

plaintext

3 2

7 c

roundKey 1

6 5

b d

start

5 7

c 1

subByte 1

e c

0 4

shiftRow

e c

4 0

mixColumn 1

2 9

d 3

roundKey 2

6 3

5 8

start

4 a

8 b

subByte 2

8 6

5 f

shiftRow

8 6

f 5

mixColumn 2

9 1

4 a

roundKey 3

1 2

e 6

start

8 3

a c

subByte 3

5 b

6 0

shiftRow

5 b

0 6

mixColumn 3

2 9

c b

roundKey 4

7 5

d b

start

5 c

1 0

subByte 4

e 0

4 a

shiftRow

e 0

a 4

roundKey 5

0 5

3 8

ciphertext

e 5

9 c