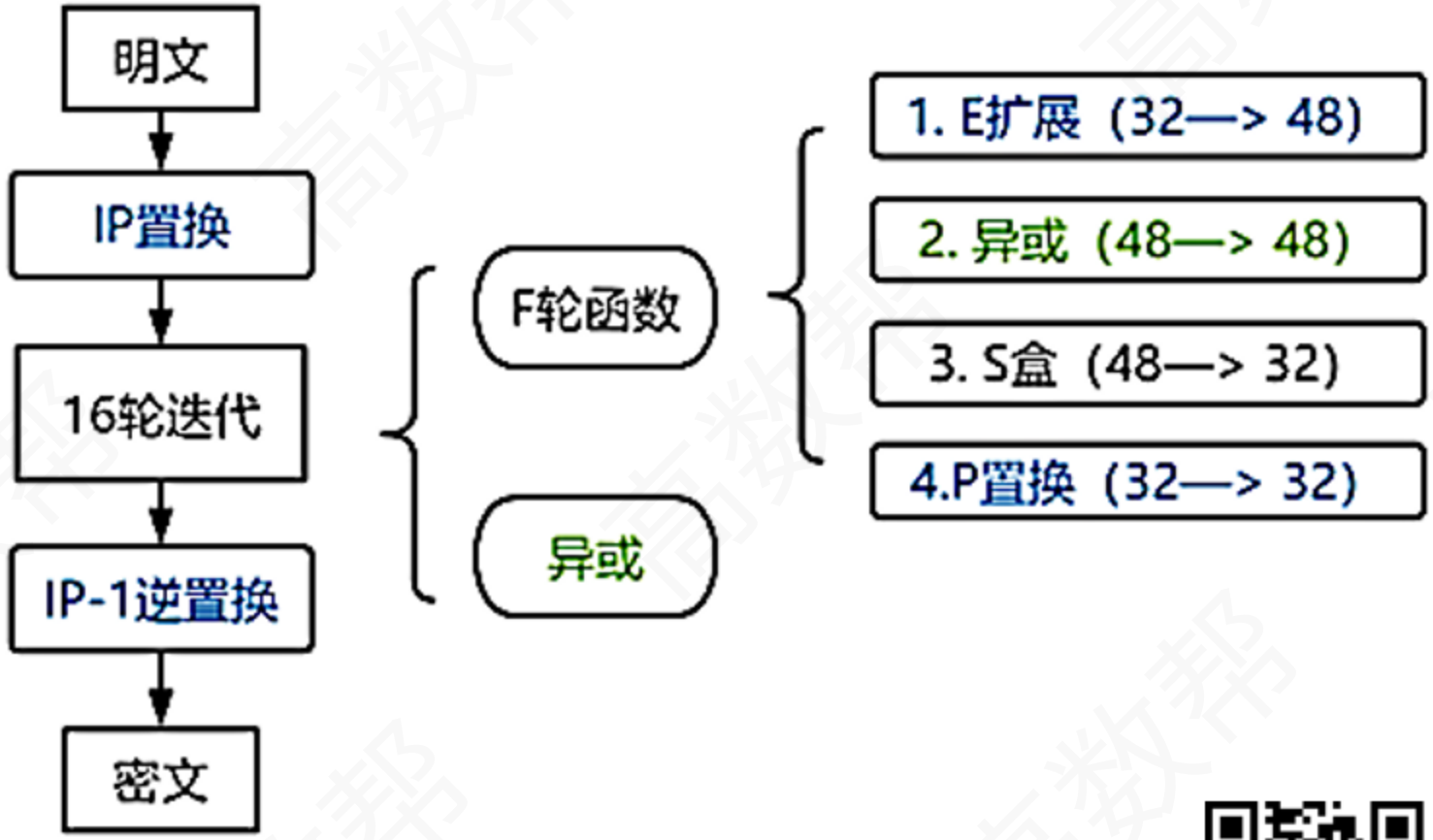
2、分组密码设计思想

扩散 (DES中P置换)：就是将明文的统计特性散布到密文中去

混淆 (DES中S盒代换)：使密文和密钥之间的统计关系变得尽可能复杂

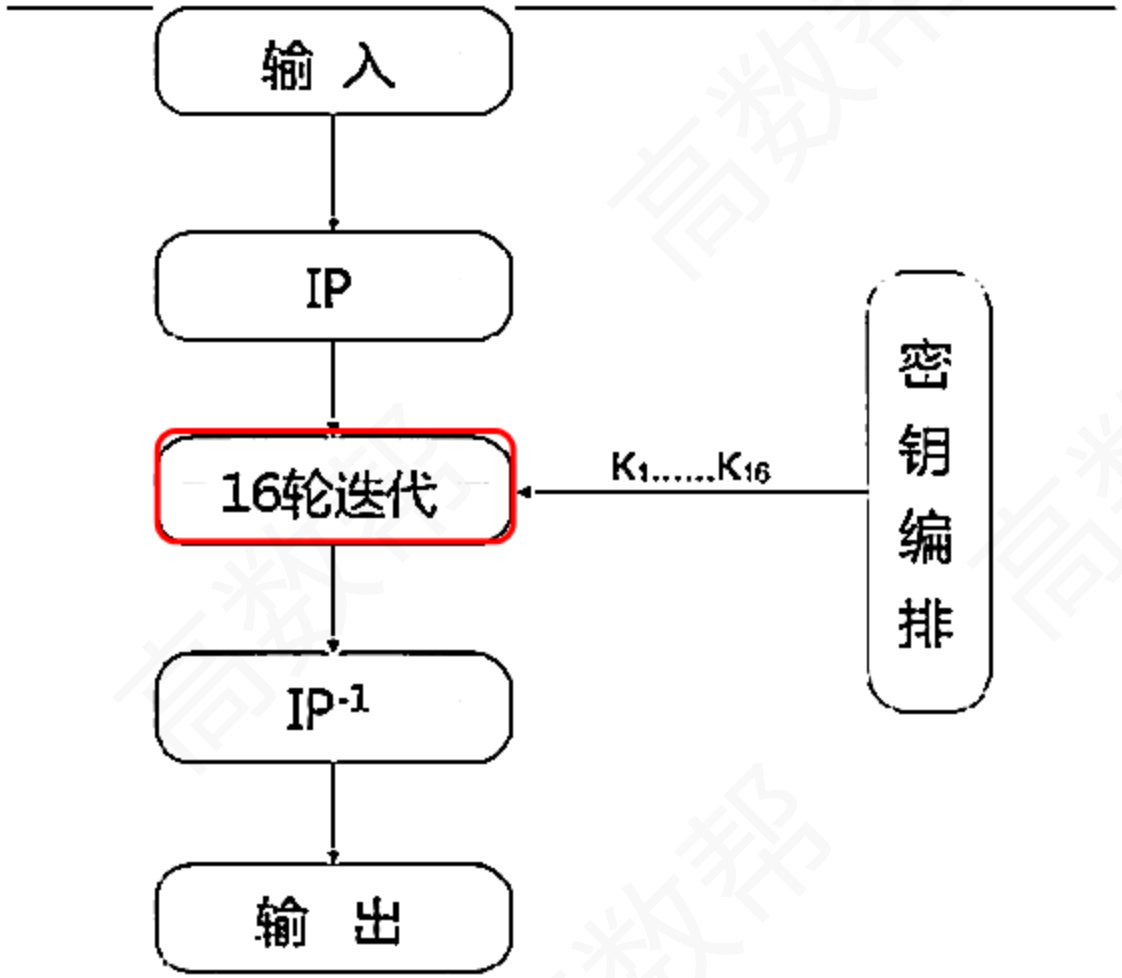
乘积密码

二、DES



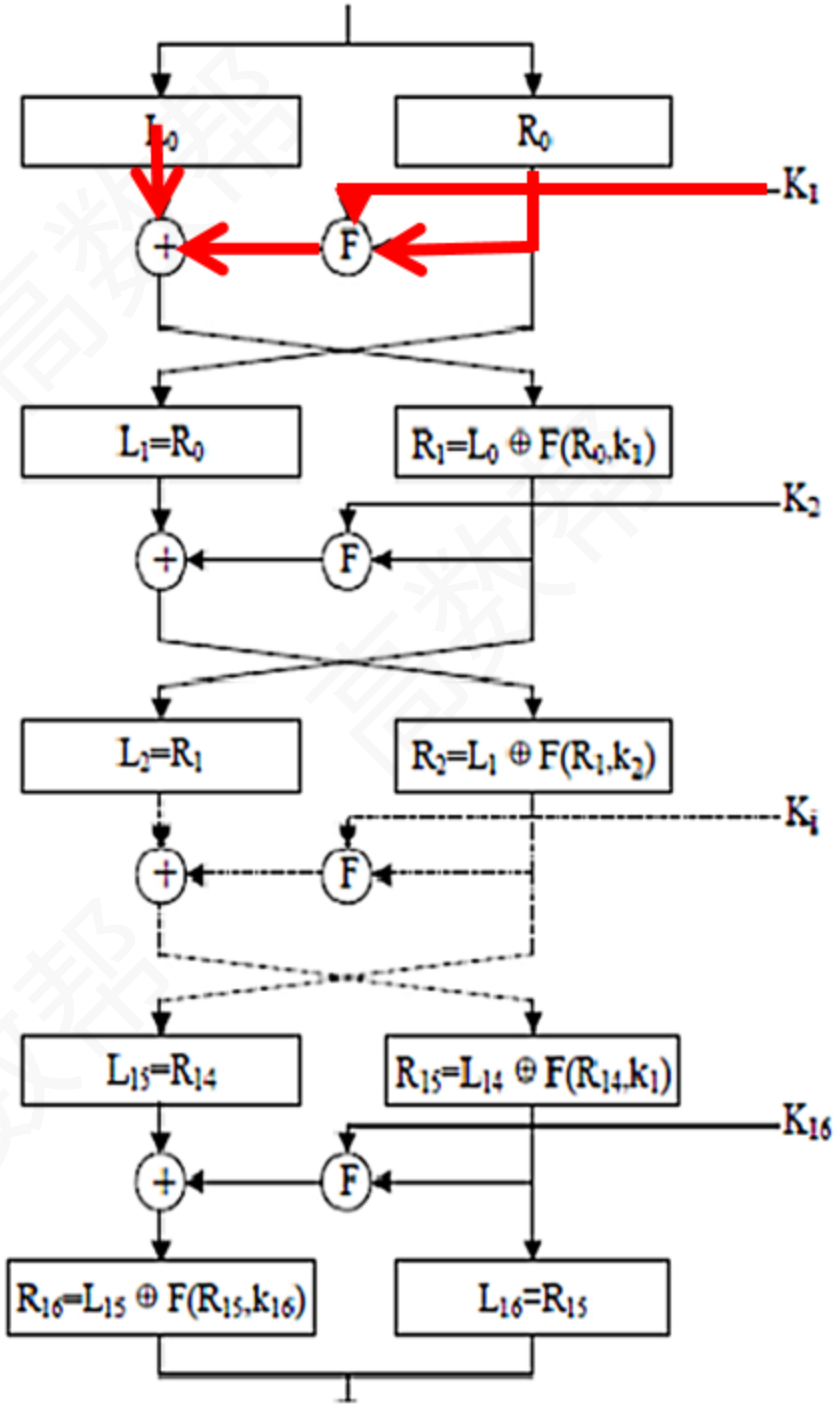
扫码观看
视频讲解更清晰

二、DES



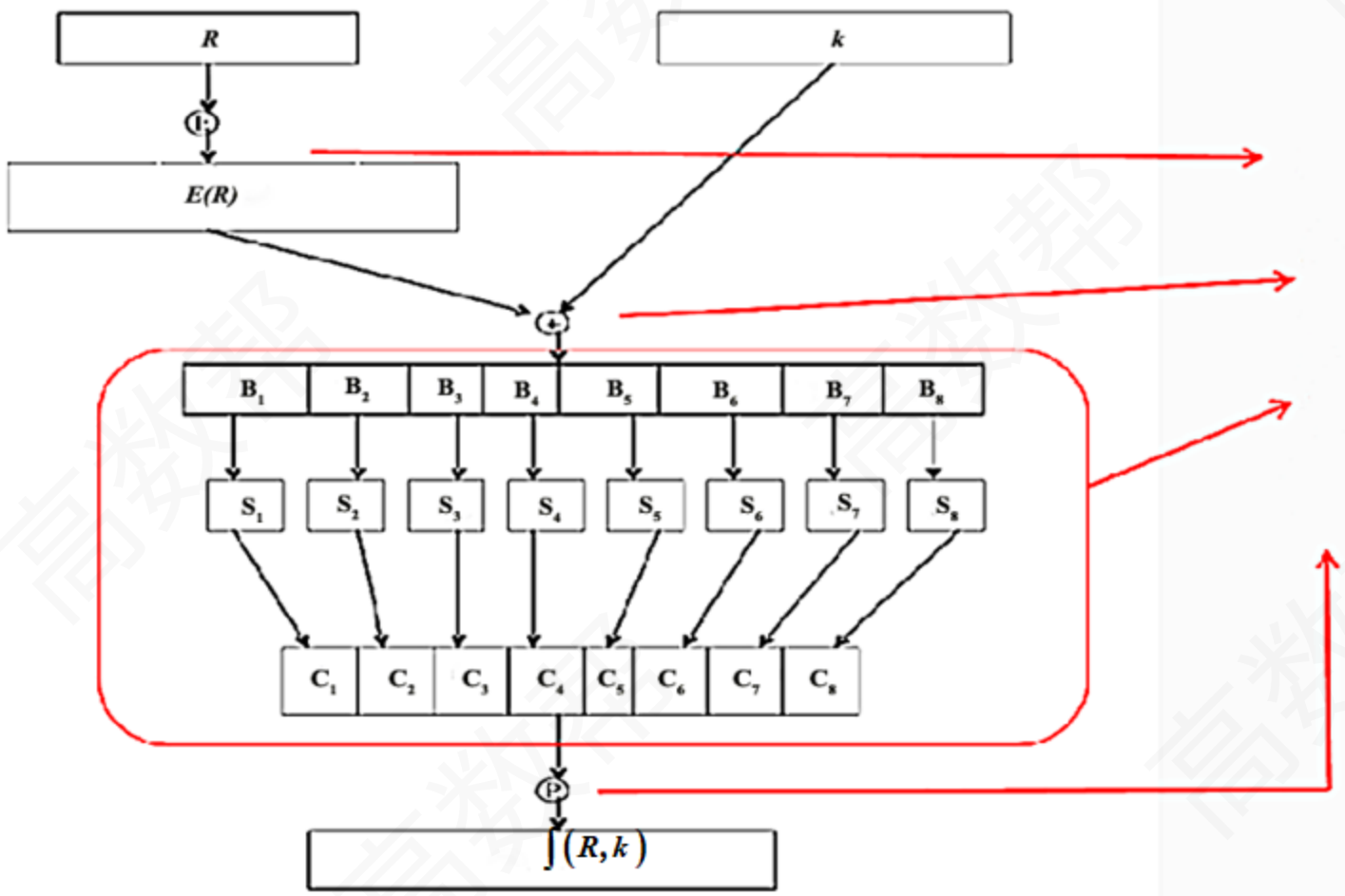
1. 16轮迭代

- ◆F轮函数
- ◆异或



二、DES

2、轮函数



- 轮函数

1.E扩展（32->48）

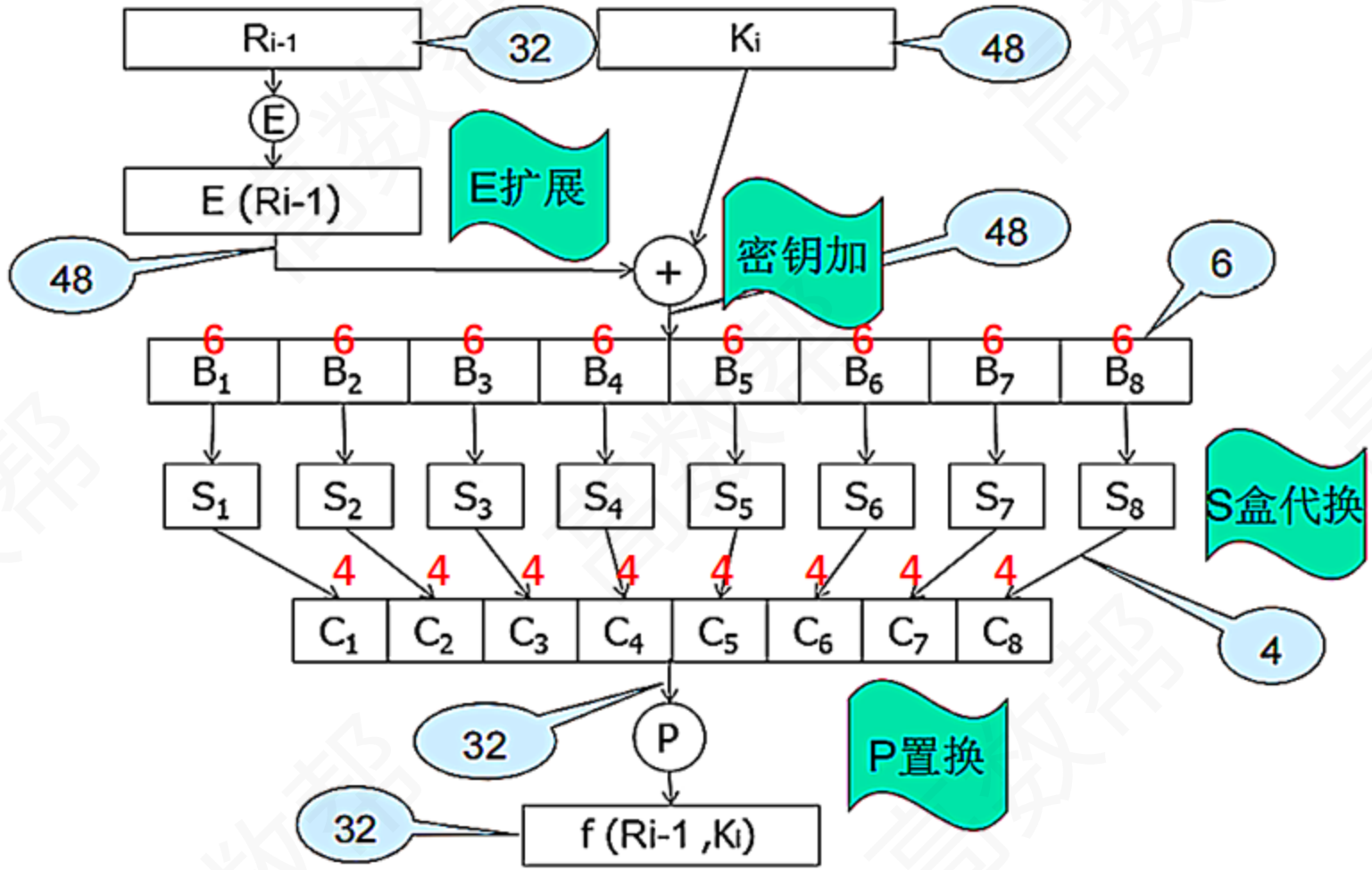
2.异或（48->48）

3.S盒（48->32）

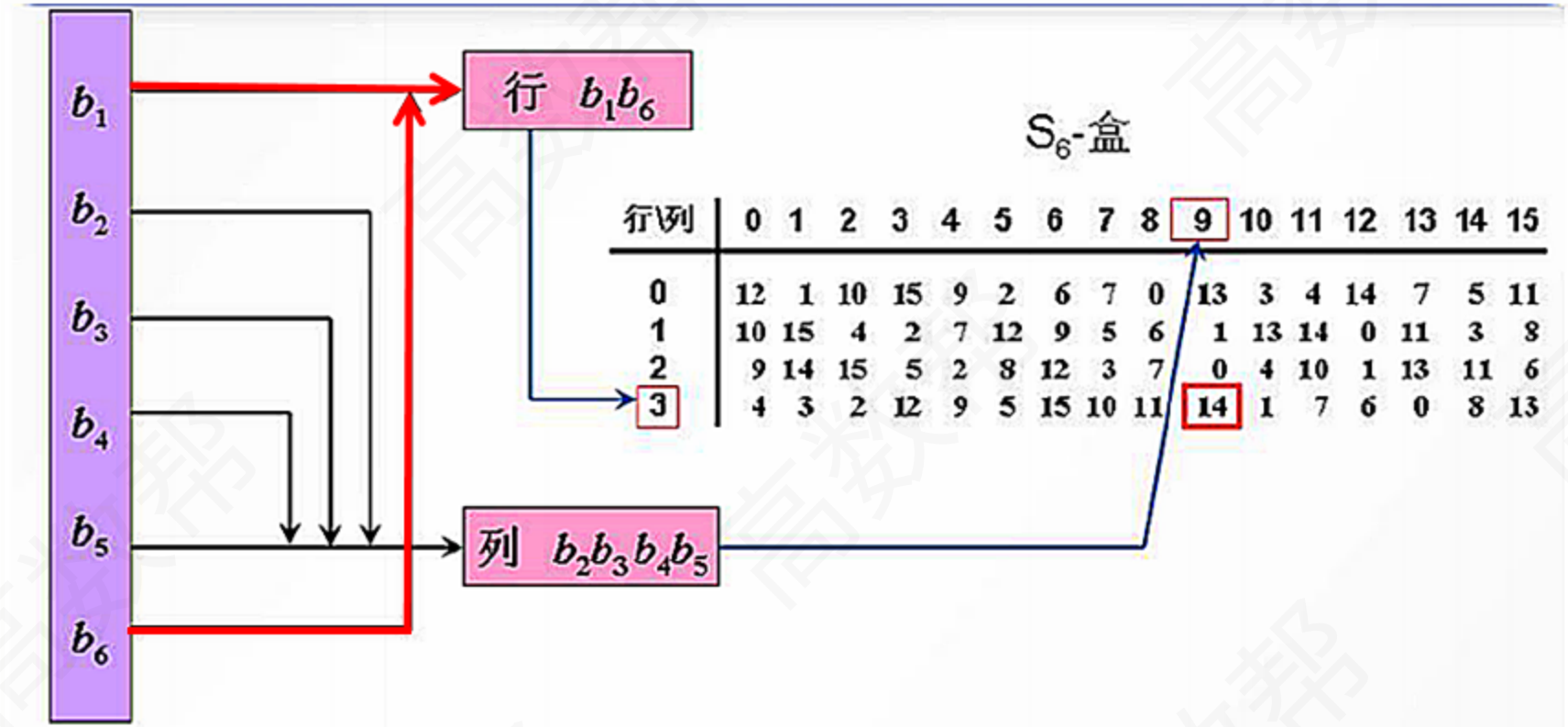
4.P置换（32->32）

二、DES

3、S盒

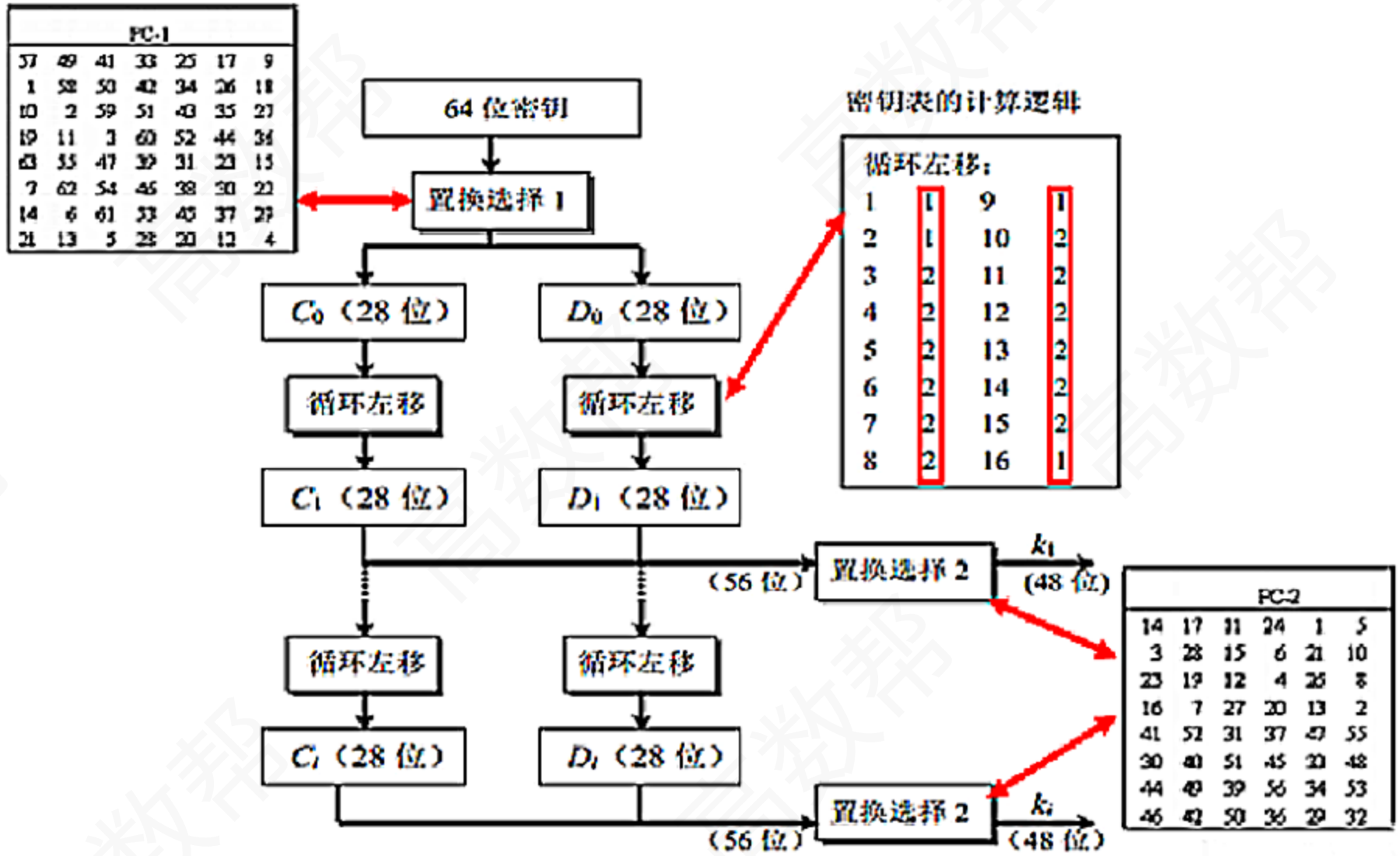

Ri-1
32
Ki
48
E
E (Ri-1)
E扩展
48
+
密钥加
48
6
6
6
6
6
6
6
6
6
B1
B2
B3
B4
B5
B6
B7
B8
S1
S2
S3
S4
S5
S6
S7
S8
S盒代换
4
4
4
4
4
4
4
4
C1
C2
C3
C4
C5
C6
C7
C8
4
32
P
P置换
32
f (Ri-1 ,Ki)

二、DES

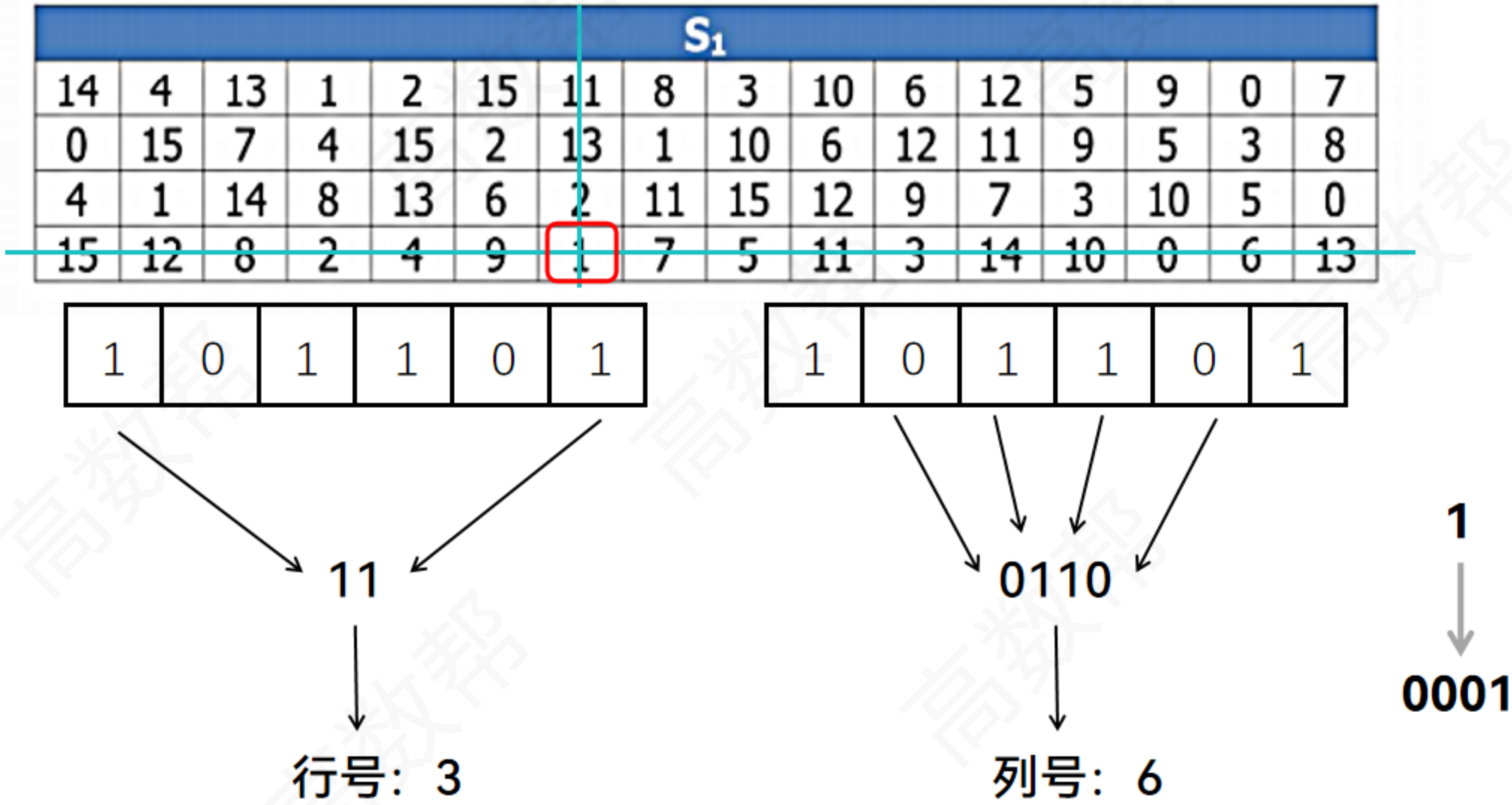

b_1
b_2
b_3
b_4
b_5
b_6
行 b_1b_6
列 $b_2b_3b_4b_5$
S_6-盒
行\列 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
0 12 1 10 15 9 2 6 7 0 13 3 4 14 7 5 11
1 10 15 4 2 7 12 9 5 6 1 13 14 0 11 3 8
2 9 14 15 5 2 8 12 3 7 0 4 10 1 13 11 6
3 4 3 2 12 9 5 15 10 11 14 1 7 6 0 8 13
$b_1b_2b_3b_4b_5b_6$
110011
行:b_1b_6=11_2=3
列:$b_2b_3b_4b_5$=1001=9
S_6-盒 3行9列
值: 14=1100

二、DES

4、密钥编排


PC-1
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
64 位密钥
置换选择 1
C_0（28 位）
D_0（28 位）
循环左移
循环左移
C_1（28 位）
D_1（28 位）
循环左移
循环左移
C_i（28 位）
D_i（28 位）
（56 位）
置换选择 2
k_1
(48 位)
（56 位）
置换选择 2
k_i
（48 位）
密钥表的计算逻辑
循环左移：
1 1 9 1
2 1 10 2
3 2 11 2
4 2 12 2
5 2 13 2
6 2 14 2
7 2 15 2
8 2 16 1
PC-2
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

【题1】DES密码算法中，已知S盒如下表所示，若输入101101，求输出。



三、AES

- 分组长度只能是128位
- 密钥长度 128/192/256bit
- 处理单位是字节

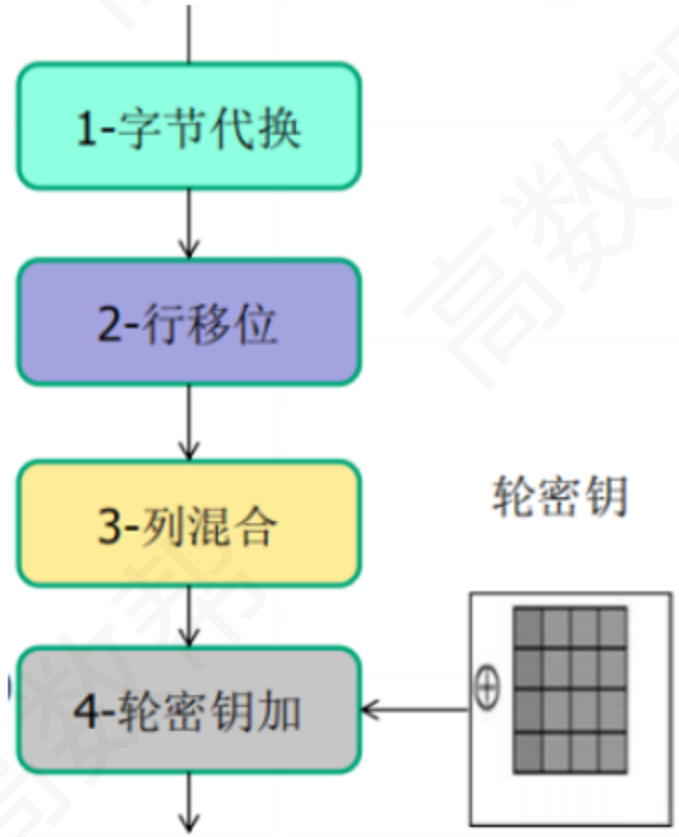
前N-1轮由4个变换组成，依次为:

（1）字节代换（SubByte）

（2）行移位（ShiftRow）

（3）列混合（MixColumn）

（4）轮密钥加（AddRoundKey）



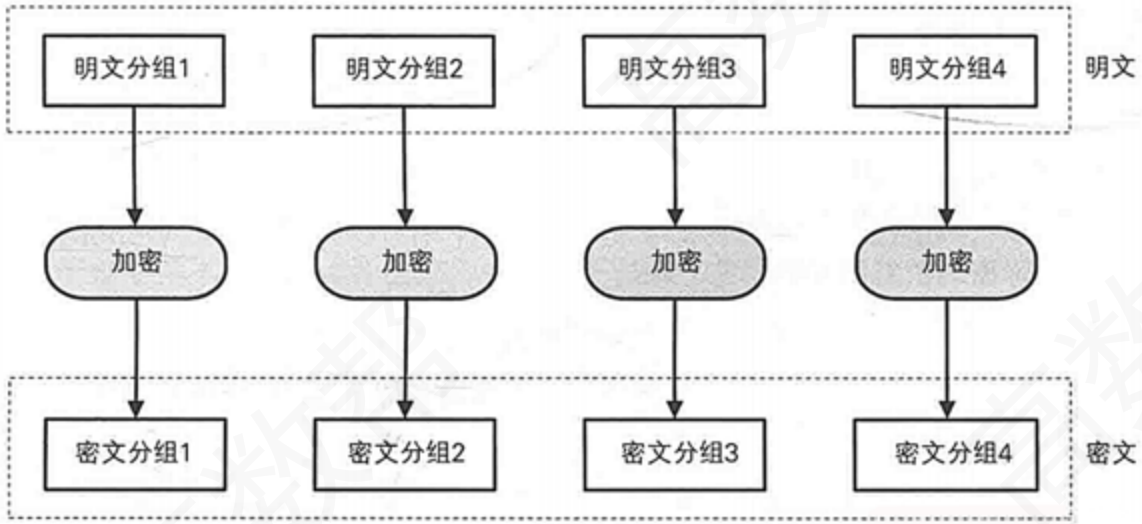
四、分组密码 分组长度 密钥长度

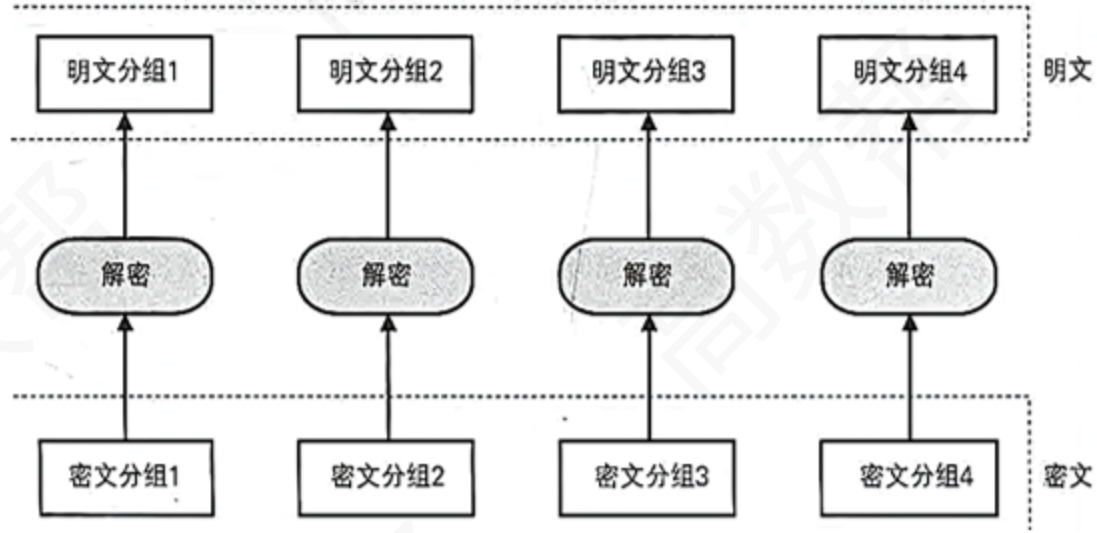
	DES	AES	MD5
分组长度	64bit	128bit	512bit
密钥长度	64/56bit	128/192/256bit	
输出	64bit		128bit

扫码观看
视频讲解更清晰

五、分组密码的运行模式

1、电子密码本(ECB)



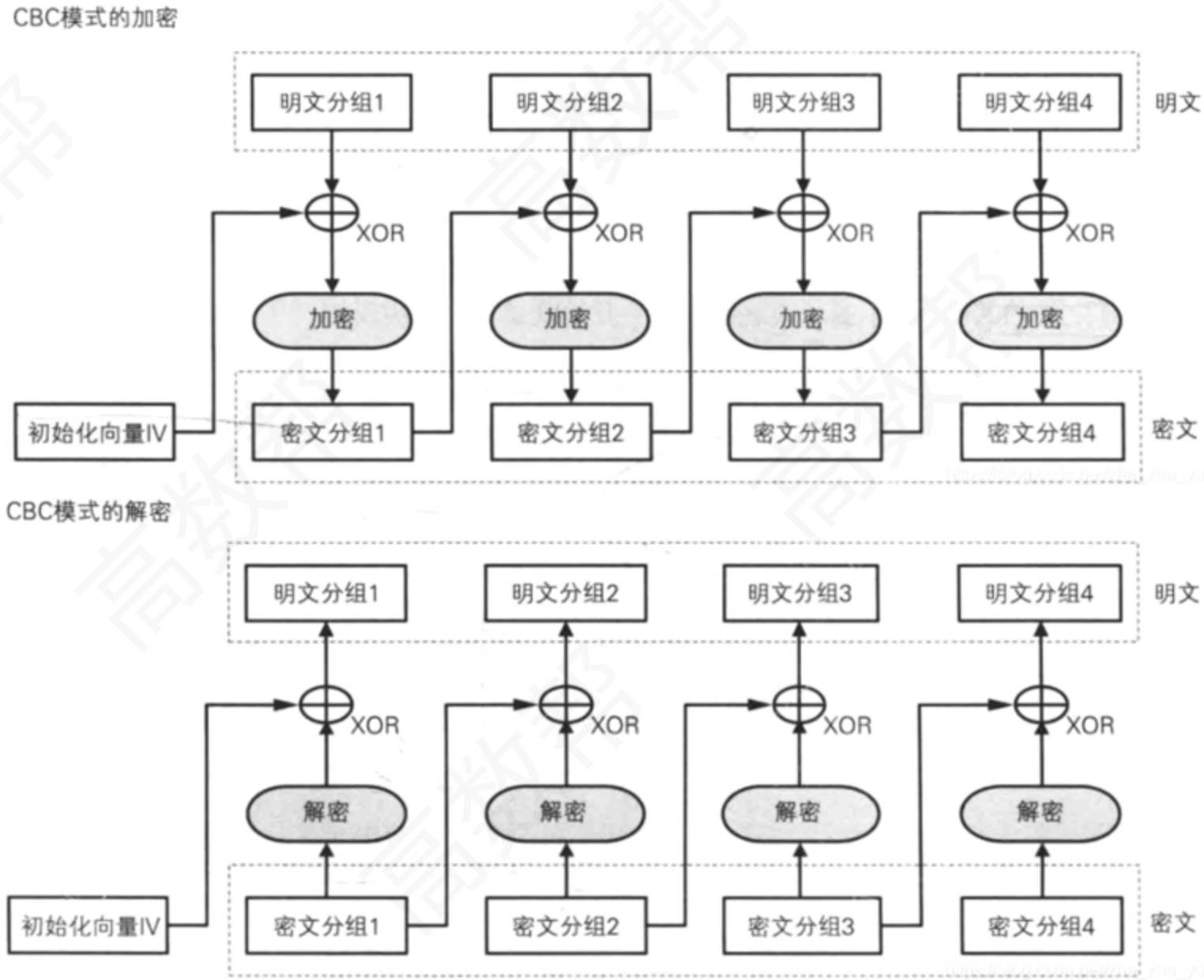


- 相同明文在相同密钥下得到相同密文
- 并行处理
- 最快最简单的分组密码模型，安全性最弱

五、分组密码的运行模式

2、密码分组链接（CBC）

- 每个密文分组不仅依赖于产生它的明文分组，还依赖前面的所有分组
- 相同明文在相同密钥下得到不同密文
- 不能实现并行处理
- 适合软件加密

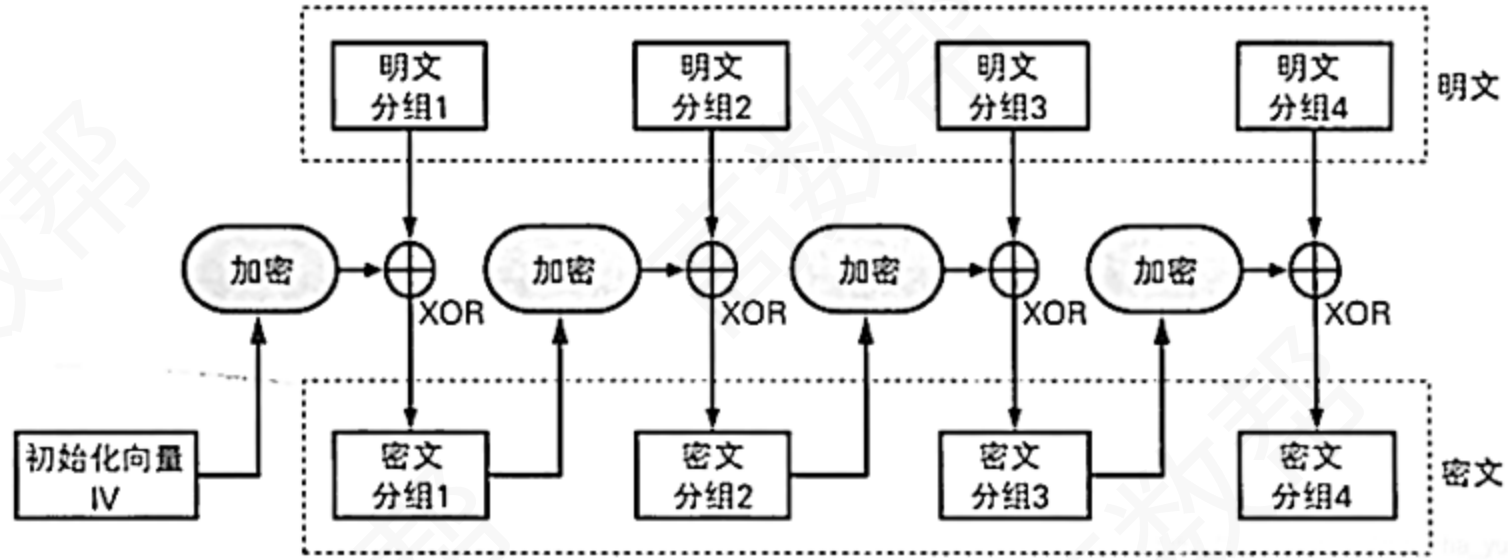


五、分组密码的运行模式

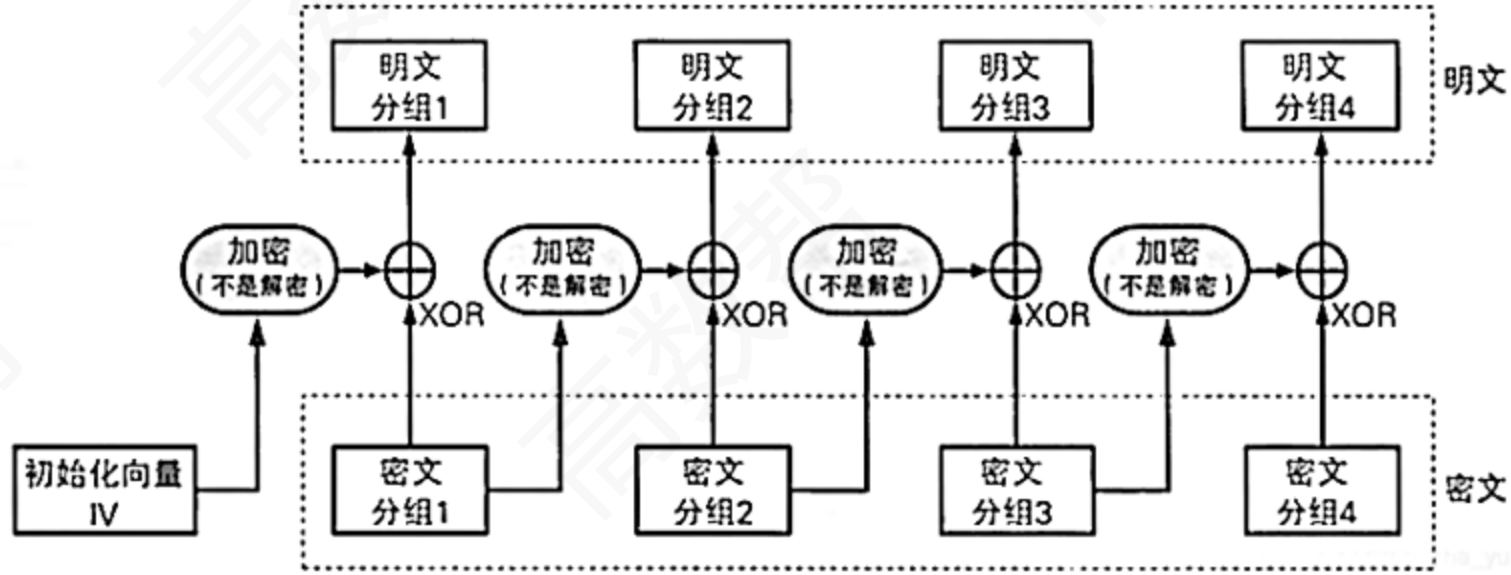
3、密码反馈(CFB)

- 相同明文用相同密钥
  加密得到不同密文

CFB模式的加密



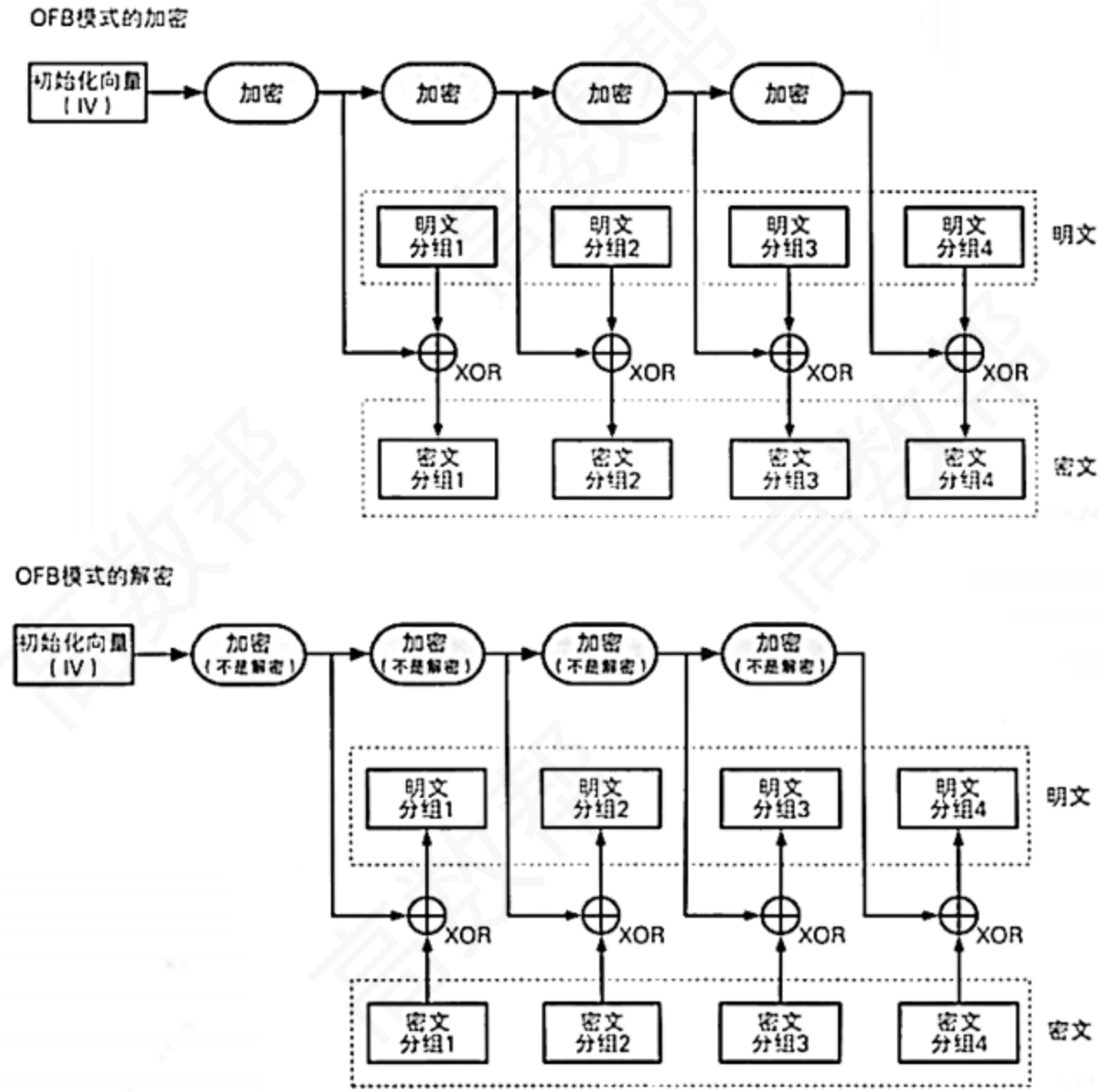
CFB模式的解密



五、分组密码的运行模式

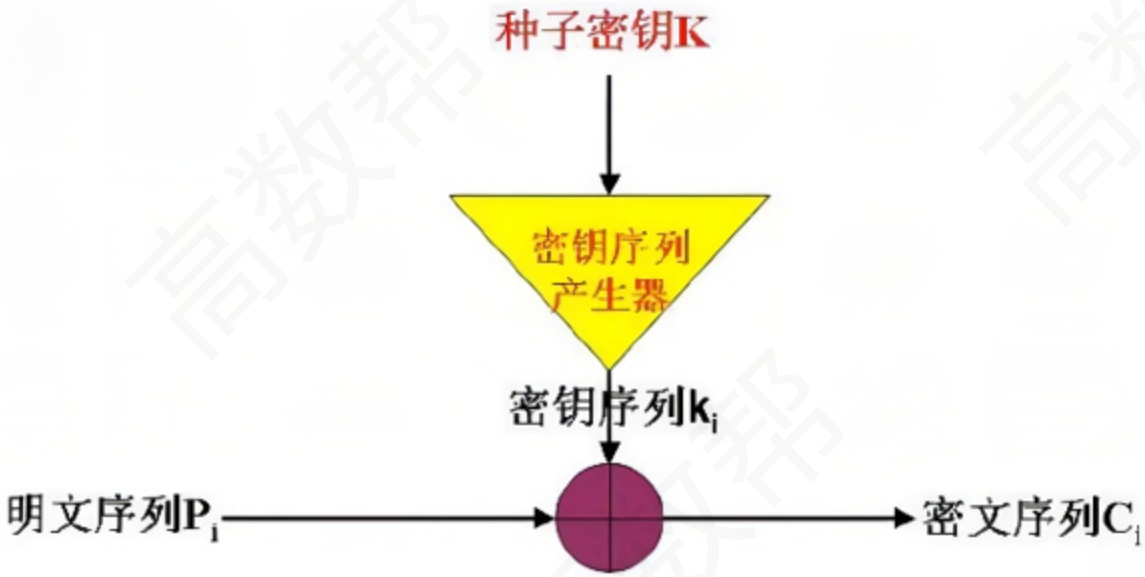
4、输出反馈(OFB)

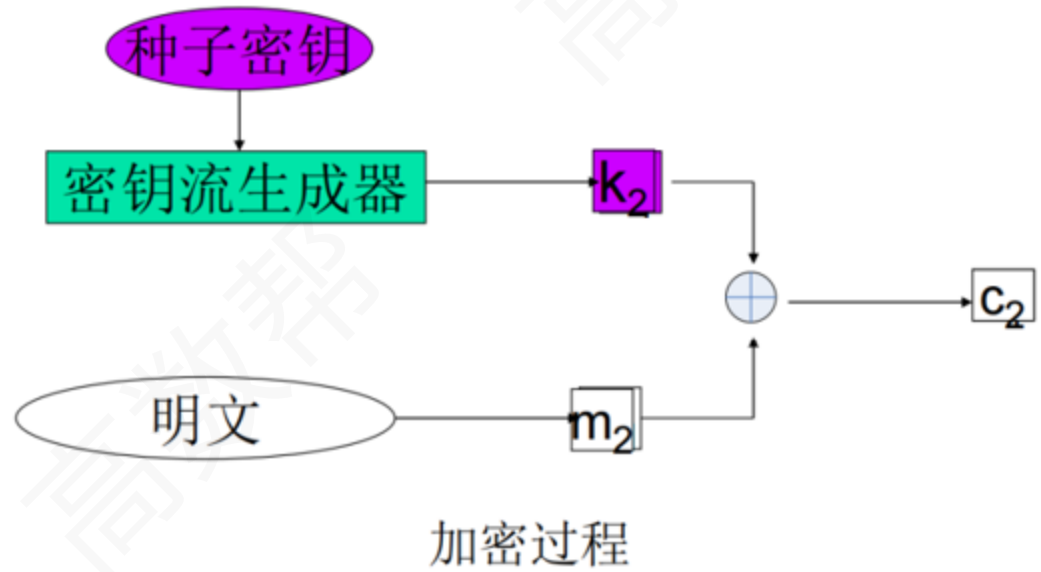
- 相同明文用相同密钥加密得到不同密文



六、序列密码

- 加解密只是异或
- 序列密码算法的设计关键在于密钥流生成器

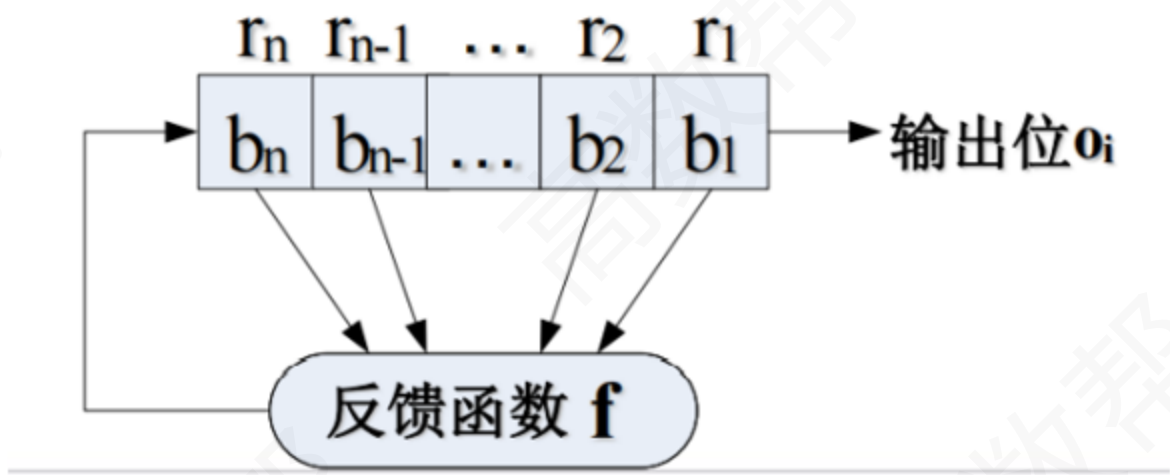




加密过程

七、反馈移位寄存器

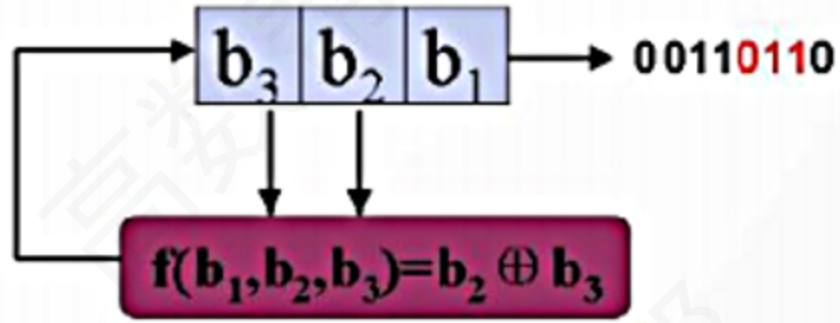
反馈移位寄存器（feedback shift register,FSR）是由n位的寄存器和反馈函数（feedback function）组成，如下图所示，n位的寄存器中的初始值称为移位寄存器的初态。



七、反馈移位寄存器

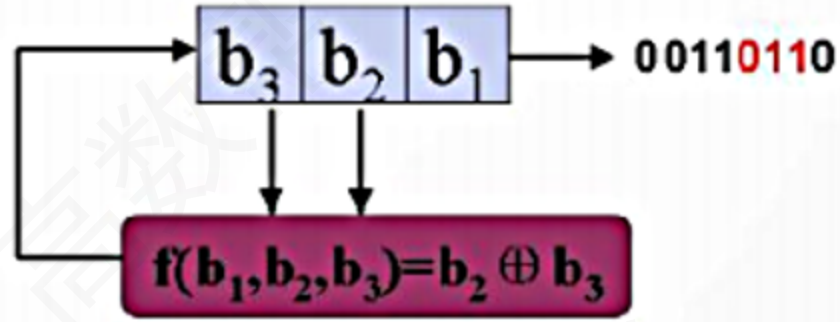
一个3-级的反馈移位寄存器，反馈函数为f(x)， f(x)=b2⊕b3，初态为100，输出序列生成过程如下:

状态	输出位
100	0
110	0
011	1
101	1
110	0
011	1
101	1
110	0



扫码观看
视频讲解更清晰

七、反馈移位寄存器



	b3		b2	b1	输出
	1	⊕	0	0	0
1⊕0	1		1	0	0
1⊕1	0		1	1	1
0⊕1	1		0	1	1
1⊕0	1		1	0	0
1⊕1	0		1	1	1
0⊕1	1		0	1	1
1⊕0	1		1	0	0

- 最后一位输出
- 反馈函数结果输入

七、反馈移位寄存器

- 移位寄存器的周期是指输出序列中连续且重复出现部分的长度。上面输出序列周期长度为3。
- 只要选择合适的反馈函数便可使序列的周期达到最大值 2^n-1，周期达到最大值的序列称为m序列。

1⊕0	1	1	0	0
1⊕1	0	1	1	1
0⊕1	1	0	1	1
1⊕0	1	1	0	0
1⊕1	0	1	1	1
0⊕1	1	0	1	1
1⊕0	1	1	0	0

八、RC4

- 至少128bit密钥
- 密钥调度算法+伪随机数生成算法

1. S、T初始化
2. 数据表S的初始置换

} 密钥调度方法（KSA）

3. 密钥流的生成 伪随机数生成方法（PRGA）

4. 加密
5. 解密

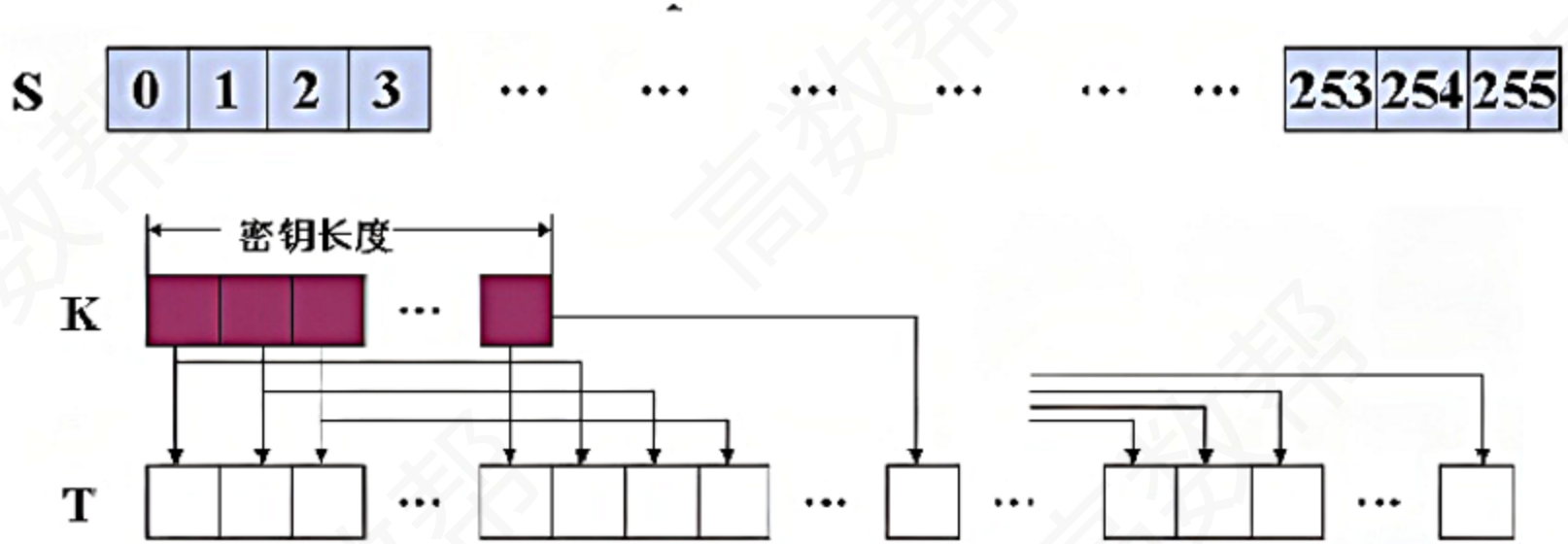
} 异或

扫码观看
视频讲解更清晰

八、RC4

1、S、T初始化

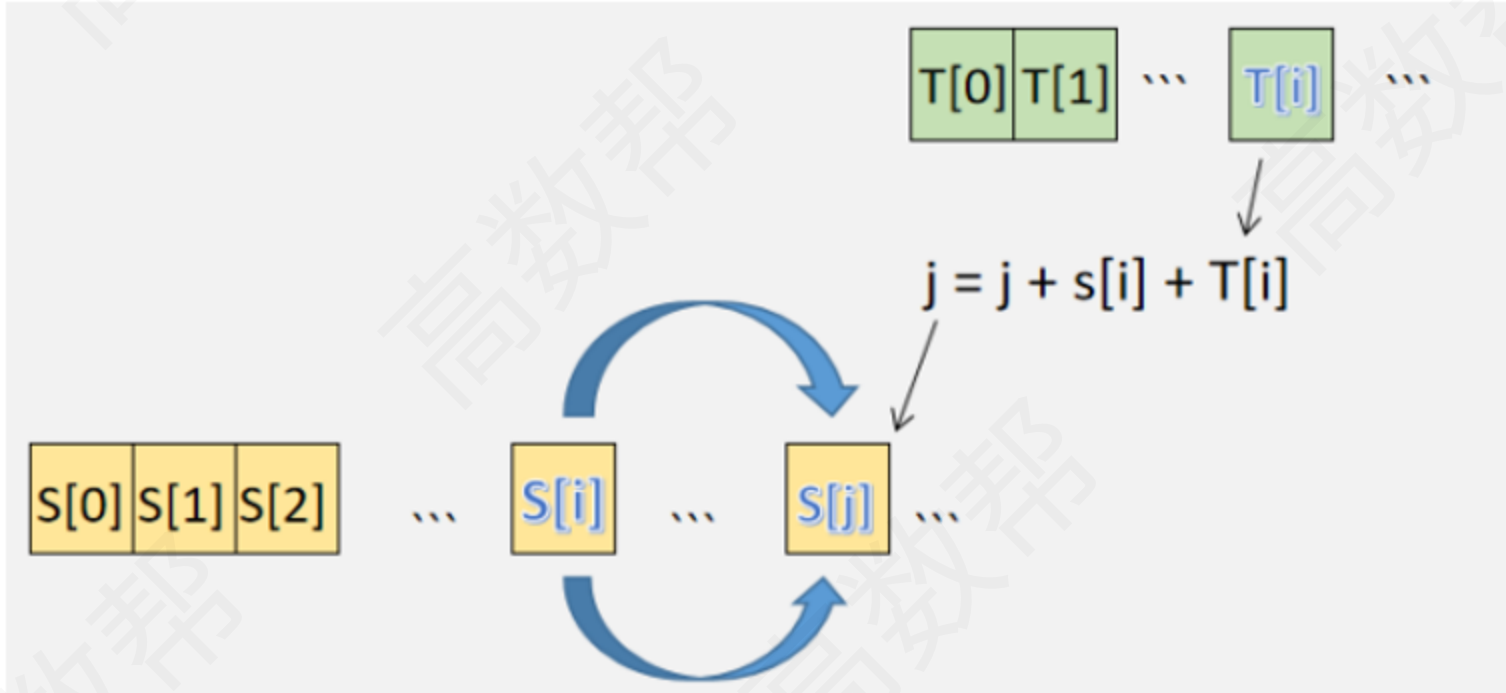
- S顺序填充
- T按照密钥顺序填充



八、RC4

2、数据表S的初始置换

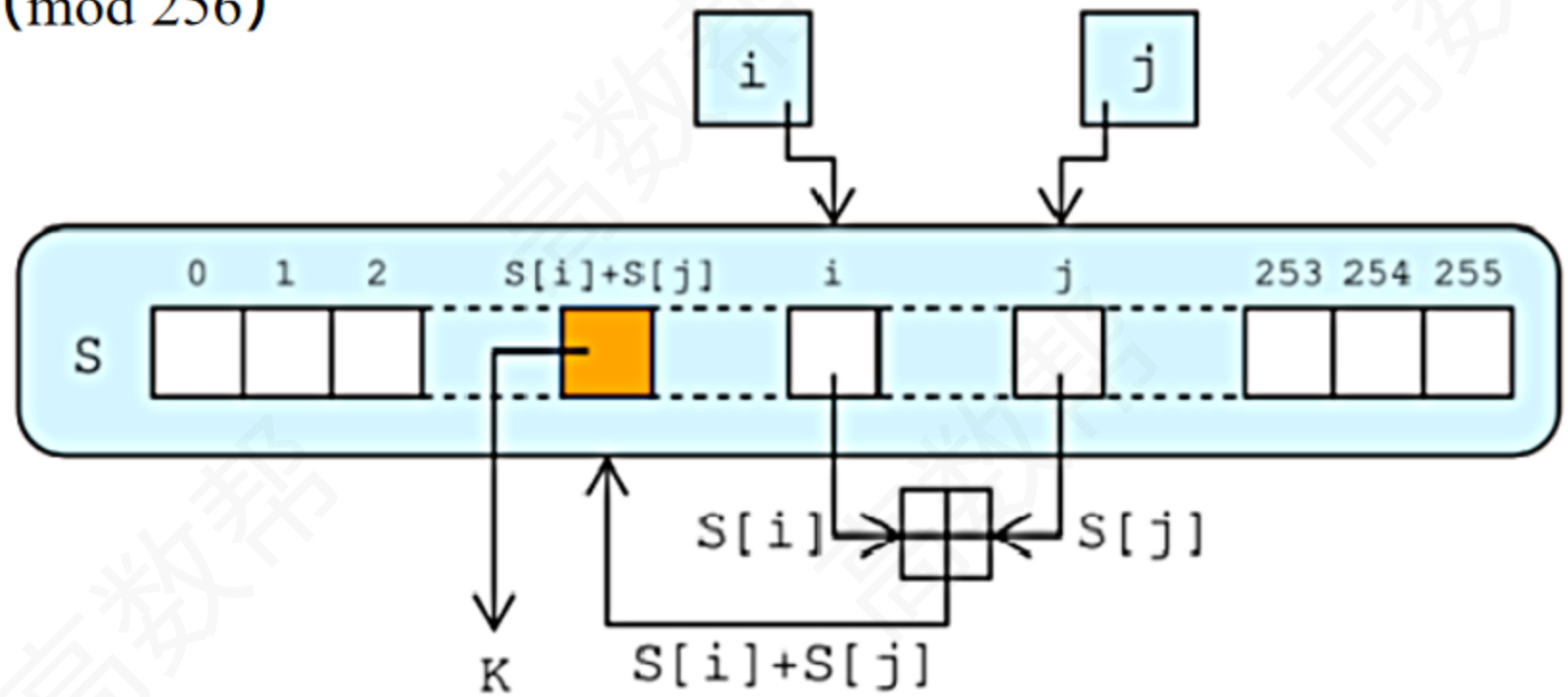
- **计算j的值** j = j+S[i]+T[i]
- **交换**S[i]、S[j]



八、RC4

3、密钥流的生成

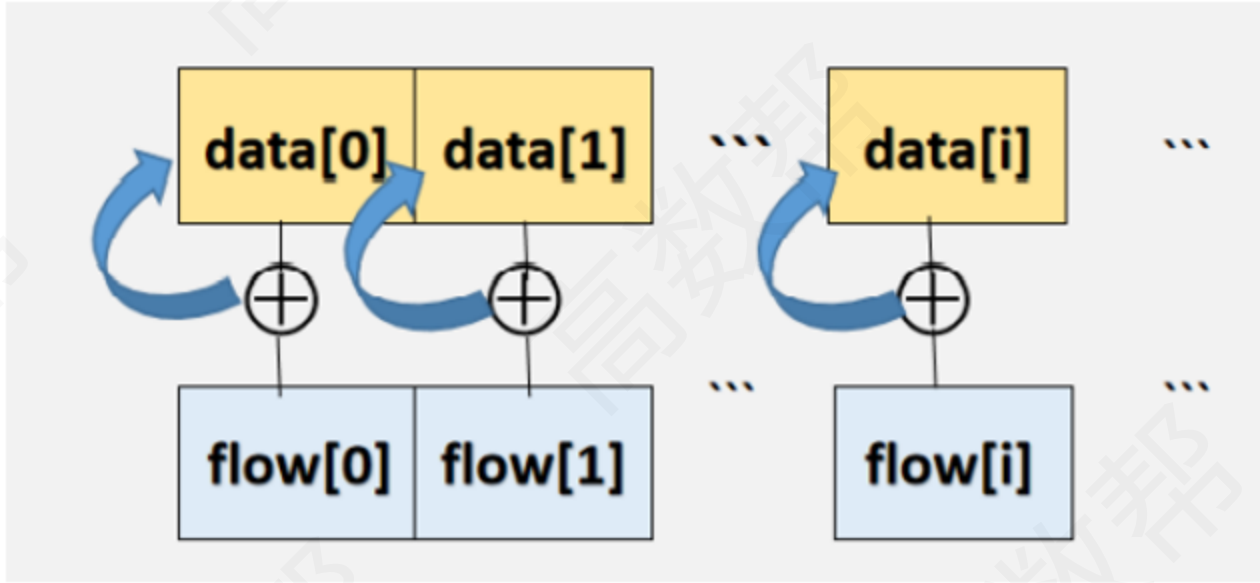
- 计算i、j 【i=i+1(mod 256)】【j=j+S[i] (mod 256)】
- 交换S[i]、S[j]
- 计算t=S[i]+S[j]（mod 256）
- S[t]即为密钥



八、RC4

4、加密解密

- 异或：相同为0 、不同为1



八、RC4

【题1】RC4算法中，假设使用3位的RC4数据表为S，密钥数据表为T，根据RC4算法进行如下操作：

（1）选取密钥，规则如下:你的学号后三位，作为密钥，填充密钥数据表T的元素。

（2）根据密钥调度算法完成数据表S的随机化。

密钥调度算法:

```
j:=0;
    for i=0 to 7 do
        j:=(j+s(i)+T(i))mod 8;
        swap(S(i),S(j));
```

扫码观看
视频讲解更清晰

八、RC4

请根据上述描述填充完成下列题目（表格下方数字为序号）：

（1）密钥数据表T如下，请填充表格元素（5分）：

（2）密钥调度算法完成后，数据表S就被随机化，请填充表格元素（5分）：

八、RC4

1、S、T初始化

- 假如使用3位(从0到7)的RC4，其操作是对8取模(而不是对256取模)。数据表S只有8个元素，初始化为:

S	0	1	2	3	4	5	6	7
	0	1	2	3	4	5	6	7

- 选取一个密钥，该密钥是由0到7的数以任意顺序组成的。例如选取5、6和7作为密钥。该密钥如下填入密钥数据表中:

T	5	6	7	5	6	7	5	6
	0	1	2	3	4	5	6	7

八、RC4

2. 数据表S的初始置换

```
j:=0;
for i=0 to 7 do
    j:=(j+s(i)+T(i)) mod 8;
    swap(S(i),S(j));
```

① 该循环以j=0和i=0开始。使用更新公式后j为： j=(0+S(0)+T(0)) mod 8=5

S数据表的第一个操作是将S(0)与S(5)互换。

八、RC4

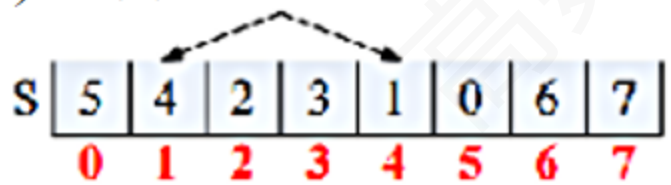
```
j:=0;
for i=0 to 7 do
    j:=(j+s(i)+T(i)) mod 8;
    swap(S(i),S(j));
```

2. 数据表S的初始置换

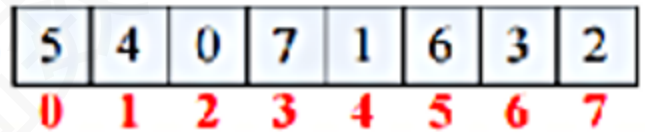
② 索引i加1后，j的下一个值为:

$$j=(5+S(1)+T(1)) \bmod 8=(5+1+6) \bmod 8=4$$

即将S数据表的S(1)和S(4)互换:



当该循环执行完后，数据表S就被随机化:



八、RC4

3.密钥流的生成

- 计算i、j

  【 i=i+1(mod 256) 】

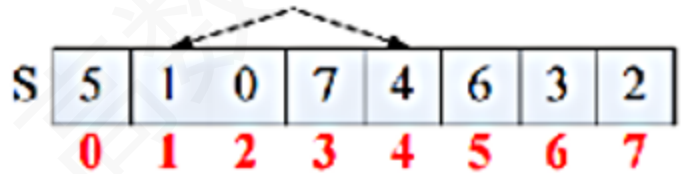
  【 j=j+S[i] (mod 256) 】
- 交换 S[i]、S[j]
- 计算 t=S[i]+S[j](mod 256)
- S[t]即为密钥

① 从j=0和i=0开始，RC4如下计算第一个密钥字:

i=(i+1) mod 8=(0+1) mod 8 =1

j=(j+s(i)) mod 8=(0+s(1)) mod 8=(0+4) mod 8=4

② swap S(1) 和 S(4)



③ 计算 t=S[1]+S[4]（mod 256）= 1+4 = 5

④ S[t] =S[5]=6 即为密钥

【题1】DES和AES不同?

（1）AES 密钥长度可变，DES 不可变

（2）DES 面向比特运算，AES 面向字节运算

扫码观看
视频讲解更清晰