Advanced Encryption Standard (AES)

Prince Rachit Sinha

What is Cryptography?

Cryptography is the art of protecting information by transforming the original message, called plaintext into an encoded message, called a cipher or ciphertext.

ABC (meaningful message)-> ZYX(cipher)

What is AES?

- AES is an encryption standard chosen by the National Institute of Standards and Technology(NIST), USA to protect classified information. It has been accepted world wide as a desirable algorithm to encrypt sensitive data.
- It is a block cipher which operates on block size of 128 bits for both encrypting as well as decrypting.
- Each Round performs same operations.

Why AES?

- In 1990's the cracking of DES algorithm became possible.
- Around 50hrs of bruteforcing allowed to crack the message.
- NIST started searching for new feasible algorithm and proposed its requirement in 1997.
- In 2001 Rijndael algorithm designed by Rijment and Daemon of Belgium was declared as the winner of the competition.
- It met all Security, Cost and Implementation criteria.

How Does it works?

- AES basically repeats 4 major functions to encrypt data.It takes 128 bit block of data and a key[laymans term password] and gives a ciphertext as output.The functions are:

I. Sub Bytes

II. Shift Rows

III. Mix Columns

IV. Add Key

How Does it works?

- The number of rounds performed by the algorithm strictly depends on the size of key.
- The following table gives overview of no. Of rounds performed with the input of varying key lengths:

Key Size(in bits)	Rounds
128	10
192	12
256	14

The larger the number of keys the more secure will be the data. The time taken by s/w to encrypt will increase with no. of rounds.

How Does it works?

Here, E=encryption function for a symmetric block cipher
m=plaintext message of size 128bits
n=ciphertext
k=key of size 128bits which is same for both encryption and decryption
D= Decryption function for symmetric block cipher

Steps for encryption and decryption

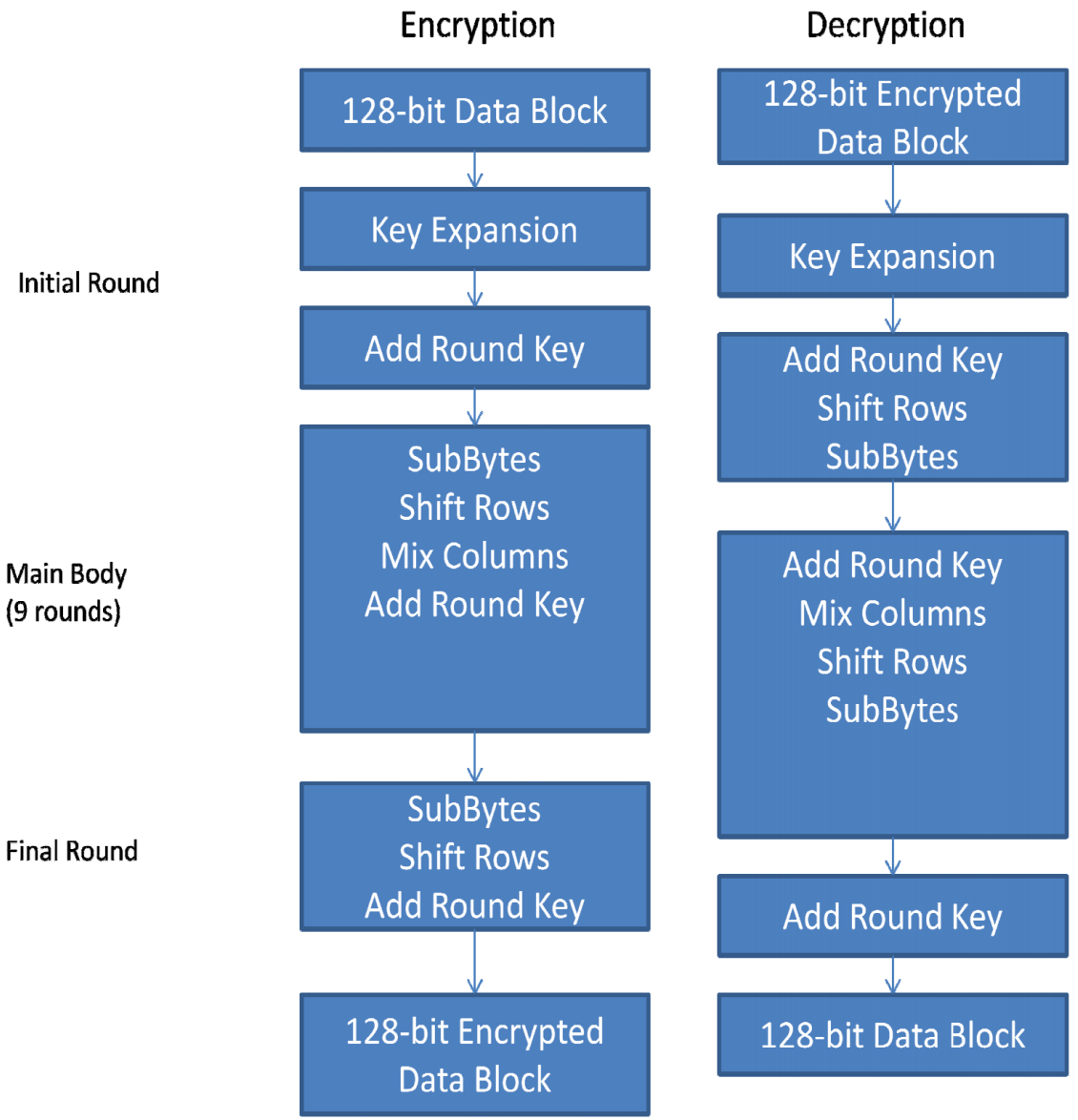
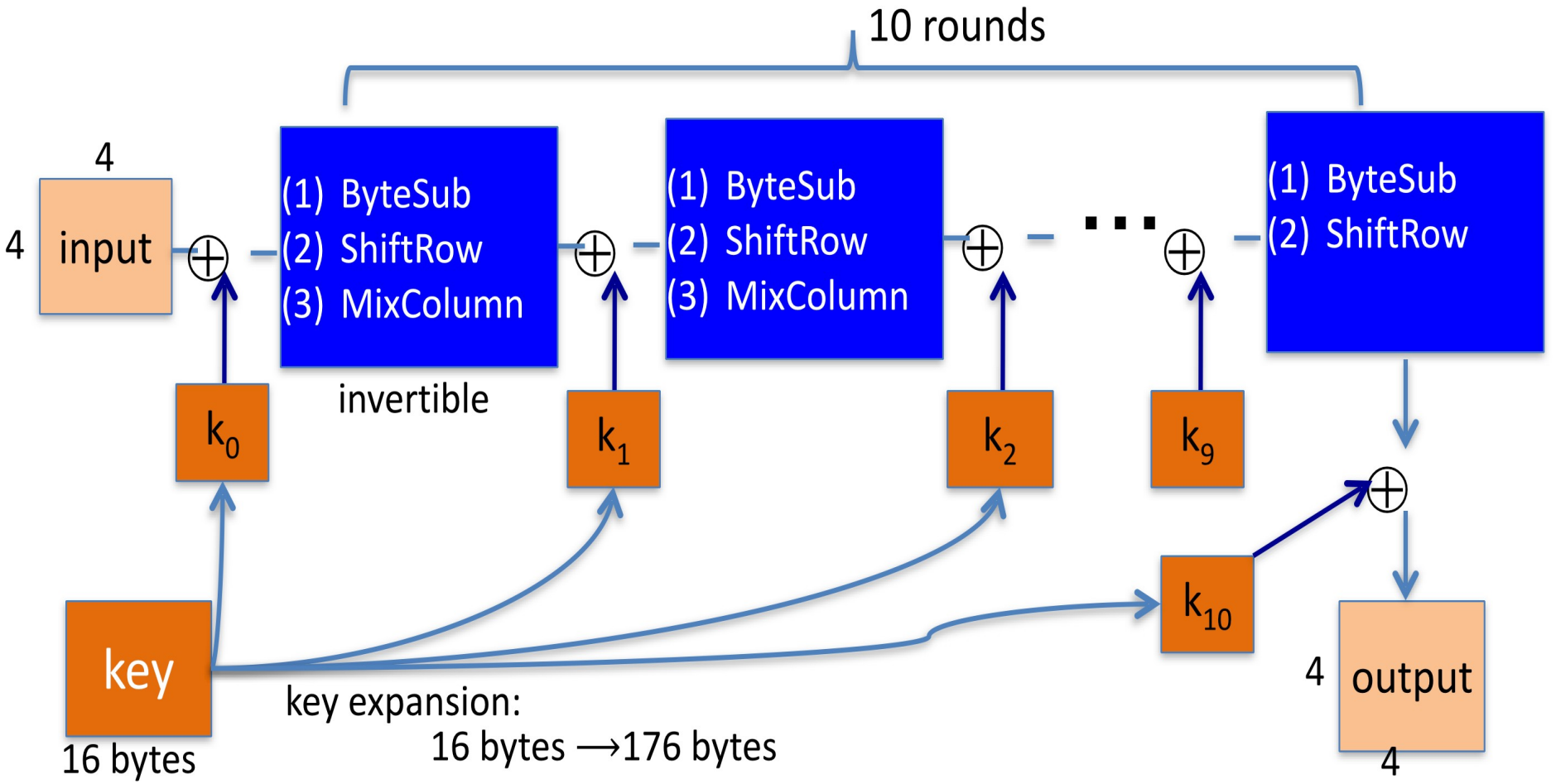


Figure 1 (Encryption on the left, Decryption on the right)

Analysis of Steps

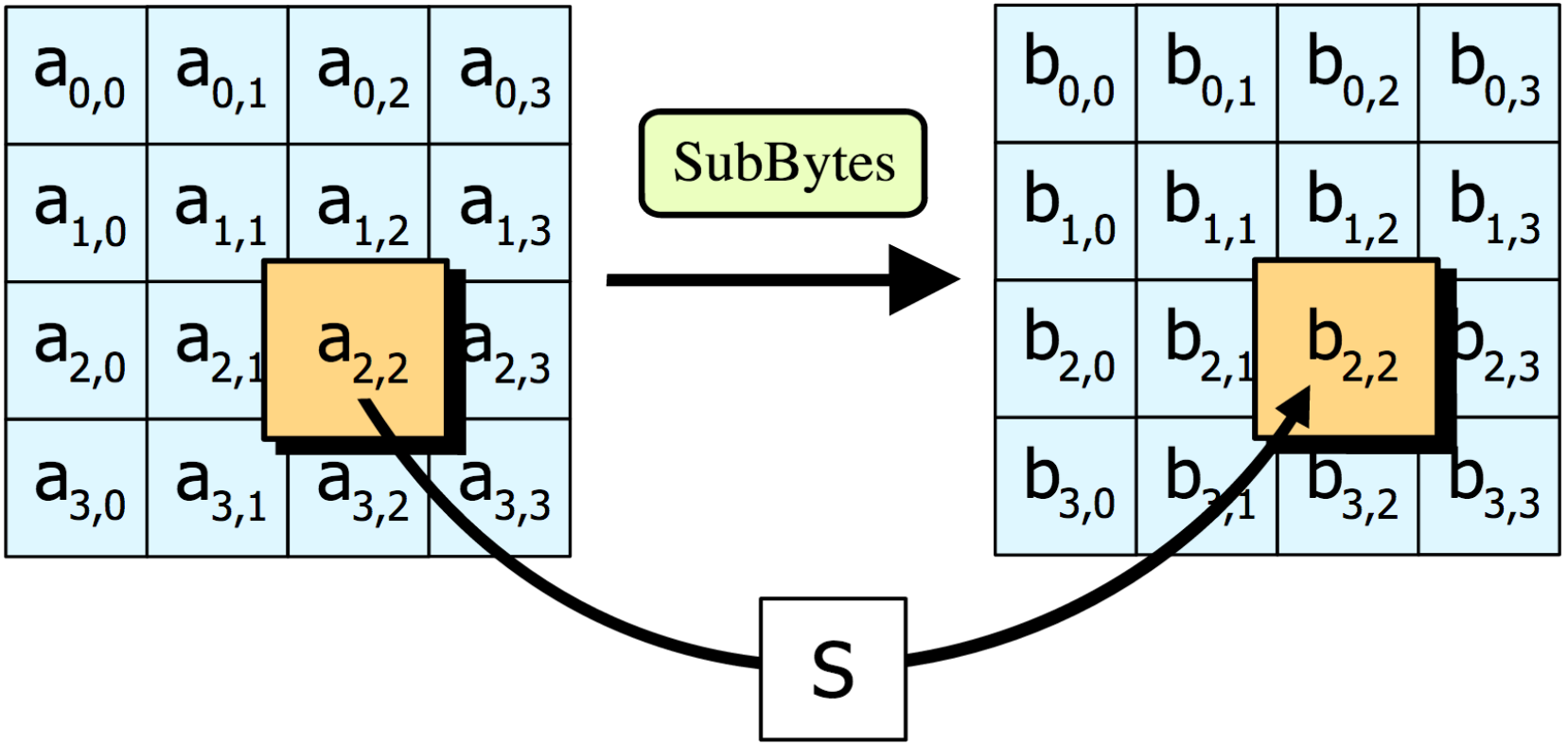
- KeyExpansions- In the key Expansion process the given 128 bits cipher key is stored in [4]x[4] bytes matrix (16*8=128 bits) and then the four column words of the key matrix is expanded into a schedule of 44 words (44*4=176) resulting in 11 round keys (176/11=16 bytes or 128 bits).
- Number of round keys = Nr + 1. Where Nr is the number of rounds (which is 10 in case of 128 bits key size) So here the round keys = 11.

Analysis of Steps



Analysis of Steps

- SubBytes- Each element of the matrix is replaced by the an element of s-box matrix.



Analysis of Steps

- SubBytes

  For an element {d1} corresponding value is {3e}

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

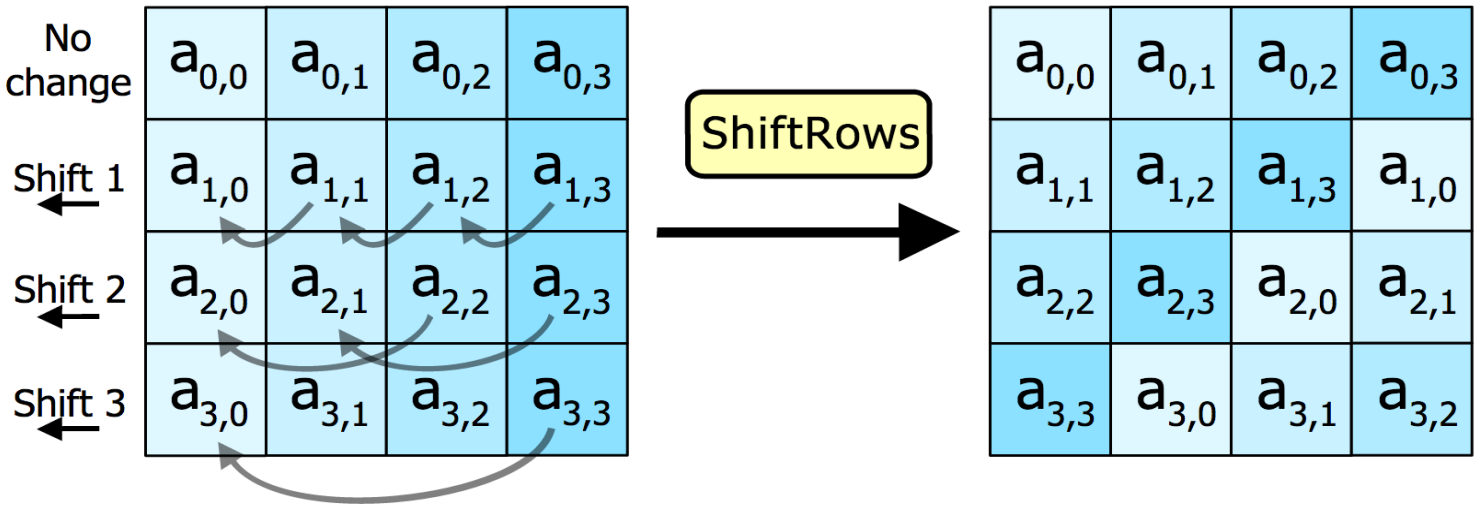
Rijndael S-box

Analysis of Steps

- SubBytes
- The S-box is a special lookup table which is constructed by Galois fields.
- The Generating function used in this algorithm is GF(2^8)
- i.e. 256 values are possible
- The elements of the sbox are written in hexadecimal system

Analysis of Steps

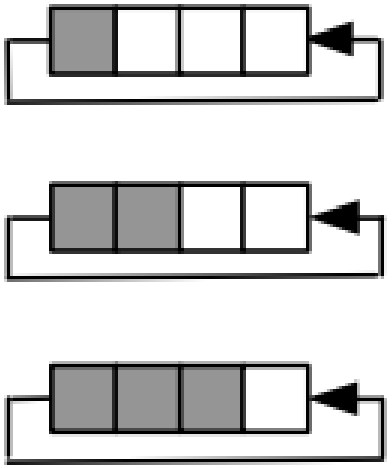
- Shift Rows
- In this step rows of the block are cylindrically shifted in left direction.
- The first row is untouched , the second by one shift, third by two and fourth by 3.



Analysis of Steps

- Shift Rows

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$



$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,1}$	$s_{1,2}$	$s_{1,3}$	$s_{1,0}$
$s_{2,2}$	$s_{2,3}$	$s_{2,0}$	$s_{2,1}$
$s_{3,3}$	$s_{3,0}$	$s_{3,1}$	$s_{3,2}$

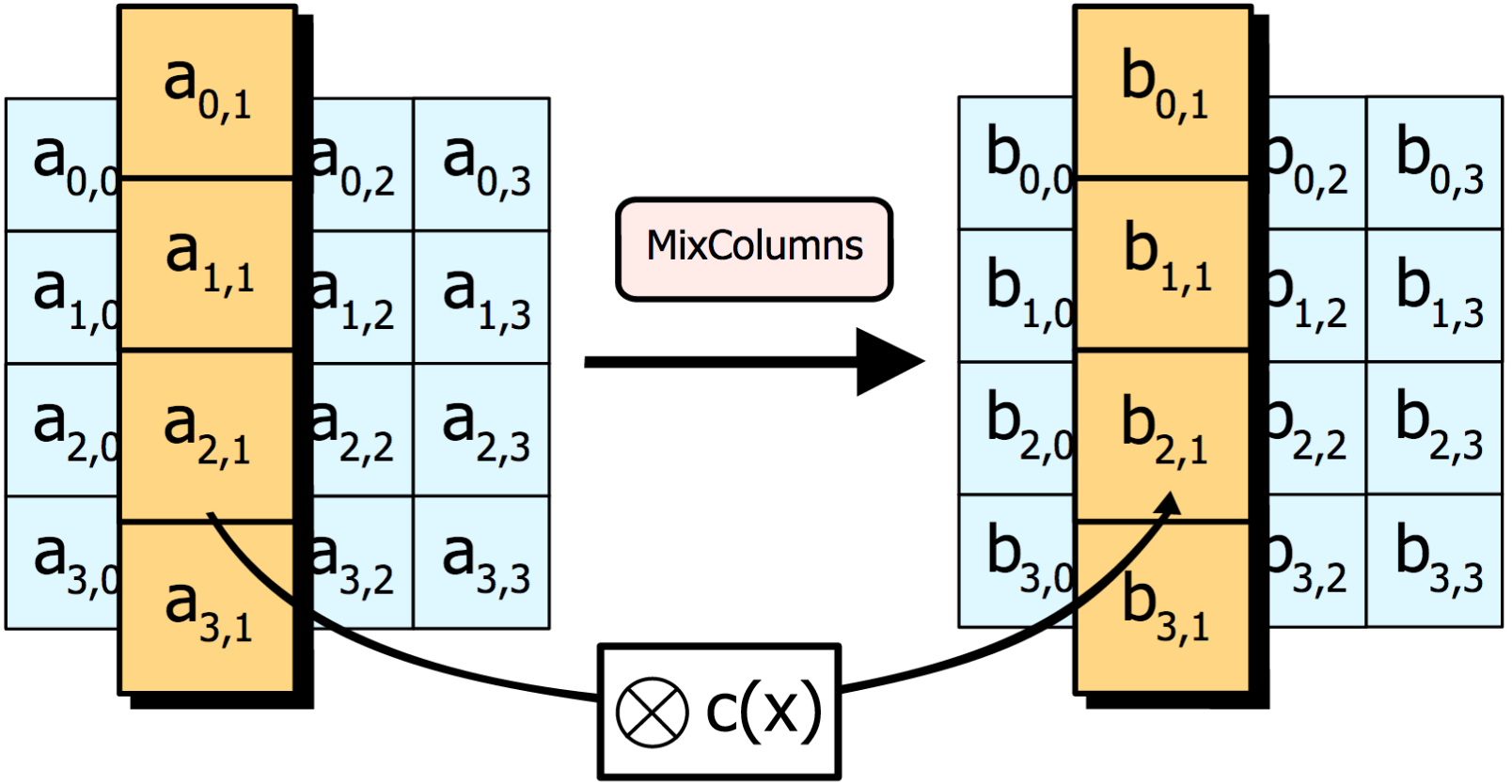
Resulting matrix after shift operation

Analysis of Steps

- Mix columns
- This is the most important part of the algorithm
- It causes the flip of bits to spread all over the block
- In this step the block is multiplied with a fixed matrix.
- The multiplication is field multiplication in galois field.
- For each row there are 16 multiplication, 12 XORs and a 4 byte output.

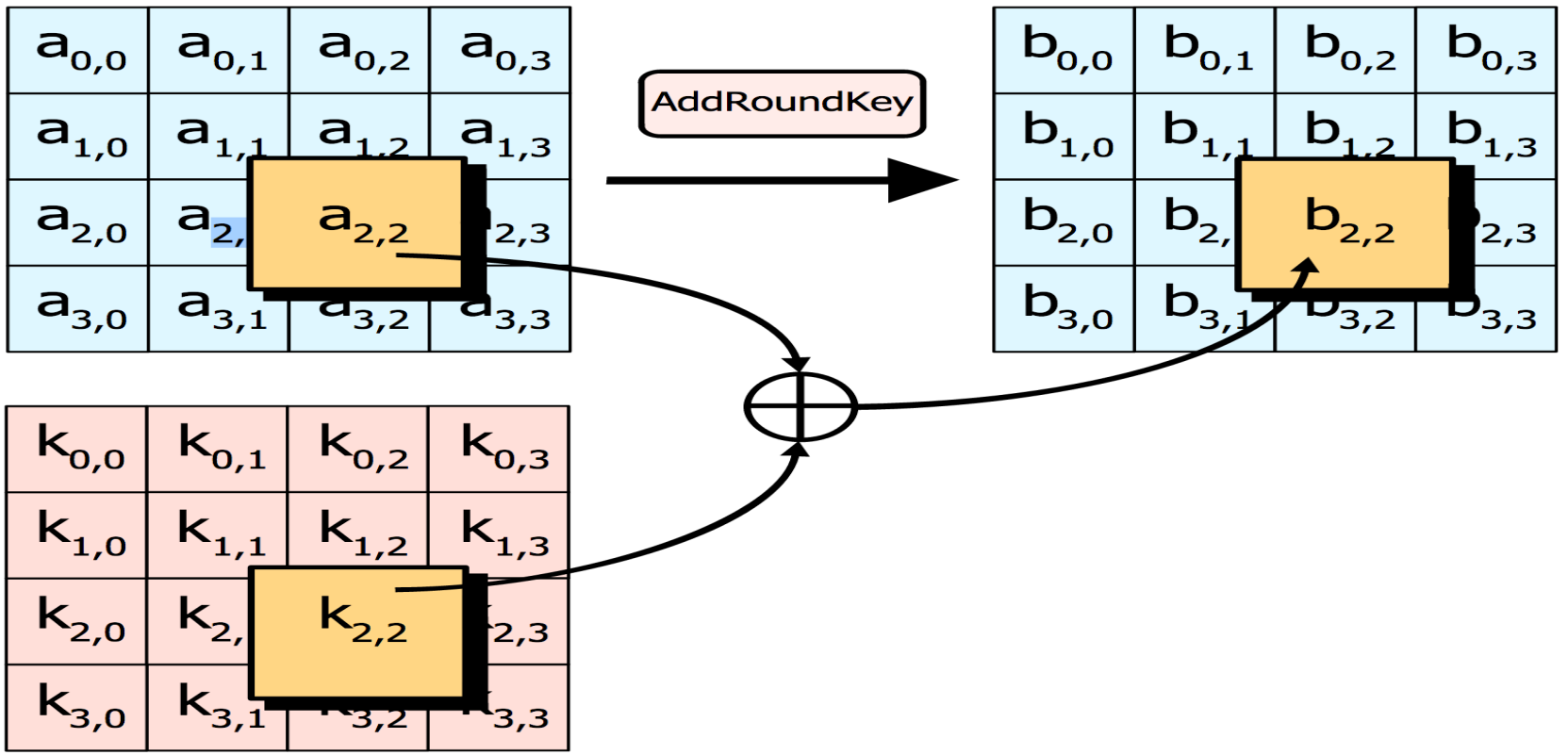
Analysis of Steps

- Mix Columns



Analysis of Steps

- Add round key



Analysis of Steps

- Add round key
- In this step each byte is XOR-ed with corresponding element of key's matrix.
- Once this step is done the keys are no longer available for this step. Using the same key will weaken the algorithm.
- To overcome this problem keys are expanded.

Analysis of Steps

- In the last round the mix column step is skipped.
- It is not documented anywhere why this is done but recently a paper was published against this method highlighting the weakening of cipher text.

Attacks

It is similar to the exhaustive key search attack(brute force attack - trying all the possible set of keys) but it is adaptive. It is 4 times better than the exhaustive key search. But it is infeasible using current technology on block cipher having a keyspace of 128 bits and above.

There are more advanced attack on AES-256 bits like the Related Key Attack, which involves several distinct keys linked together by a common relation which reduces the keyspace to 99.5 bits which is also infeasible.

Thank You!

Questions appreciated