

### 1. Transpo of state

State:		After Transpo
0x6353e08c		0x6309cdba
0x0960e104	→	0x536070ca
0xcd70b751		0xe0e1b7d0
0xbacad0e7		0x 8c0451e7

### 2. First row calc

						0x63	09	cd	ba
						0x53	60	70	ca
						0xe0	e1	b7	d0
						0x8c	04	51	e7
	0x02	03	01	01		0x5f	57	f7	1d
	0x01	02	03	01					
	0x01	01	02	03					
	0x03	01	01	02					

$$0x5f = 0x02 * 0x63 + 0x03 * 0x53 + 0x01 * 0xe0 + 0x01 * 0x8c = 0xc6 + 0xf5 + 0xe0 + 0x8c = 0x5f$$

$$0x57 = 0x02 * 0x09 + 0x03 * 0x60 + 0x01 * 0xe1 + 0x01 * 0x04 = 0x12 + 0xa0 + 0xe1 + 0x04 = 0x57$$

$$0xf7 = 0x02 * 0xcd + 0x03 * 0x70 + 0x01 * 0xb7 + 0x01 * 0x51 = 0x81 + 0x90 + 0xb7 + 0x51 = 0xf7$$

$$0x1d = 0x02 * 0xba + 0x03 * 0xca + 0x01 * 0xd0 + 0x01 * 0xe7 = 0x6f + 0x45 + 0xd0 + 0xe7 = 0x1d$$

### 3. Second row calc

						0x63	09	cd	ba
						0x53	60	70	ca
						0xe0	e1	b7	d0
						0x8c	04	51	e7
	0x02	03	01	01		0x5f	57	f7	1d
	0x01	02	03	01		0x72	f5	be	b9
	0x01	01	02	03					
	0x03	01	01	02					

$$0x72 = 0x01 * 0x63 + 0x02 * 0x53 + 0x03 * 0xe0 + 0x01 * 0x8c = 0x63 + 0xa6 + 0x3b + 0x8c = 0x72$$

$$0xf5 = 0x01 * 0x09 + 0x02 * 0x60 + 0x03 * 0xe1 + 0x01 * 0x04 = 0x09 + 0xc0 + 0x38 + 0x04 = 0xf5$$

$$0xbe = 0x01 * 0xcd + 0x02 * 0x70 + 0x03 * 0xb7 + 0x01 * 0x51 = 0xcd + 0xe0 + 0xc2 + 0x51 = 0xbe$$

$$0xb9 = 0x01 * 0xba + 0x02 * 0xca + 0x03 * 0xd0 + 0x01 * 0xe7 = 0xba + 0x8f + 0x6b + 0xe7 = 0xb9$$

#### 4. Third row calc

						0x63	09	cd	ba
						0x53	60	70	ca
						0xe0	e1	b7	d0
						0x8c	04	51	e7
	0x02	03	01	01		0x5f	57	f7	1d
	0x01	02	03	01		0x72	f5	be	b9
	0x01	01	02	03		0x64	bc	3b	f9
	0x03	01	01	02					

$$0x64 = 0x01 * 0x63 + 0x01 * 0x53 + 0x02 * 0xe0 + 0x03 * 0x8c = 0x63 + 0x53 + 0xdb + 0x8f = 0x64$$

$$0xbc = 0x01 * 0x09 + 0x01 * 0x60 + 0x02 * 0xe1 + 0x03 * 0x04 = 0x09 + 0x60 + 0xd9 + 0x0c = 0xbc$$

$$0x3b = 0x01 * 0xcd + 0x01 * 0x70 + 0x02 * 0xb7 + 0x03 * 0x51 = 0xcd + 0x70 + 0x75 + 0xf3 = 0x3b$$

$$0xf9 = 0x01 * 0xba + 0x01 * 0xca + 0x02 * 0xd0 + 0x03 * 0xe7 = 0xba + 0xca + 0xbb + 0x32 = 0xf9$$

#### 5. Fourth row calc

						0x63	09	cd	ba
						0x53	60	70	ca
						0xe0	e1	b7	d0
						0x8c	04	51	e7
	0x02	03	01	01		0x5f	57	f7	1d
	0x01	02	03	01		0x72	f5	be	b9
	0x01	01	02	03		0x64	bc	3b	f9
	0x03	01	01	02		0x15	92	29	1a

$$0x15 = 0x03 * 0x63 + 0x01 * 0x53 + 0x01 * 0xe0 + 0x02 * 0x8c = 0xa5 + 0x53 + 0xe0 + 0x03 = 0x15$$

$$0x92 = 0x03 * 0x09 + 0x01 * 0x60 + 0x01 * 0xe1 + 0x02 * 0x04 = 0x1b + 0x60 + 0xe1 + 0x08 = 0x92$$

$$0x29 = 0x03 * 0xcd + 0x01 * 0x70 + 0x01 * 0xb7 + 0x02 * 0x51 = 0x4c \wedge 0x70 \wedge 0xb7 \wedge 0xa2 = 0x29$$

$$0x1a = 0x03 + 0xba + 0x01 * 0xca + 0x01 * 0xd0 + 0x02 * 0xe7 = 0xd5 + 0xca + 0xd0 + 0xd5 = 0x1a$$

6. Result:

0x5f57f71d  
0x72f5beb9  
0x64bc3bf9  
0x1592291a

7. Final Result (After transposition):

0x5f726415  
0x57f5bc92  
0xf7be3b29  
0x1db9f91a