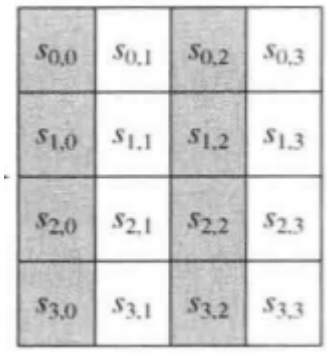
AES加密解析

• AES加密过程：

为方便概述，这里以16字节规格的明文为例子。直接开始讲过程。



这是输入的明文矩阵。矩阵中的一个元素代表一个字节，字节有8个比特。化成16进制就是两位16进制的数。

步骤一

字节代替（Substitute Bytes）：用S盒完成；

举例：取明文中的 $S_{0,0}$假设值为{A5}，那么就找到s盒中的第十行第五列，然后把{A5}改成s盒中对应的数字。

x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	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	B6	DA	21	10	FF	F3	D2
8	CD	0C	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	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

这个是s盒，以上述为例，{A5}改成{06}

重点理解S盒构造方法：

1. 初始化S盒，为{00}{01}...{FF}
2. 求S盒中对应的值在$GF(2^8)$下的逆元。举例{F5}转化成二级制为11110101. 对应的多项式为：$x^7+x^6+x^5+x^4+x^2+1$。也就是设多项式y使得

$$y*(x^7+x^6+x^5+x^4+x^2+1)\equiv 1(mod \quad x^8+x^4+x^3+x+1)$$

最终可求得$y=x^6+x^2+x$,转化成二级制就是01000110，也就是{46}。

接着根据约定俗成的矩阵相乘得到一个新的二进制数。

$$\begin{bmatrix}1&0&0&0&1&1&1&1\\1&1&0&0&0&1&1&1\\1&1&1&0&0&0&1&1\\1&1&1&1&0&0&0&1\\1&1&1&1&1&0&0&0\\0&1&1&1&1&1&0&0\\0&0&1&1&1&1&1&0\\0&0&0&1&1&1&1&1\end{bmatrix}\begin{bmatrix}b_0\\b_1\\b_2\\b_3\\b_4\\b_5\\b_6\\b_7\end{bmatrix}$$

其中在求得y之后，按低位向高位以此向下排列，与矩阵相乘。

可求得位列向量$b_0 \sim b_7$= {10100001}.

在求得位列向量之后，把该向量与{11000110}取异或操作。

$$\begin{bmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

所以得$b_7' \sim b_0'$为{11100110}。也就是{E6}。查S盒的表可得，第F行第5列为{E6}。

构造S盒的难点在于求多项式的逆元，请大家要熟练掌握求多项式的逆元。

步骤二

行移位（ShiftRows）：置换

对于已经进行过字节代替的明文，行位移的做法是第0行向左移动0个字节，第1行向左移动1个字节，把
溢出的字节添在丢失的字节位上。

步骤三

列混淆（MixColumns）：利用$GF(2^8)$

书上的方法可能看起来比较难以理解，所以我打算用自己的方法来写。
当我们在步骤二完成后，已经求出了一个全新的矩阵，现在我们需要把这个矩阵乘以一个规定的矩阵。

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} = \begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}$$作为其中的一个例子，我们计算一下{03}*$S_{1,0}$。

把{03}转化成16进制，{00000011}.对应的多项式为$x+1$.那么现在就是求
$[(x+1)*S_{1,0}] \quad mod(x^8+x^4+x^3+x+1)$

那么问题就又转化成多项式的乘法与加法，并且在$GF(2^8)$的有限域下进行，即结果都要
$mod(x^8+x^4+x^3+x+1)$
以上方法虽然麻烦点，但是便于理解。当理解上述方法后，就可以看懂书上的方法了。

步骤四

轮密钥加变换
这步骤十分简单，不说了。