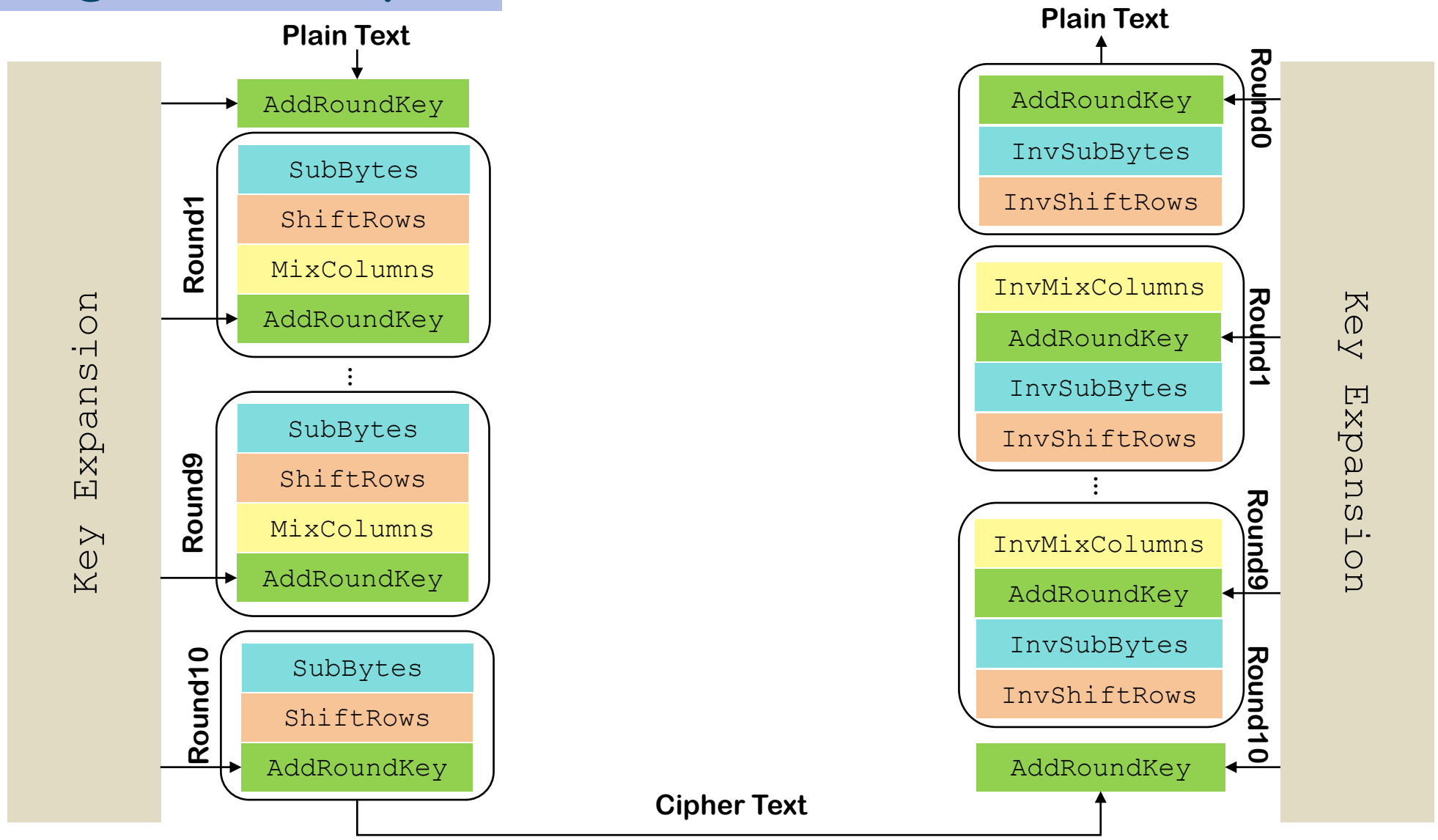
Computer Engineering Faculty
University of Isfahan

Advanced Encryption Standard

AES Algorithm Steps



Computer Engineering Faculty
University of Isfahan

Computer Engineering Faculty
University of Isfahan

Plain text =

193DE3BEA0F4E22B9AC68D2AE9F84808

19	A0	9A	E9
3D	F4	C6	F8
E3	E2	8D	48
BE	2B	2A	08

SubBytes Transform

	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	B3	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	B4
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	CB	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

19	**A0**	**9A**	**E9**
3D	**F4**	**C6**	**F8**
E3	**E2**	**8D**	**48**
BE	**2B**	**2A**	**08**

D4	**E0**	**B8**	**1E**
27	**BF**	**B4**	**41**
11	**98**	**5D**	**52**
AE	**F1**	**E5**	**30**

Computer Engineering Faculty
University of Isfahan

Shift Rows

D4	E0	B8	1E
27	BF	B4	41
11	98	5D	52
AE	F1	E5	30

D4	E0	B8	1E
BF	B4	41	27
5D	52	11	98
30	AE	F1	E5

Computer Engineering Faculty
University of Isfahan

Mixed Columns

D4	E0	B8	1E
BF	B4	41	27
5D	52	11	98
30	AE	F1	E5

Computer Engineering Faculty
University of Isfahan

Constant Matrix

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

$\bullet$

D4
BF
5D
30

$=$

P1

$$P1 = (02 \bullet D4) + (03 \bullet BF) + (01 \bullet 5D) + (01 \bullet 30)$$

GF(2^8)

Example

57 = 0101 0111
83 = 1000 0011

Computer Engineering Faculty
University of Isfahan

$$57 \bullet 83 = (x^6 + x^4 + x^2 + x + 1)(x^7 + x + 1)$$

$$= x^{13} + x^{11} + x^9 + x^8 + x^7 + x^7 + x^5 + x^3 + x^2 + x + x^6 + x^4 + x^2 + x + 1$$

$$= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$$

$$= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \; modulo \; \boldsymbol{x^8 + x^4 + x^3 + x + 1}$$

$$= x^7 + x^6 + 1$$

$$= C1$$

GF(2^8)

Example

02 = 0000 0010
D4 = 1101 0100

Computer Engineering Faculty
University of Isfahan

$$02 \bullet \text{D4} = (x)(x^7 + x^6 + x^4 + x^2)$$

$$= x^8 + x^7 + x^5 + x^3$$

$$= x^8 + x^7 + x^5 + x^3 \; modulo \; \boldsymbol{x^8 + x^4 + x^3 + x + 1}$$

$$= x^7 + x^5 + x^4 + x + 1$$

$$= 1011\,0011$$

$$= B3$$

Mixed Columns

Constant Matrix

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

$\bullet$

D4
BF
5D
30

$=$

P1

$$P1 = (02 \bullet D4) + (03 \bullet BF) + (01 \bullet 5D) + (01 \bullet 30)$$

$02 \bullet D4 = B3$ $\quad 1011\ 0011$

$03 \bullet BF = DA$ $\quad 1101\ 1010\ \oplus$

$01 \bullet 5D = 5D$ $\quad 0101\ 1101\ \oplus$

$01 \bullet 30 = 30$ $\quad 0011\ 0000\ \oplus$

$0000\ 0100$

Computer Engineering Faculty
University of Isfahan

Mixed Columns

Constant Matrix

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

$\bullet$

D4
BF
5D
30

$=$

04

$$P1 = (02 \bullet D4) + (03 \bullet BF) + (01 \bullet 5D) + (01 \bullet 30)$$

$02 \bullet D4 = B3$ $\quad 1011\ 0011$

$03 \bullet BF = DA$ $\quad 1101\ 1010\ \oplus$

$01 \bullet 5D = 5D$ $\quad 0101\ 1101\ \oplus$

$01 \bullet 30 = 30$ $\quad 0011\ 0000\ \oplus$

$0000\ 0100$

Computer Engineering Faculty
University of Isfahan

Mixed Columns

D4	E0	B8	1E
BF	B4	41	27
5D	52	11	98
30	AE	F1	E5

Computer Engineering Faculty
University of Isfahan

Constant Matrix

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

$\bullet$

D4
BF
5D
30

$=$

04
66
81
E5

04	E0	48	28
66	CB	F8	06
81	19	D3	26
E5	9A	7A	4C

Add Round Key

```
CB = 1100 1011        05 = 0000 0101
54 = 0101 0100        4C = 0100 1100
     1001 1111 = 9F        0100 1001 = 49
```

Computer Engineering Faculty
University of Isfahan

04	E0	48	28
66	CB	F8	06
81	19	D3	26
E5	9A	7A	4C

$\oplus$

Key Round

A0	88	23	2A
FA	54	A3	6C
FE	26	39	76
17	B1	39	05

A4	68	6B	02
9C	9F	5B	6A
7F	35	EA	50
F2	2B	43	49

Key Expansion

Computer Engineering Faculty
University of Isfahan

$$w_{4\times i+j} = w_{4\times(i-1)+j} \oplus w_{4\times i+j-1} \qquad 1 \le j \le 3$$

$$w_{4\times i} = t_{4\times i} \oplus w_{4\times(i-1)} \qquad 1 \le i \le 10$$

$$k_i = w_{4\times i} w_{4\times i+1} w_{4\times i+2} w_{4\times i+3} \qquad 0 \le i \le 10$$

Original key = `2B7E151628AED2A6ABF7158809CF4F3C`

Key Expansion

Computer Engineering Faculty
University of Isfahan

Original key = `2B7E151628AED2A6ABF7158809CF4F3C`

k_0

Original Key

2B	28	AB	09
7E	AE	F7	CF
15	D2	15	4F
16	A6	88	3C
w_0	w_1	w_2	w_3

Key Expansion

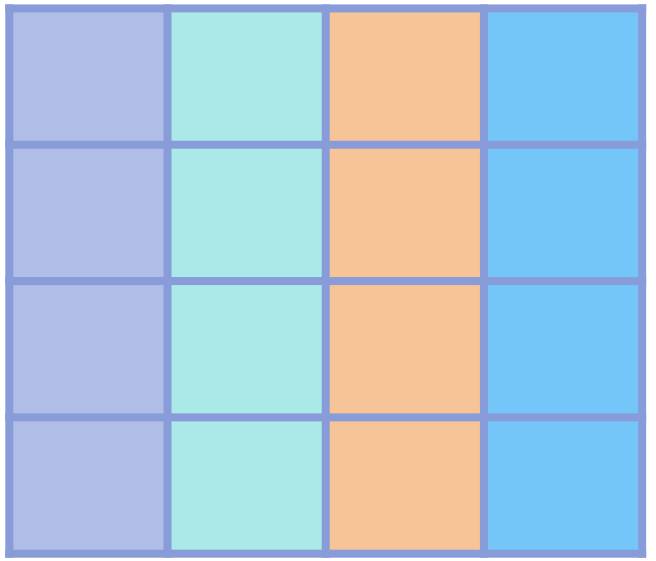
K_{i-1}

2B	28	AB	09
7E	AE	F7	CF
15	D2	15	4F
16	A6	88	3C

$w_{4(i-1)}$ $w_{4(i-1)+1}$ $w_{4(i-1)+2}$ $w_{4(i-1)+3}$

$$W_{4i} = t_{4i} \oplus w_{4(i-1)}$$
$$W_{4i+1} = w_{4i} \oplus w_{4(i-1)+1}$$
$$W_{4i+2} = w_{4i+1} \oplus w_{4(i-1)+2}$$
$$W_{4i+3} = w_{4i+2} \oplus w_{4(i-1)+3}$$

K_i



w_{4i} w_{4i+1} w_{4i+2} w_{4i+3}

Computer Engineering Faculty
University of Isfahan

Key Expansion

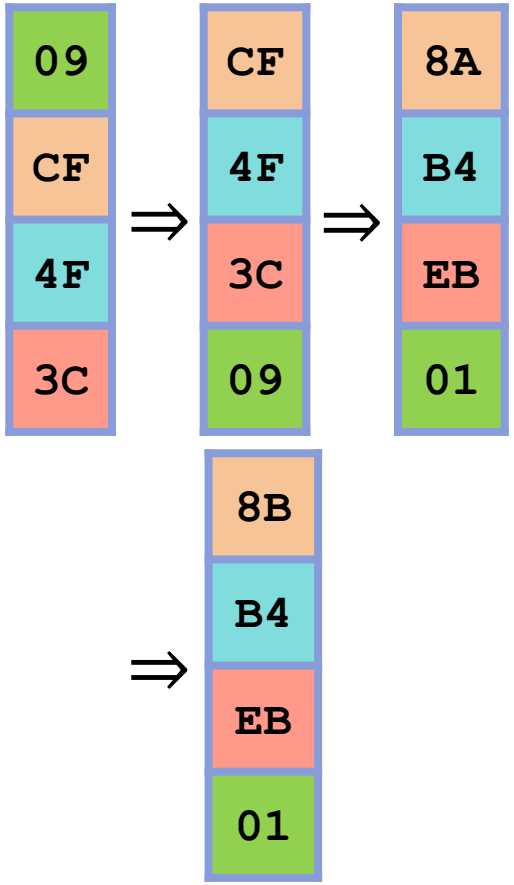
Computer Engineering Faculty
University of Isfahan

$$t_{4i} = \text{SubWord}(\text{RotWord}(W_{4(i-1)+3})) \oplus \text{RConstant}_i$$

	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	B3	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	B4
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	CB	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

Round	RConstant
1	01 00 00 00
2	02 00 00 00
3	04 00 00 00
4	08 00 00 00
5	10 00 00 00
6	20 00 00 00
7	40 00 00 00
8	80 00 00 00
9	1B 00 00 00
10	36 00 00 00

$W_{4(i-1)+3}$



Key Expansion

K_{i-1}

2B	28	AB	09
7E	AE	F7	CF
15	D2	15	4F
16	A6	88	3C

$w_{4(i-1)}$ $w_{4(i-1)+1}$ $w_{4(i-1)+2}$ $w_{4(i-1)+3}$

8B
B4
EB
01

$$W_{4i} = t_{4i} \oplus w_{4(i-1)}$$
$$W_{4i+1} = w_{4i} \oplus w_{4(i-1)+1}$$
$$W_{4i+2} = w_{4i+1} \oplus w_{4(i-1)+2}$$
$$W_{4i+3} = w_{4i+2} \oplus w_{4(i-1)+3}$$

K_i

A0			
FA			
FE			
17			

w_{4i} w_{4i+1} w_{4i+2} w_{4i+3}

Computer Engineering Faculty
University of Isfahan

Key Expansion

K_{j-1}

2B	28	AB	09
7E	AE	F7	CF
15	D2	15	4F
16	A6	88	3C
$w_{4(i-1)}$	$w_{4(i-1)+1}$	$w_{4(i-1)+2}$	$w_{4(i-1)+3}$

$$W_{4i} = t_{4i} \oplus w_{4(i-1)}$$
$$W_{4i+1} = w_{4i} \oplus w_{4(i-1)+1}$$
$$W_{4i+2} = w_{4i+1} \oplus w_{4(i-1)+2}$$
$$W_{4i+3} = w_{4i+2} \oplus w_{4(i-1)+3}$$

K_i

A0	88		
FA	54		
FE	2C		
17	B1		
w_{4i}	w_{4i+1}	w_{4i+2}	w_{4i+3}

Computer Engineering Faculty
University of Isfahan

Key Expansion

		K_{i-1}	
2B	28	AB	09
7E	AE	F7	CF
15	D2	15	4F
16	A6	88	3C
$w_{4(i-1)}$	$w_{4(i-1)+1}$	$w_{4(i-1)+2}$	$w_{4(i-1)+3}$

$$W_{4i} = t_{4i} \oplus w_{4(i-1)}$$
$$W_{4i+1} = w_{4i} \oplus w_{4(i-1)+1}$$
$$W_{4i+2} = w_{4i+1} \oplus w_{4(i-1)+2}$$
$$W_{4i+3} = w_{4i+2} \oplus w_{4(i-1)+3}$$

		K_i	
A0	88	23	
FA	54	A3	
FE	2C	39	
17	B1	39	
w_{4i}	w_{4i+1}	w_{4i+2}	w_{4i+3}

Computer Engineering Faculty
University of Isfahan

Key Expansion

K_{i-1}

2B	28	AB	09
7E	AE	F7	CF
15	D2	15	4F
16	A6	88	3C

$w_{4(i-1)}$ $w_{4(i-1)+1}$ $w_{4(i-1)+2}$ $w_{4(i-1)+3}$

$$W_{4i} = t_{4i} \oplus w_{4(i-1)}$$
$$W_{4i+1} = w_{4i} \oplus w_{4(i-1)+1}$$
$$W_{4i+2} = w_{4i+1} \oplus w_{4(i-1)+2}$$
$$W_{4i+3} = w_{4i+2} \oplus w_{4(i-1)+3}$$

K_i

A0	88	23	2A
FA	54	A3	6C
FE	2C	39	76
17	B1	39	05

w_{4i} w_{4i+1} w_{4i+2} w_{4i+3}

Computer Engineering Faculty
University of Isfahan

Key Expansion Example

Original key = 2B7E151628AED2A6ABF7158809CF4F3C

Computer Engineering Faculty
University of Isfahan

K_0 = 2B7E151628AED2A6ABF7158809CF4F3C

K_1 = A0FAFE1788542CB123A33939A26C7605

K_2 = F2C295F27A96B9435935807A7359F67F

K_3 = 3D80477D4716FE3E1E237E446D7A883B

K_4 = EF44A541A8525B7FB671253BDB0BAD00

K_5 = D4D1C6F87C839D87CAF2B8BC11F915BC

K_6 = 6D88A37A110B3EFDDBF98641CA0093FD

K_7 = 4E54F70E5F5FC9F384A64FB24EA6DC4F

K_8 = EAD27321B58DBAD2312BF5607F8D292F

K_9 = AC7766F319FADC2128D12941575C006E

K_{10} = D014F9A8C9EE2589E13F0CC8B6630CA6

Example

Computer Engineering Faculty
University of Isfahan

Plain Text `3243F6A8885A308D313198A2E0370734`

Original key `2B7E151628AED2A6ABF7158809CF4F3C`

Cipher Text `3925841D02DC09FBDC118597196A0B32`

Computer Engineering Faculty
University of Isfahan

Thanks

for reading ☺