

#### 《现代密码学》第四讲

## 分组密码 (三)





## 上讲内容回顾

- ▶ DES算法的整体结构——Feistel结构
- ▶ DES算法的轮函数
- ▶ DES算法的密钥编排算法
- > DES的解密变换





## 本节主要内容

- ●AES算法的整体结构
- ●AES算法的轮函数
- ●AES算法的密钥编排算法
- ●AES的解密变换





## 本节主要内容

- ●AES算法的整体结构
- AES算法的轮函数
- ●AES算法的密钥编排算法
- ●AES的解密变换





## AES的概述

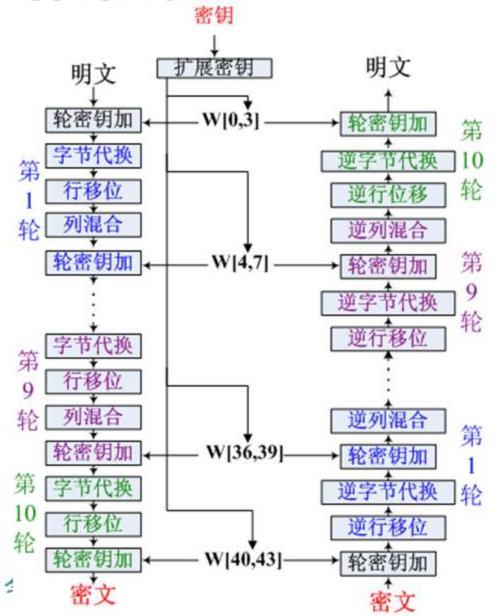
设计者: Joan Bagmen和Vincent Rijmen 高级数据加密标准 (Advanced Encryption Standard, AES) Rijndael 二〉AES

版本	密钥长度	分组长度	迭代轮数
加入小	(Nk words)	(Nb words)	(Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14



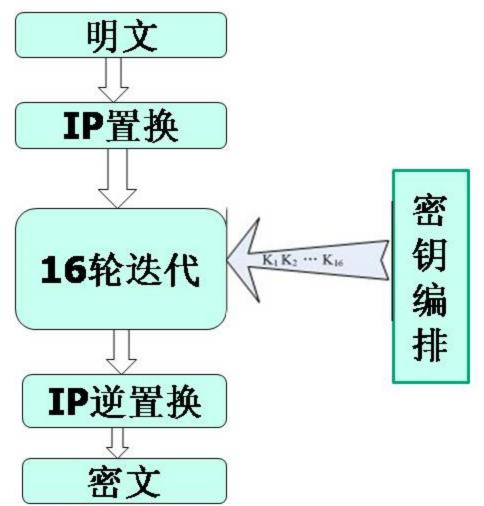
## AES的整体结构





## AES的整体结构









## 本节主要内容

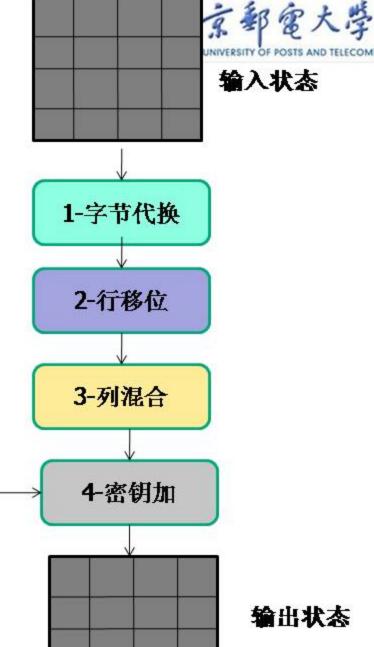
- ●AES算法的整体结构
- ●AES算法的轮函数
- AES算法的密钥编排算法
- ●AES的解密变换



## AES的轮函数

- 1) 字节代换 (SubByte)
- 2) 行移位 (ShiftRow)
- 3) 列混合 (MixColumn)
- 4) 密钥加 (AddRoundKey)

轮密钥





输出状态



## 1-字节代换 (ByteSub)

$a_{00}$	$a_{01}$	$a_{02}$	$a_{03}$	代换 表	$b_{00}$	$b_{01}$	$b_{02}$	$b_{03}$
$a_{10}$		2	$a_{13}$		$b_{10}$	I P	).; 2	$b_{13}$
$a_{20}$	$d_{ZI}$	!ij 2.	$a_{23}$		$b_{20}$	$b_{21}^{-6}$	0 <sub>ij</sub> 2	$b_{23}$
$a_{30}$	$a_{31}$	$a_{32}$	$a_{33}$		$b_{30}$	$b_{31}$	$b_{32}$	$ b_{33} $





## 1-字节代换 (ByteSub)

	0	1	2	3	4	5	6	7	8	9	A	В	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	<b>C5</b>	30	01	67	2B	FE	D7	AB	76
1	CA	82	С9	7D	FA	59	47	FO	AD	D4	A2	AF	9C	A4	72	co
2	B7	FD	93	26	36	3F	F7	CC	34	A5	<b>E</b> 5	F1	71	D8	31	15
3	04	<b>C</b> 7	23	СЗ	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	AO	52	3B	D6	В3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5 <b>B</b>	6A	СВ	BE	39	4A	4C	58	CF
6	DO	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	В6	DA	21	10	FF	F3	D2
8	CD	OC	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	ОВ	DE
A	EO	32	3A	OA	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
В	E7	С8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
С	BA	78	25	2E	1C	A6	B4	<b>C6</b>	E8	DD	74	1F	4B	BD	8B	84
D	70	3E	B5	66	48	03	F6	0E	61	35	57	В9	86	C1	1D	9I
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	OD	BF	E6	42	68	41	99	2D	0F	ВО	54	BB	16





## 2-行移位 (ShiftRow)

$a_{00}$	$a_{0I}$	$a_{02}$	$a_{03}$	不移位	$\rightarrow a_{00}$	$a_{01}$	$a_{02}$	$a_{03}$
$a_{10}$	$a_{II}$	$a_{12}$	$a_{13}$	左循环 1字节	$\rightarrow a_{11}$	$a_{12}$	$a_{13}$	$a_{10}$
$a_{20}$	$a_{21}$	$a_{22}$	$a_{23}$	左循环 2字节	$\rightarrow a_{22}$	$a_{23}$	$a_{20}$	$a_{21}$
$a_{30}$	$a_{3I}$	$a_{32}$	<i>a</i> <sub>33</sub>	<u>左循环</u> 3字节	$\rightarrow a_{33}$	$a_{30}$	$a_{3I}$	$a_{32}$





## 3-列混合(MixColumn)

$a_{00}$	$a_{01}$	$a_{02}$	$a_{03}$	$a_{0j}$
$a_{10}$	$a_{11}$	$a_{12}$	<i>a</i> <sub>13</sub>	$a_{1j}$
$a_{20}$	$a_{21}$	$a_{22}$	$a_{23}$	$a_{2j}$
$a_{30}$	$a_{3I}$	$a_{32}$	$ a_{33} $	$ a_{3j} $





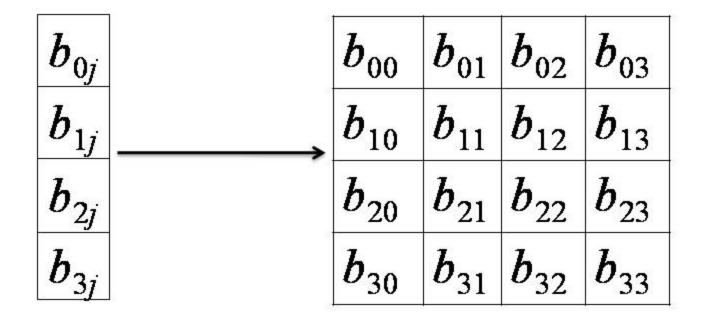
## 3-列混合 (MixColumn)

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix}$$





## 3-列混合 (MixColumn)





▶ AES选择的既约多项式为  $m(x)=x^8+x^4+x^3+x+1$ 

▶ GF (28) 上的元素表示方法: 字节表示 Byte:  $a_7a_6a_5a_4a_3a_2a_1a_0$ 多项式表示 s(x):  $s(x) = a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ 

m(x) 字节表示:00000001 00011011 (0x011B)





[5]: 
$$0x57 + 0x83 = ?$$
  
 $(x^6+x^4+x^2+x+1) + (x^7+x+1)=x^7+x^6+x^4+x^2$   
 $0x57 + 0x83 = 0xD4$   
[5]:  $0x57 \times 0x83 = ?$   
 $(x^6+x^4+x^2+x+1) \times (x^7+x+1)$   
 $=(x^{13}+x^{11}+x^9+x^8+x^7)+(x^7+x^5+x^3+x^2+x)+(x^6+x^4+x^2+x+1)$   
 $=x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1$   
 $=x^7+x^6+1 \mod m(x)=x^8+x^4+x^3+x+1$ 



GF(28) 上的快速乘法:

1)  $a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0 \times 0x02 / a(x) \times x$ 

- ▶ 当字节的最高位为0时(a(x)的7次项系数为0),左移补0;
- ▶ 当字节的最高位为1时 (a(x)的7次项系数为1),左移补0,再按位模0x011B







- GF (28) 上的快速乘法:
  - 2)  $a_7a_6a_5a_4a_3a_2a_1a_0 \times b_7b_6b_5b_4b_3b_2b_1b_0 / \mathbf{a}(x) \times \mathbf{b}(x)$

$$[a(x) \times b(x)] \mod m(x) =$$
  
{  $[a(x) \mod m(x)] \times [b(x) \mod m(x)]$ }  $\mod m(x)$ 

$$\boldsymbol{a}(x) \times [\boldsymbol{b}(x) + c(x)] = \boldsymbol{a}(x) \times \boldsymbol{b}(x) + c(x) \times \boldsymbol{a}(x)$$

$$a(x) \times b(x) =$$



$$[b_0 \times a(x)]$$

$$+ [b_{1}x \times a(x)] \quad A^{(0)} = a(x) \bmod m(x)$$

$$+ [b_{2}x^{2} \times a(x)] \quad A^{(1)} = x \times a(x) = x \times A^{(0)} \bmod m(x)$$

$$+ [b_{3}x^{3} \times a(x)] \quad A^{(2)} = x^{2} \times a(x) = x \times A^{(1)} \bmod m(x)$$

$$+ [b_{4}x^{4} \times a(x)] \quad A^{(3)} = x^{3} \times a(x) = x \times A^{(2)} \bmod m(x)$$

$$+ [b_{5}x^{5} \times a(x)] \quad A^{(4)} = x^{4} \times a(x) = x \times A^{(3)} \bmod m(x)$$

$$+ [b_{6}x^{6} \times a(x)] \quad A^{(5)} = x^{5} \times a(x) = x \times A^{(4)} \bmod m(x)$$

$$+ [b_{7}x^{7} \times a(x)] \quad A^{(6)} = x^{6} \times a(x) = x \times A^{(5)} \bmod m(x)$$

$$+ [b_{7}x^{7} \times a(x)] \quad A^{(6)} = x^{6} \times a(x) = x \times A^{(6)} \bmod m(x)$$

$$+ [a_{7}x^{7} \times a(x)] \quad A^{(6)} = x^{6} \times a(x) = x \times A^{(6)} \bmod m(x)$$

$$a(x) \times b(x) = b_0 A^{(0)} + b_1 A^{(1)} + b_2 A^{(2)} + b_3 A^{(3)} + b_4 A^{(4)} + b_5 A^{(5)} + b_6 x^6 A^{(6)} + b_7 A^{(7)}$$





## 3-列混合 (MixColumn)

#### 课堂练习: 列混合运算(128比特分组)

(02	03	01	01)	ľ	87		47	
					6E		37	
01	01	02	01 03	•	46	=	94	
03	01	01	02)		<b>A</b> 6		ED	





## 4—密钥加 (AddRoundKey)

a <sub>00</sub>	<i>a</i> <sub>01</sub>	a <sub>02</sub>	a <sub>03</sub>
a <sub>10</sub>	a <sub>11</sub>	a <sub>12</sub>	a <sub>13</sub>
a <sub>20</sub>	a <sub>21</sub>	a <sub>22</sub>	a <sub>23</sub>
a <sub>30</sub>	a <sub>31</sub>	a <sub>32</sub>	a <sub>33</sub>



$k_{00}$	k <sub>01</sub>	$k_{02}$	$k_{03}$
k <sub>10</sub>	k <sub>11</sub>	k <sub>12</sub>	k <sub>13</sub>
k <sub>20</sub>	k <sub>21</sub>	k <sub>22</sub>	k <sub>23</sub>
k <sub>30</sub>	k <sub>31</sub>	k <sub>32</sub>	k <sub>33</sub>

$b_{00}$	$b_{01}$	$b_{02}$	$b_{03}$
b <sub>10</sub>	b <sub>11</sub>	b <sub>12</sub>	$b_{13}$
b <sub>20</sub>	$b_{21}$	b <sub>22</sub>	b <sub>23</sub>
b <sub>30</sub>	$b_{31}$	$b_{32}$	$b_{33}$



## 本节主要内容

- AES算法的整体结构
- AES算法的轮函数
- ●AES算法的密钥编排算法
- ●AES的解密变换





密钥编排指从种子密钥得到轮密钥的过程,AES的密钥编排由密钥扩展和轮密钥选取两部分组成,其基本原则如下:

- ▶1)轮密钥的总比特数等于轮数加1再乘以分组长度;如128比特的明文经过10轮的加密,则总共需要(10+1)\*128=1408比特的密钥.
- >2) 种子密钥被扩展成为扩展密钥;
- >3)轮密钥从扩展密钥中取,其中第1轮轮密钥取扩展密钥的前N<sub>b</sub>个字,第2轮轮密钥取接下来的N<sub>b</sub>个字,依次类推.





#### ▶1) 密钥扩展

扩展密钥是以4字节字为元素的一维阵列,表示为 $W[Nb*(N_r+1)]$ ,其中前 $N_k$ 个字取为种子密钥,以后每个字按递归方式定义. 扩展算法根据 $N_k$ <6和 $N_k$ >6有所不同。



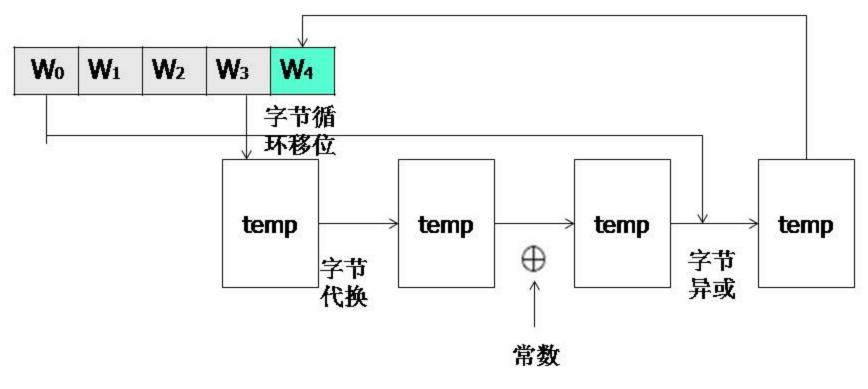


当Nk≤6时,扩展算法如下:

```
KeyExpansion (byteKey[4*Nk], W[Nb*(Nr+1)])
   for (i = 0; i < Nk; i ++)
    W[i]=(Key[4*i], Key[4*i+1], Key[4*i+2], Key[4*i+3]);
    for (i = Nk; i < Nb*(Nr+1); i ++)
    temp=W[i-1];
    if (i % Nk = 0)
            temp=SubByte (RotByte (temp)) Rcon[i /Nk];
    W[i]=W[i-Nk] temp:
```



$$i=4$$
  $i\%4==0$ 

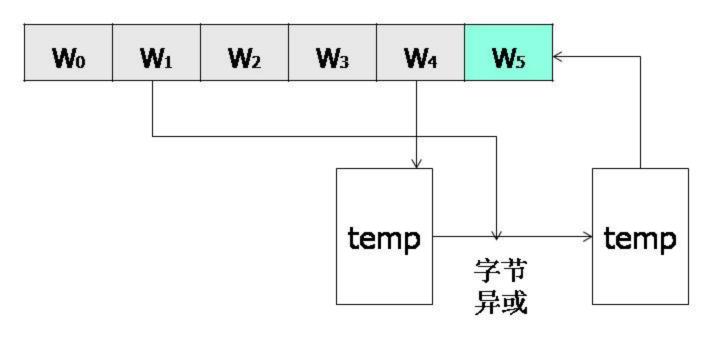


Nk=4





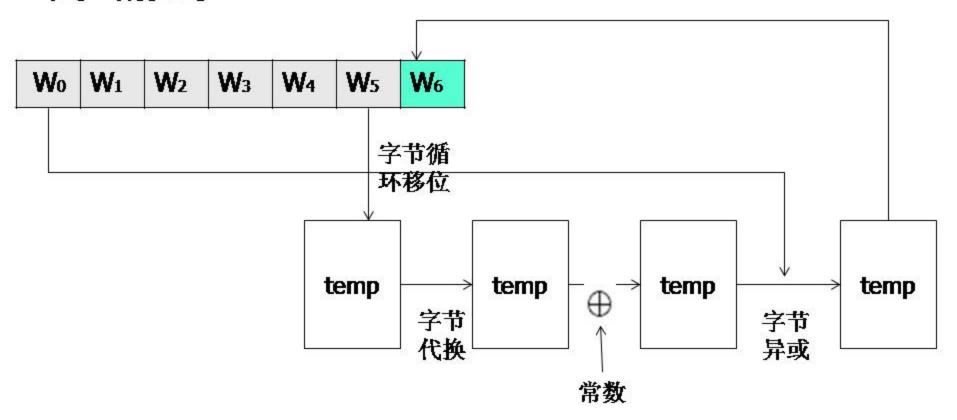
 $i=55\%4 \neq 0$ 







i=6 i%6 = = 0



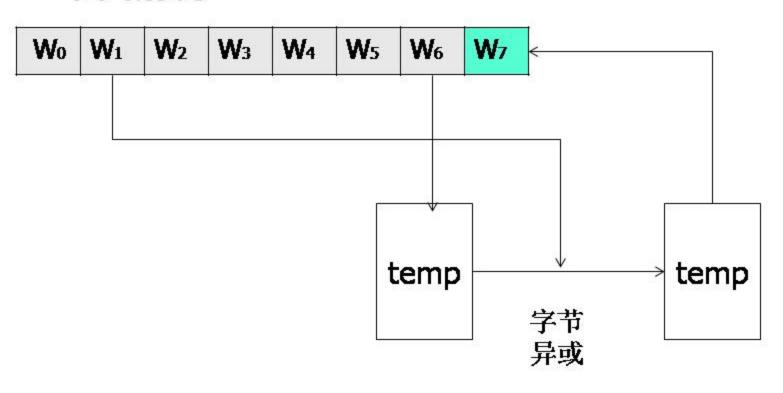
Nk=6



#### 北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIO

## AES算法的密钥编排算法

i=7 i%6 ±0







- Key[4\*Nk]为种子密钥,看作以字为元素的一维 阵列;
- 函数SubByte()返回4字节字,其中每一个字 节都是用Rijndael的S盒作用到输入字对应的字节 得到;
- 函数RotByte() 也返回4字节字,该字由输入的字循环移位得到,即当输入字为(a, b, c, d)时,输出字为(b, c, d, a).

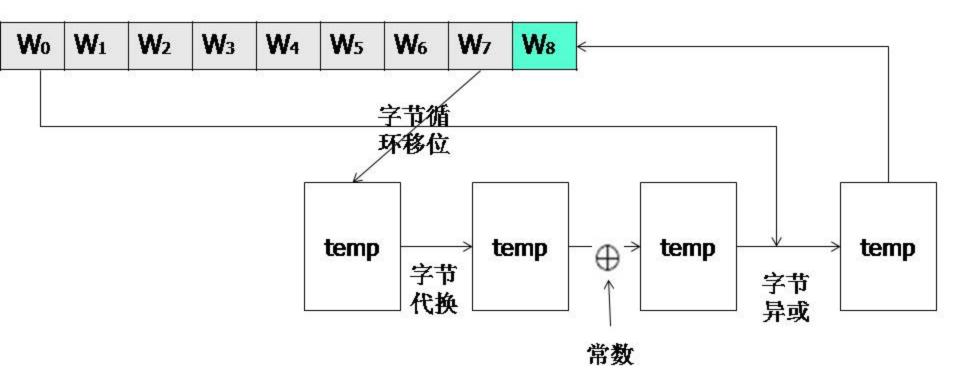




```
当Nk>6时,扩展算法如下:
KeyExpansion (byte Key[4*Nk], W[Nb*(Nr+1)])
    for (i=0; i < Nk; i ++)
    W[i] = (Key[4*i], Key[4*i+1], Key[4*i+2], Key[4*i
+3]):
for (i = Nk; i < Nb*(Nr+1); i ++)
     temp=V[i-1]:
    if (i % Nk = = 0)
         temp=SubByte (RotByte (temp)) Rcon[i /Nk];
       else if (i % Nk=4)
           temp=SubByte (temp);
W[i] = W[i - Nk]^{\hat{}} temp:
```



i=8i%8 = = 0

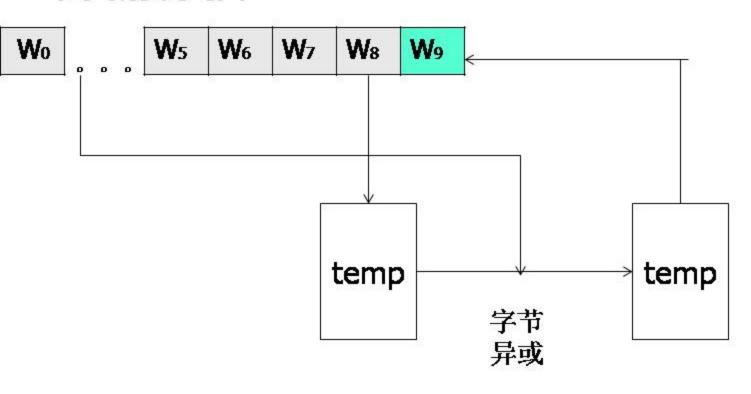






北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

i=9 i%8 ≠0 or 4

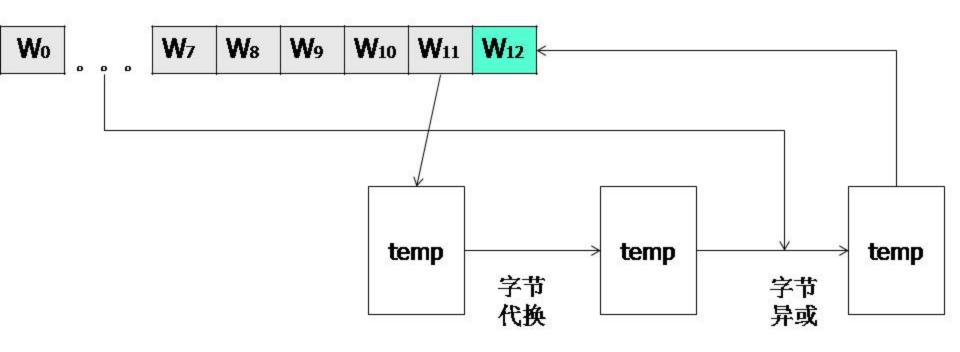






# AES算法的密钥编排算法 BEDING UNIVERSITY OF POSTS AND TELECOM

$$i=12$$
  $i\%8==4$ 



Nk=8





Rcon[i/Nk] 为轮常数,其值与Nk无关,定义为 (字节用十六进制表示,同时理解为GF(28)上的 元素):

```
Rcon [i]=(RC[i], 00, 00, 00)
其中RC[i] 是GF(28) 中值为x<sup>i-1</sup>的元素,因此
RC[1] =1(即'01')
RC[2] = x(即'02')
RC[i]=x•RC[i-1]= x<sup>i-1</sup>
```





#### ▶2) 轮密钥选取

轮密钥i(即第i 个轮密钥)由轮密钥缓冲字 ₩[Nb\* i]到₩[Nb\*(i+1)]给出:

$W_0$	$\mathbf{W}_1$	$\mathbf{W}_2$	<b>W</b> <sub>3</sub>	$W_4$	$W_5$	$W_6$	$W_7$	0	0	0	$\mathbf{W}_{40}$	$W_{41}$	W <sub>42</sub>	$W_{43}$	
-------	----------------	----------------	-----------------------	-------	-------	-------	-------	---	---	---	-------------------	----------	-----------------	----------	--

轮密钥0

轮密钥1

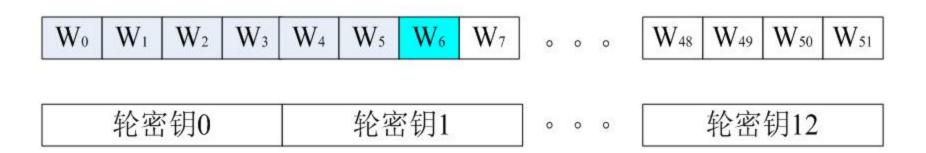
0 0 0

轮密钥10

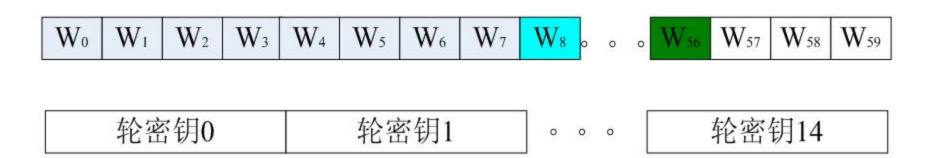
Nb=4及Nk=4时的密钥扩展与轮密钥选取







#### Nb=4及Nk=6时的密钥扩展与轮密钥选取



Nb=4及Nk=8时的密钥扩展与轮密钥选取





## 本节主要内容

- ●AES算法的整体结构
- AES算法的轮函数
- ●AES算法的密钥编排算法
- ●AES的解密变换





## AES 的解密变换

AES解密运算是加密运算的逆运算,其中轮函数的逆为:

•1) By te Sub的逆变换由代换表的逆表做字节代换, 也可通过如下两步实现: 首先进行仿射变换的逆 变换,再求每一字节在GF(28)上逆元.

•2) 行移位运算的逆变换是循环右移,位移量与 左移时相同.





## AES的解密变换

•3) 列混合运算的逆运算是类似的,即每列都用一个特定的多项式d(x)相乘,d(x)满足

$$(03x^3+01x^2+01x+02)*d(x)=01$$

由此可得

$$d(x) = 0Bx^3 + 0Dx^2 + 09x + 0E$$

•4) 密钥加运算的逆运算是其自身。





## 主要知识点小结

> AES算法的整体结构

▶ AES算法的轮函数



扩散与混淆



000000	1110	000001	00000	1000000	o maoo	1000000	111111
00000110	0100	0000111	111111	1000000	00001	1000001	1110000
000100	1101	<b>099101</b>	01111	1000000	111111110	1000010	100000
0001110	0001	000011111	01 D <b>6</b> 0	1000100	100000	1000011	D00010
0011000	0010	<b>OOKOO</b> II	111D0	1000000	1110101	1010000	D10000
<b>00110110</b>	1111	<b>001101111</b>	0 <b>0</b> 01D0	1000000	ommo	1010101	100001
<b>0011100</b>	1011	0011101	11LDQ1	1001000	000010	1010010	D00001
0011110	1000	0011111	000011	1001100	1010111	1010111	D10111
<b>010000</b>	0011		1D01D0	1100000	111111111	1100000	D10101
	1010		OT LED	1100000	1110000	1100001	<b>101011</b>
	0110	<b>OHOHOI</b>	111D000	1100000	10001	1101010	DOOD11
	1100	0101111	1D0111	1100100	O DIII 1	1101011	<b>110101</b>
<b>O111000</b>	0101	011001	1D0011	1110000	0000111	1110000	1101010
<b>OIIIOIO</b>	1001	<b>01110111</b>	Provide September 1	1110000	SECRETARIST CONTROLLER		
	0000			1111000	The second secon	A 10 10 10 10 10 10 10 10 10 10 10 10 10	
	0111		1D000	1111100	ommo	1111111	1111010
2022							





## THE END!

