甘赞栩 GAN ZAN XU 学号：2020131129

G→71→0x47 A →65 →0x41 N →78 →0x4E space →32 →0x20 Z →90 →0x5A A →65 →0x41

N →78 →0x4E space →32 →0x20 X →88 →0x58 U →85 →0x55

0 →48 →0x30 1 →49 →0x31 2 →50 →0x32 3 →51 →0x33 9 →57 →0x39

则明文为：0x47414E205A414E20 5855 0000 0000 0006

密文为：0x3230323031333131 3239 0000 0000 0006

明文

47	5A	58	00
41	41	55	00
4E	4E	00	00
20	20	00	06

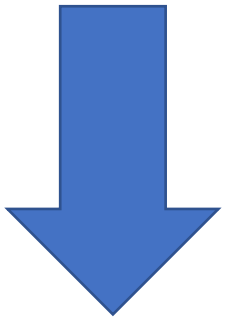
密文

32	31	32	00
30	33	39	00
32	31	00	00
30	31	00	06

1.轮密钥加

47	5A	58	00
41	41	55	00
4E	4E	00	00
20	20	00	06

32	31	32	00
30	33	39	00
32	31	00	00
30	31	00	06



异或

75	6B	6A	00
71	72	6C	00
7C	7F	00	00
10	11	00	00

1.字节代替

75	6B	6A	00
71	72	6C	00
7C	7F	00	00
10	11	00	00

字节代替

9D	7F	02	63
A3	40	50	63
15	D2	63	63
A9	82	63	6F

表4-9 AES算法的S盒（十六进制）

Y X	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

2.行移位

9D	7F	02	63
A3	40	50	63
15	D2	63	63
A9	82	63	6F

行移位

9D	7F	02	63
40	50	63	A3
63	63	15	D2
6F	A9	82	63

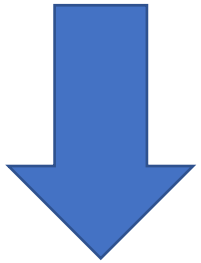
3.列混合

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

X

9D	7F	02	63
40	50	63	A3
63	63	15	D2
6F	A9	82	63

计算：



C4	F4	46	2E
67	8A	DA	57
75	4B	A2	D2
E3	26	5B	A3

4.轮密钥加

设初始密钥扩展之后下一轮子密钥（K_4、K_5、K_6、K_7）

密钥扩展：

32	31	32	00	32	4A	B2	62
30	33	39	00	30	58	5C	35
32	31	00	00	32	84	7B	6E
30	31	00	06	36	3D	1F	33
k0	k1	k2	k3	k4	k5	k6	K7

32	4A	B2	62
30	58	5C	35
32	84	7B	6E
36	3D	1F	33
k4	k5	k6	K7

32	4A	B2	62
30	58	5C	35
32	84	7B	6E
36	3D	1F	33

C4	F4	46	2E
67	8A	DA	57
75	4B	A2	D2
E3	26	5B	A3

轮密钥加

F6	BE	F4	4C
57	D2	86	36
47	CC	D9	A2
D5	1B	C2	90