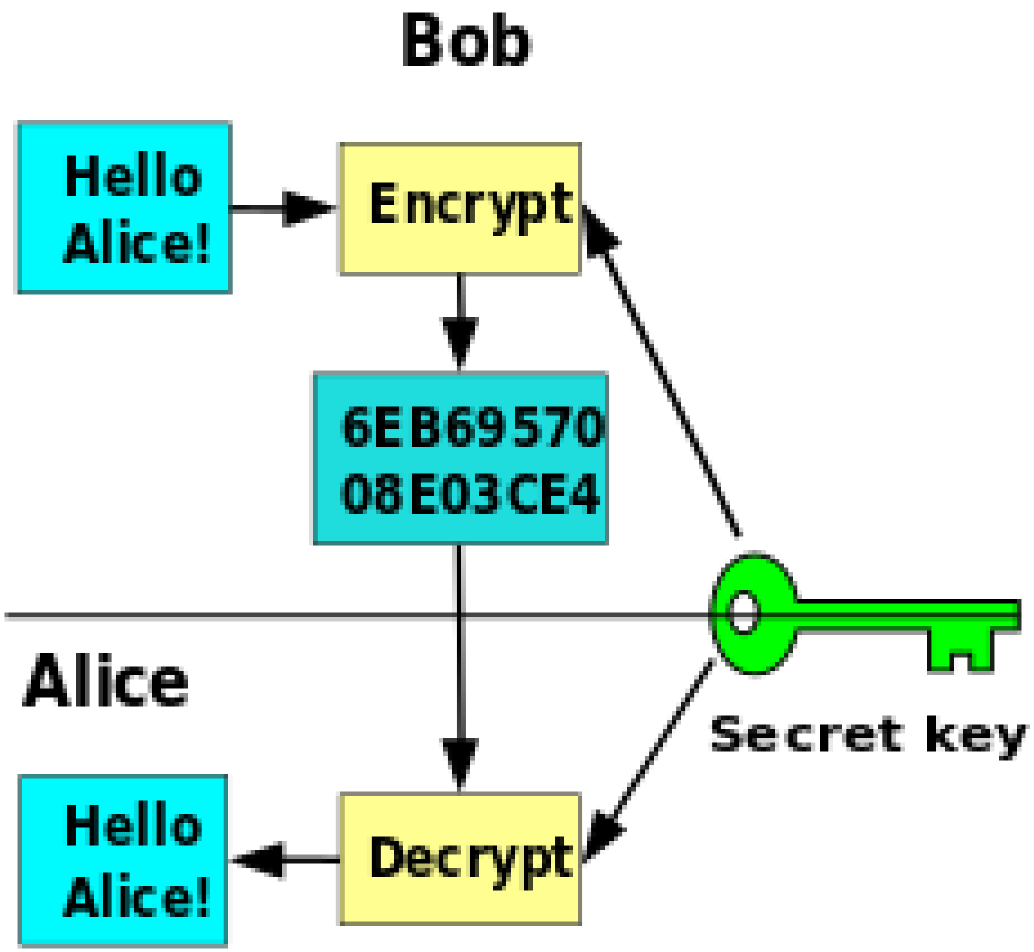
Cryptography

Cryptography



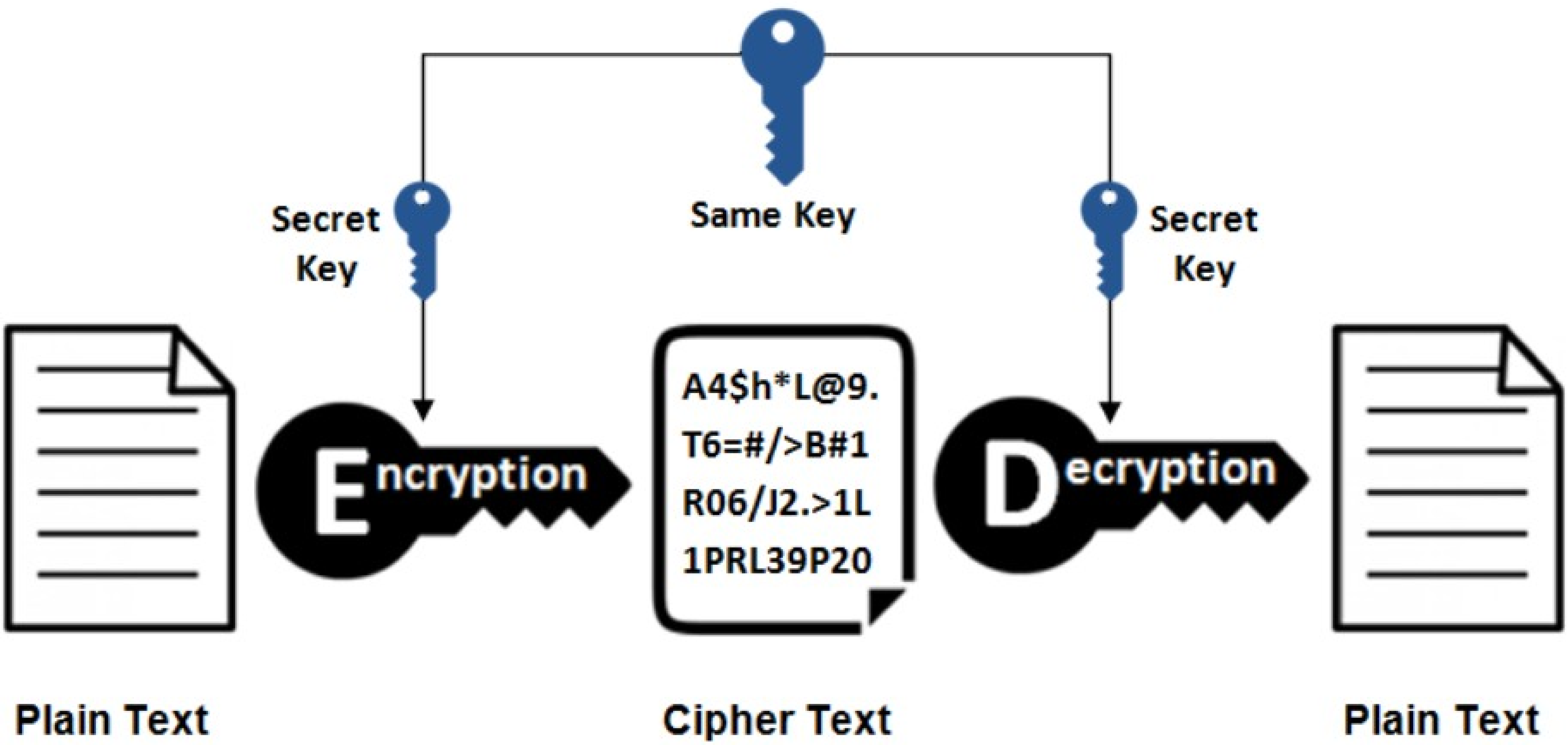
Cryptography

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents.

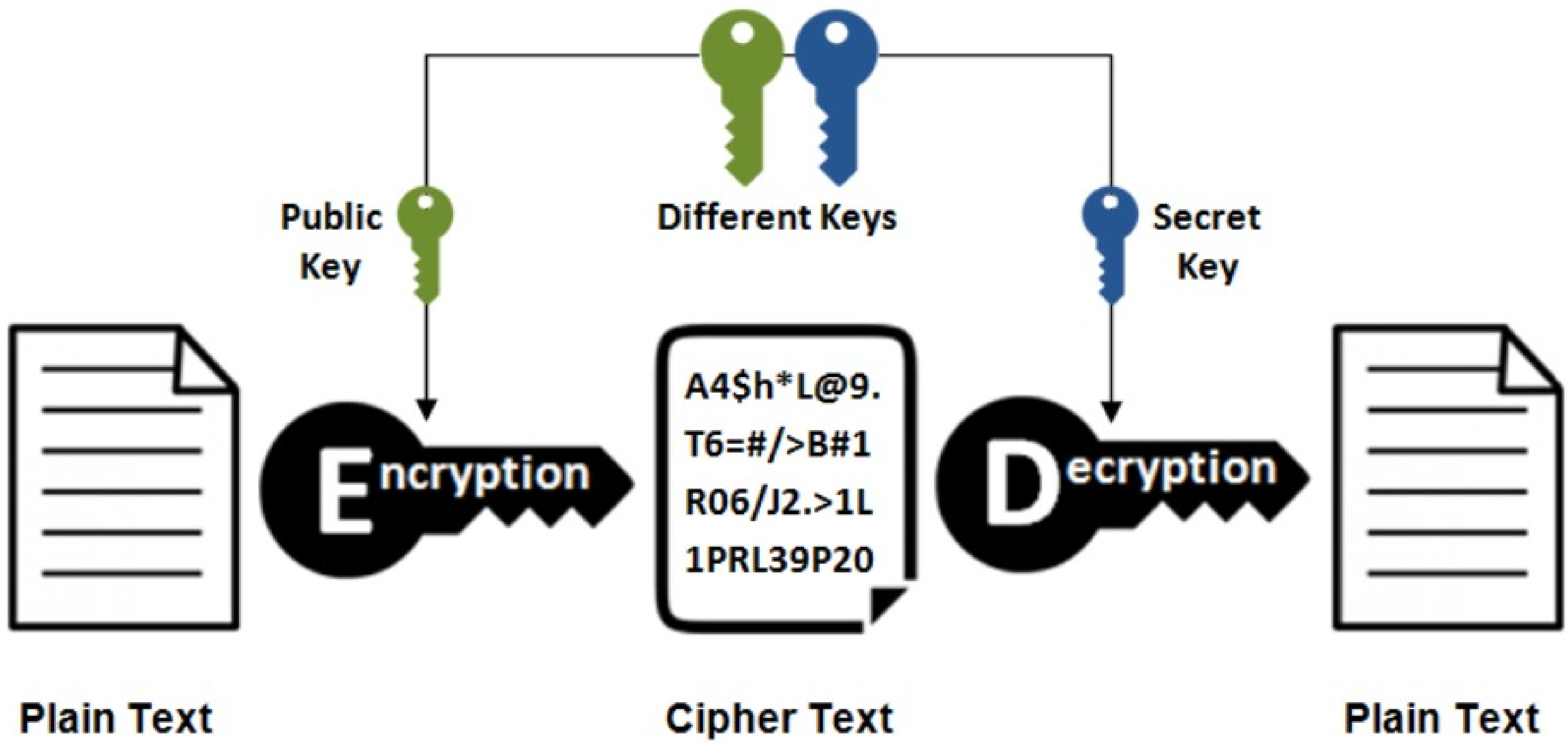
ABC (meaningful message)-> ZYX(cipher)

Symmetric
vs
Asymmetric
Cryptography

Symmetric Encryption



Asymmetric Encryption



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. [1,2]
- It met all Security, Cost and Implementation criteria. [3]

How Does it works?

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

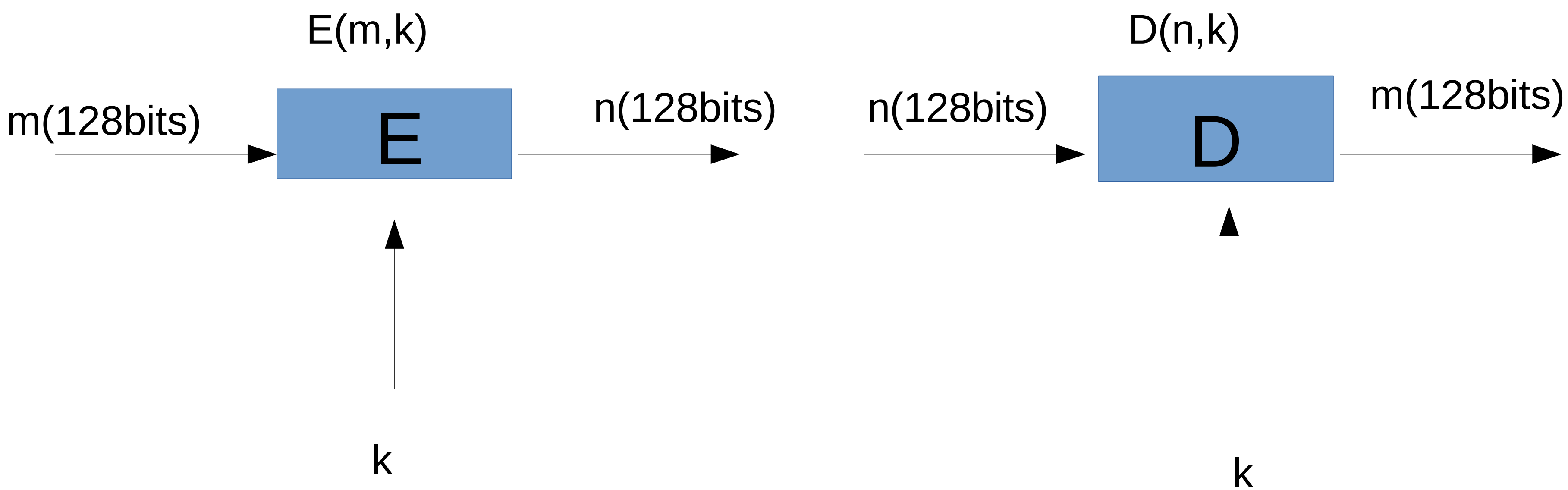
I. Substitute Bytes

II. Shift Rows

III. Mix Columns

IV. Add Key

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

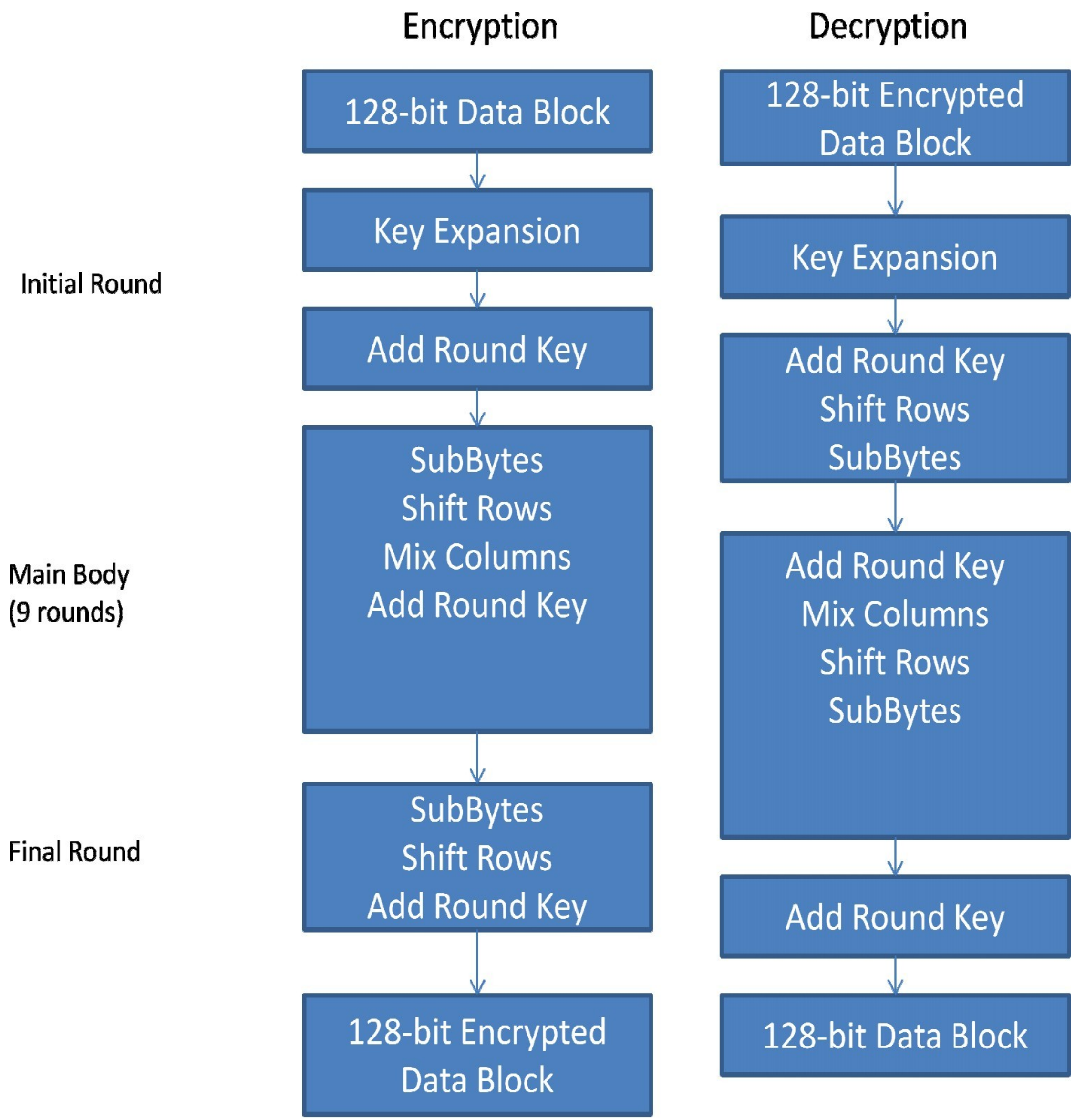
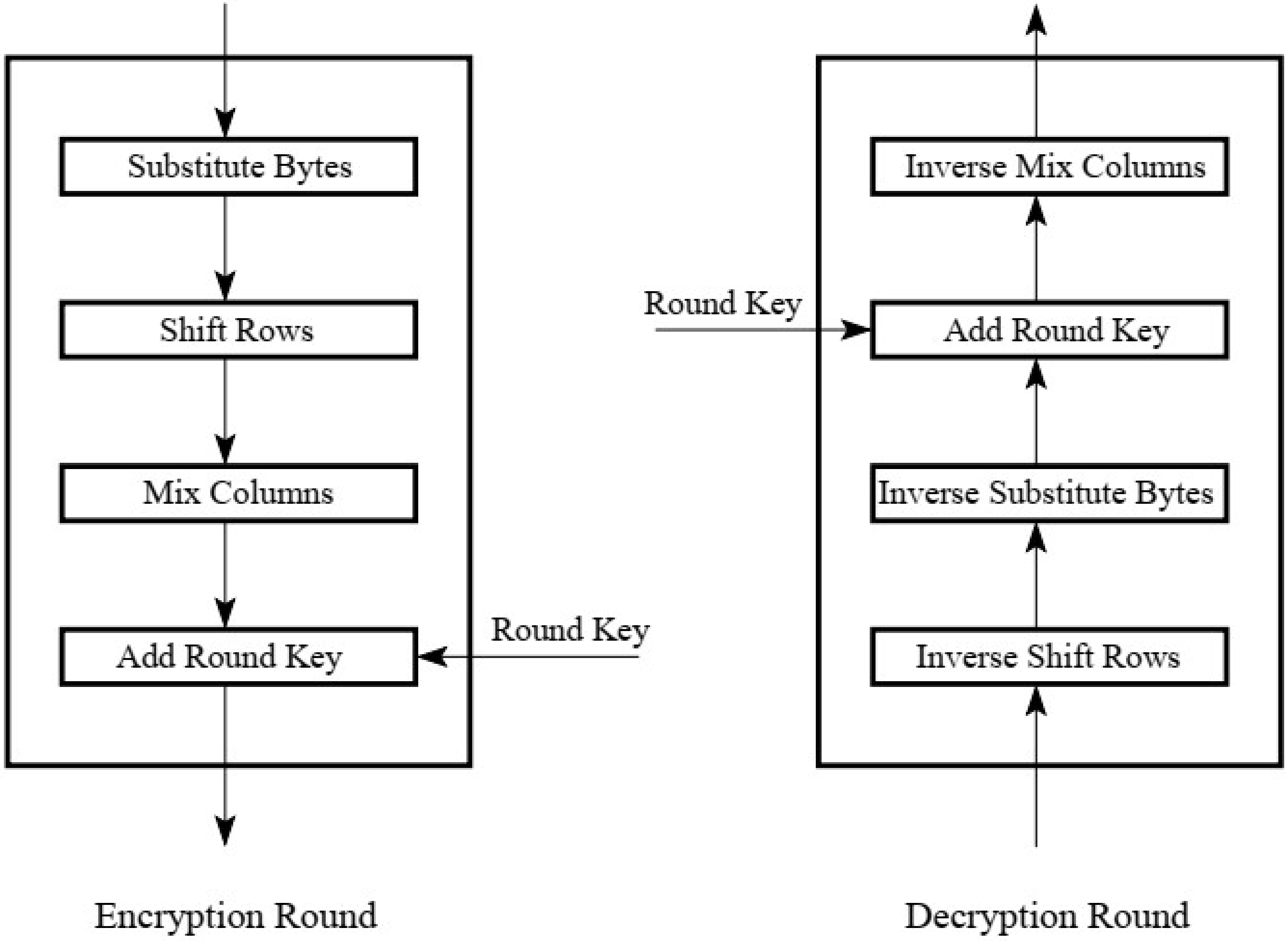


Figure 1 (Encryption on the left, Decryption on the right)

How Does it works?

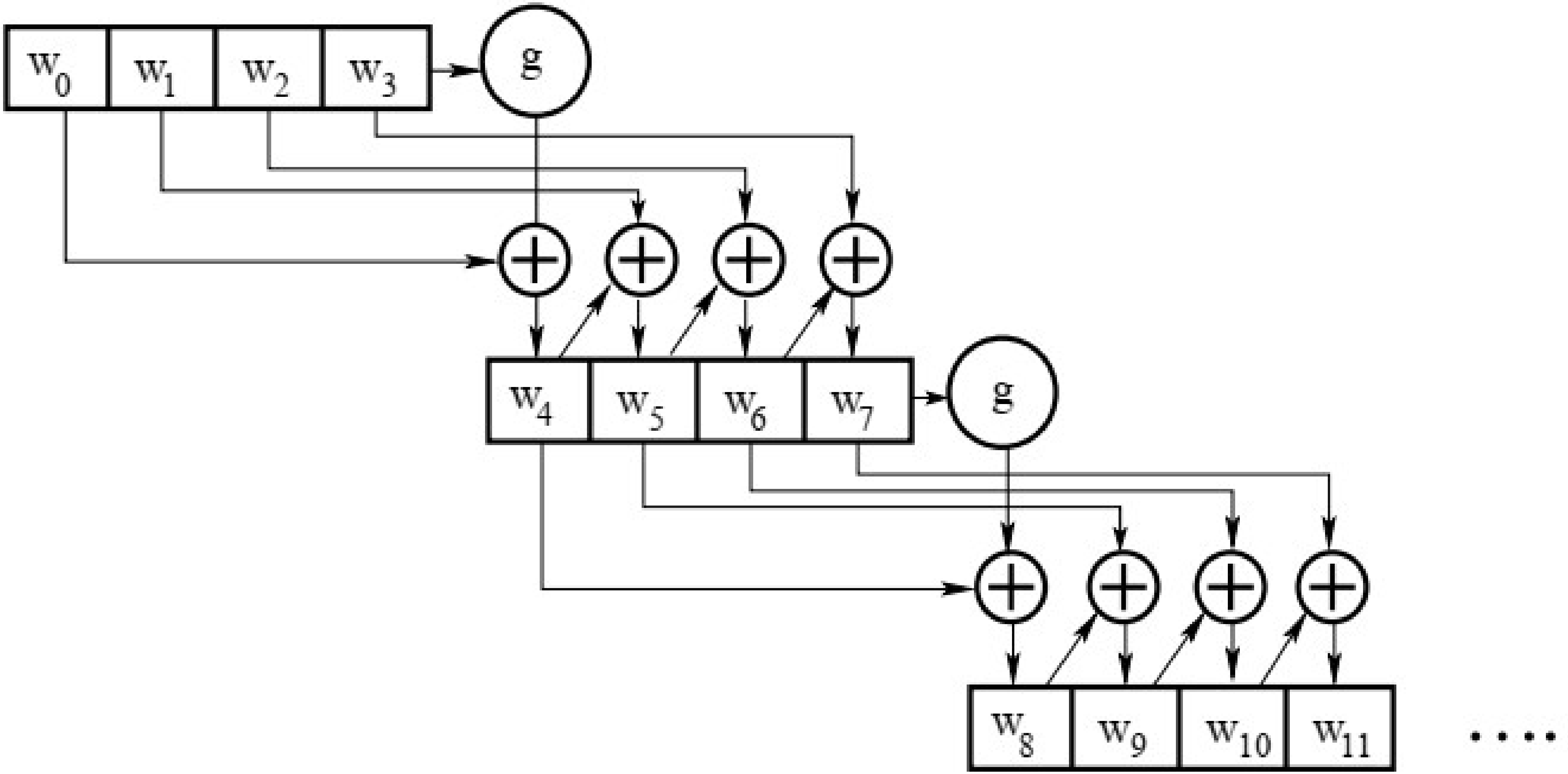


Analysis of Steps

- **Key-expansions-** 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).

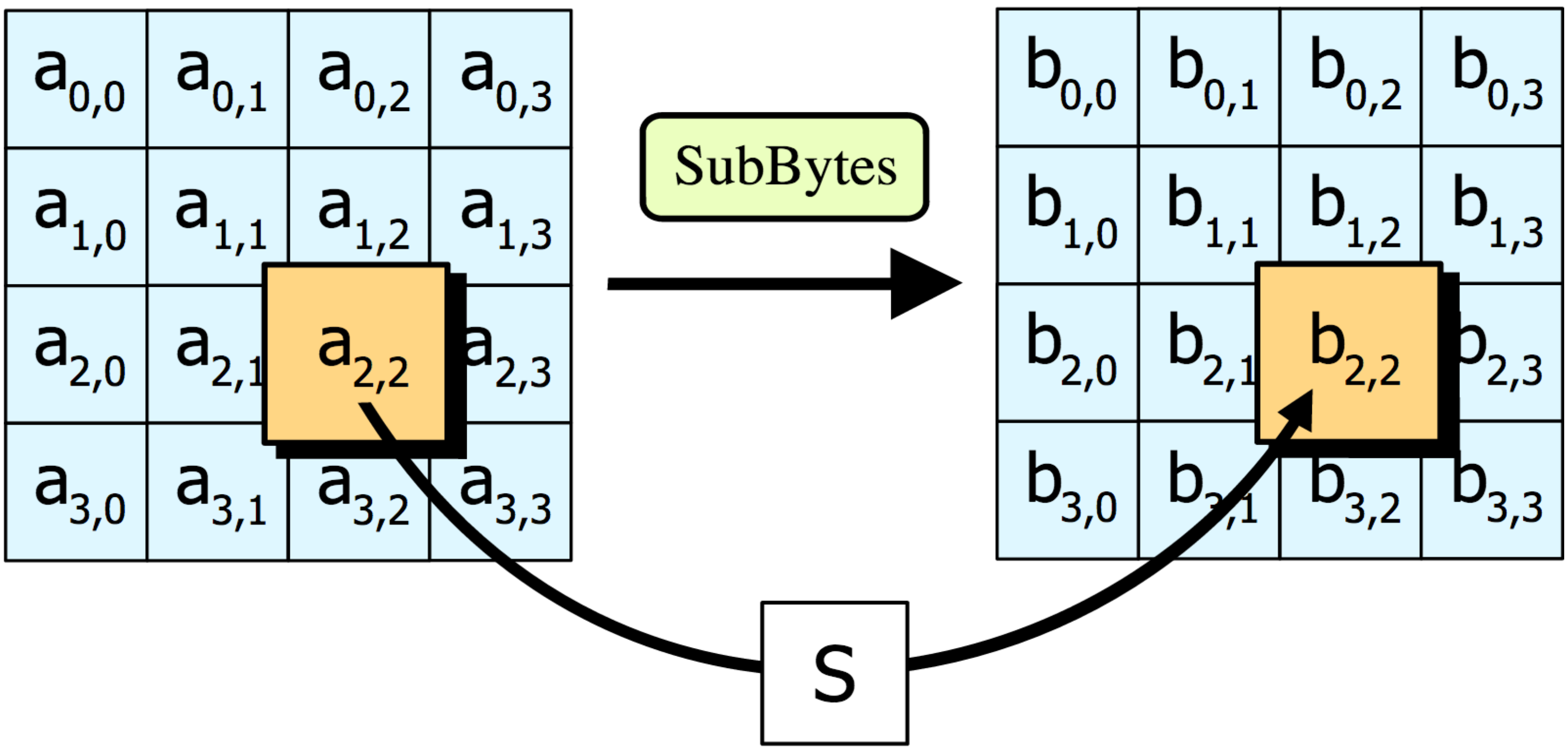
- Number of round keys = Nr + 1. Where Nr is the number of rounds (which is 10 in case of 128 bits key size) So here the round keys = 11.

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

- Inverse SubBytes

right (low-order) nibble

left (high-order) nibble

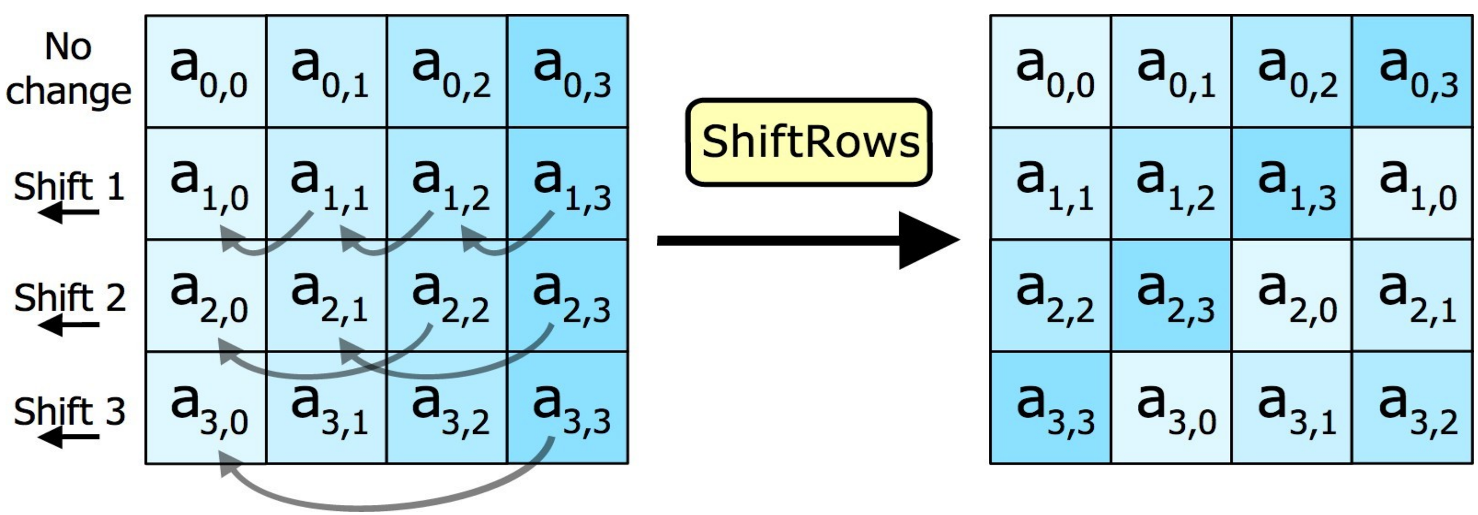
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed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

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

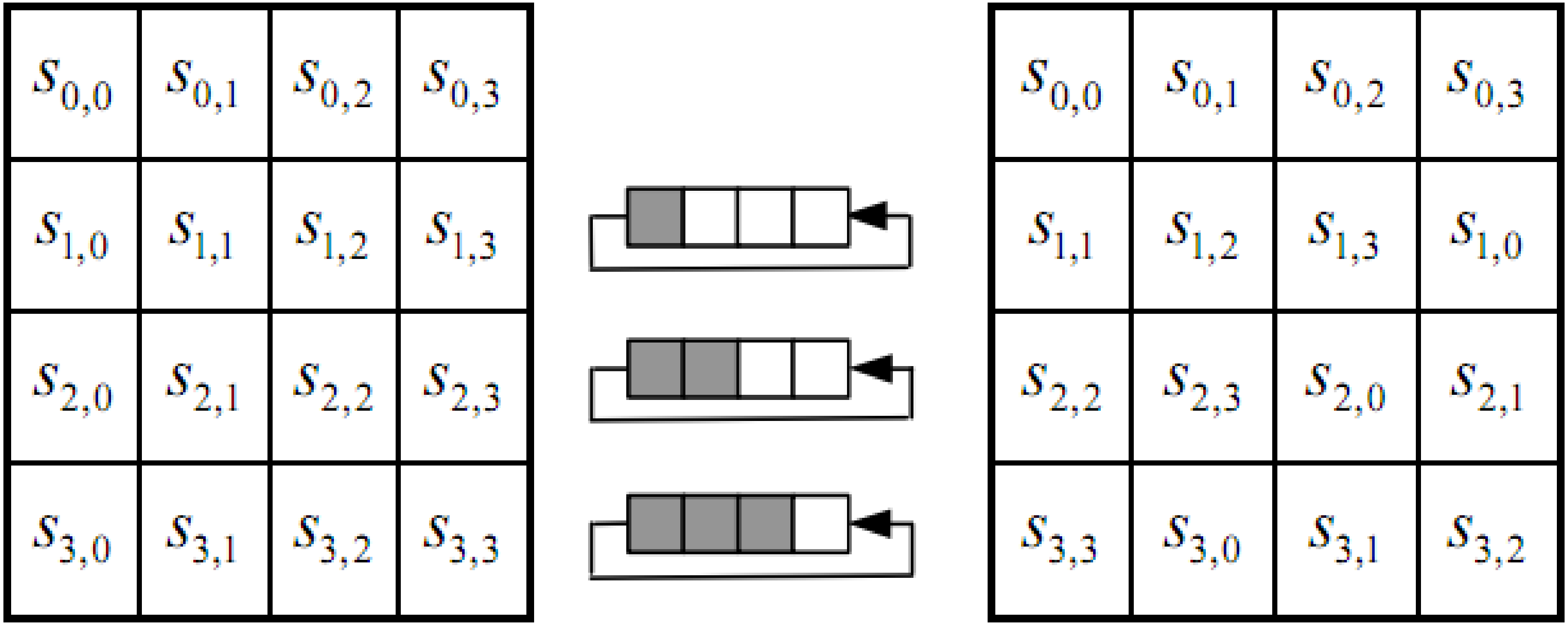
Analysis of Steps

- 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



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

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} s_{0.0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1.0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2.0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3.0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} = \begin{bmatrix} s'_{0.0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1.0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2.0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3.0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}$$

$$
\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}
\begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix}
=
\begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}
\Rightarrow
$$

$$
\begin{aligned}
s'_{0,j} &= (2 \bullet s_{0,j}) \oplus (3 \bullet s_{1,j}) \oplus s_{2,j} \oplus s_{3,j} \\
s'_{1,j} &= s_{0,j} \oplus (2 \bullet s_{1,j}) \oplus (3 \bullet s_{2,j}) \oplus s_{3,j} \\
s'_{2,j} &= s_{0,j} \oplus s_{1,j} \oplus (2 \bullet s_{2,j}) \oplus (3 \bullet s_{3,j}) \\
s'_{3,j} &= (3 \bullet s_{0,j}) \oplus s_{1,j} \oplus s_{2,j} \oplus (2 \bullet s_{3,j})
\end{aligned}
$$

Predefine Matrix

2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2

*

State Array

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

New State Array

$(\{02\} \cdot \{87\}) \oplus (\{03\} \cdot \{6E\}) \oplus \{46\} \oplus \{A6\} = \{47\}$

$\{87\} \oplus (\{02\} \cdot \{6E\}) \oplus (\{03\} \cdot \{46\}) \oplus \{A6\} = \{37\}$

$\{87\} \oplus \{6E\} \oplus (\{02\} \cdot \{46\}) \oplus (\{03\} \cdot \{A6\}) = \{94\}$

$(\{03\} \cdot \{87\}) \oplus \{6E\} \oplus \{46\} \oplus (\{02\} \cdot \{A6\}) = \{ED\}$

47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC

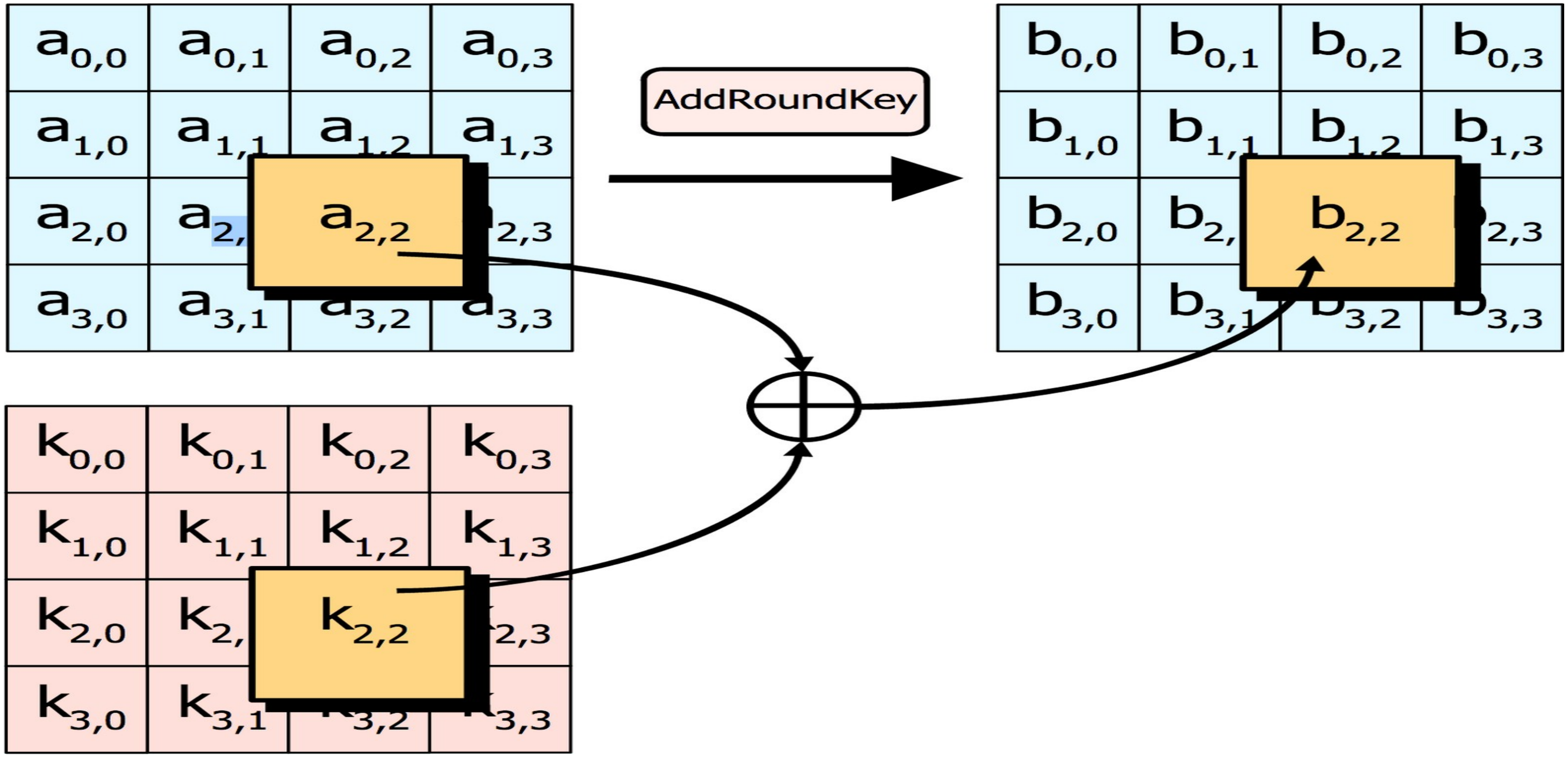
Analysis of Steps

- Inverse Mix Columns

$$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \times \begin{bmatrix} s_{0.0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1.0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2.0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3.0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} = \begin{bmatrix} s'_{0.0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1.0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2.0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3.0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}$$

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.

Analysis of Steps

- In the last round of Encryption the mix column step is skipped.

Self Study

- Rationale behind the steps
- Sbox and Inverse Sbox table generation

RSA

- RSA is one of the oldest asymmetric encryption algorithm
- The acronym "RSA" comes from the surnames of Ron Rivest, Adi Shamir and Leonard Adleman
- The security of RSA relies on the practical difficulty of factoring the product of two large prime numbers, the "factoring problem".

RSA algorithm steps

1. Key Generation

Step-1: Select two large prime numbers p and q where $p \neq q$.
Step-2: Calculate $n = p * q$.
Step-3: Calculate $\Phi(n) = (p-1) * (q-1)$.
Step-4: Select e such that, e is relatively prime to $\Phi(n)$, i.e. $\gcd(e, \Phi(n)) = 1$ and $1 < e < \Phi(n)$
Step-5: Calculate $d = e^{-1} \bmod \Phi(n)$ or $ed = 1 \bmod \Phi(n)$.
Step-6: Public key = $\{e, n\}$, private key = $\{d, n\}$.

Example

<u>Step – 1:</u> Select two prime numbers p and q where p ≠ q.
Example, Two prime numbers p = 13, q = 11.

<u>Step – 2:</u> Calculate n = p * q.
Example, n = p * q = 13 * 11 = 143.

<u>Step – 3:</u> Calculate Φ(n) = (p-1) * (q-1).
Example, Φ(n) = (13 – 1) * (11 – 1) = 12 * 10 = 120.

<u>Step – 4:</u> Select e such that, e is relatively prime to Φ(n),
i.e. gcd(e, Φ(n)) = 1 and 1 < e < Φ(n).
Example, Select e = 13, gcd (13, 120) = 1.

<u>Step - 5:</u> Calculate $d = e^{-1} \bmod \Phi(n)$ or $e * d = 1 \bmod \Phi(n)$

Example, Finding d: $e * d \bmod \Phi(n) = 1$

$13 * d \bmod 120 = 1$

(How to find: $d * e = 1 \bmod \Phi(n)$

$d = ((\Phi(n) * i) + 1) / e$

$d = (120 + 1) / 13 = 9.30$ ($\because i = 1$)

$d = (240 + 1) / 13 = 18.53$ ($\because i = 2$)

$d = (360 + 1) / 13 = 27.76$ ($\because i = 3$)

$d = (480 + 1) / 13 = 37$ ($\because i = 4$))

<u>Step - 6:</u> Public key = {e, n}, private key = {d, n}.

Example, Public key = {13, 143}

and private key = {37, 143}

2. Encryption

Find out *cipher text* using the formula,
$C = P^e \bmod n$ where, $P < n$.

Example, Plain text $P = 13$. (Where, $P <$
$C = P^e \bmod n = 13^{13} \bmod 143 = 52$.

3. Decryption

P = C^d mod n. Plain text P can be obtain
using the given formula.

Example, Cipher text C = 52
P = C^d mod n = 52^{37} mod 143 = 13.

References

1. AES Proposal: Rijndael, Joan Daemen, Vincent Rijmen
2. The Design of Rijndael, Joan Daemen, Vincent Rijmen
3. https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf