

#### Question Number 3

- Using your favorite programming language implement the AES key-expansion algorithm
- Now use the state matrix initialized with your name in Problem 1 as your initial key
- Show the 10 rounds keys in the main assignment1.
- For the fifth round-key show all the steps of the key-expansion algorithm that leads to the sixth round key.

#### Solution.

• AES Key Expansion Algorithm

```
def key_expansion(key):
    all_keys = [key]
    for i in range(10):
        previous_key = transpose_key(all_keys[i])
        prev_last_col = previous_key[-1]
        prev_last_col = rotate_col(prev_last_col)
        prev_last_col = sub_col(prev_last_col)
        prev_last_col = xor_cols(prev_last_col, [RoundConst[i], 0, 0, 0])
        new_key = []
        new_key.append(xor_cols(prev_last_col, previous_key[0]))
        new_key.append(xor_cols(new_key[0], previous_key[1]))
        new_key.append(xor_cols(new_key[1], previous_key[2]))
        new_key.append(xor_cols(new_key[2], previous_key[3]))
        all_keys.append(transpose_key(new_key))
    return all_keys
def main():
    round_keys = key_expansion(initial_key)
    for i, key in enumerate(round_keys):
        print_key(key,i)
if __name__ == "__main__":
    main()
```



## • Initial Key Note

- 1. Dump initial key. The initial key taken from python code in file with name Key\_Expansion.py (when python code rerun this key will be updated)
- 2. Python File Key\_Expansion.py should run in the directory Question\_03(As it is creating .tex file in current directory, which is then used by the latex code to fetch keys)

Initial Key:

0xB3	0x2F	0x2F	0x63
0xB7	0x3B	0x63	0x83
0x29	0x63	0x00	0xED
0x63	0x83	0xFC	0xB7

## • All 10 Round Keys

- 1. Dump all round keys. All round keys taken from output of python code in file with name Key\_Expansion.py (when python code rerun these keys will be updated)
- 2. Python File Key\_Expansion.py should run in the directory Question\_03(As it is creating .tex file in current directory, which is then used by the latex code to fetch all round keys)
- 3. All Round keys are shown on **next page**.





Round 1 Key :

0x5E	0x71	0x5E	0x3D
0xE2	0xD9	0xBA	0x39
0x80	0xE3	0xE3	0x0E
0x98	0x1B	0xE7	0x50

Round 2 Key :

0x4E	0x3F	0x61	0x5C
0x49	0x90	0x2A	0x13
0xD3	0x30	0xD3	0xDD
0xBF	0xA4	0x43	0x13

Round 3 Key :

0x37	0x08	0x69	0x35
0x88	0x18	0x32	0x21
0xAE	0x9E	0x4D	0x90
0xF5	0x51	0x12	0x01

Round 4 Key :

0xC2	0xCA	0xA3	0x96
0xE8	0xF0	0xC2	0xE3
0xD2	0x4C	0x01	0x91

Round 5 Key :

0xC3	0x09	0xAA	0x3C
0x69	0x99	0x5B	0xB8
0x2F	0x63	0x62	0xF3
0xF3	0xC1	0xE1	0xC0

Round 6 Key :

0x8F	0x86	0x2C	0x10
0x64	0xFD	0xA6	0x1E
0x95	0xF6	0x94	0x67
0x18	0xD9	0x38	0xF8

Round 7 Key:

0xBD	0x3B	0x17	0x07
0xE1	0x1C	0xBA	0xA4
0xD4	0x22	0xB6	0xD1
0xD2	0x0B	0x33	0xCB

Round 8 Key :

0x74	0x4F	0x58	0x5F
0xDF	0xC3	0x79	0xDD
0xCB	0xE9	0x5F	0x8E

Round 9 Key :

0xAE	0xE1	0xB9	0xE6
0xC6	0x05	0x7C	0xA1
0xA2	0x4B	0x14	0x9A
0xD8	0xC4	0xEB	0x0F

Round 10 Key:

0xAA	0x4B	0xF2	0x14
0x7E	0x7B	0x07	0xA6
0xD4	0x9F	0x8B	0x11
0x56	0x92	0x79	0x76



## • AES Key Expansion - Stepwise Solution for Round 5 Key

Below is a stepwise explanation of the transformations involved in generating the round key for the sixth round, from the fifth round key

Note: Following result is generated from the python code

## Step 1: Initial Fifth Round Key

The initial key is provided as a 4x4 matrix at the start of the fifth round:

0x090xC30x3C0xAA0x990x5B0xB8Fifth Round Key: 0x2F0x630xF30x620xE10xF30xC10xC0

# Step 2: Rotate the Last Column

The last column is rotated as follows:

Last Column Before Rotation Last Column After Rotation

0x3C	0xB8
0xB8	0xF3
0xF3	0xC0
0xC0	0x3C

# Step 3: Substitute Bytes

Apply the S-Box substitution to the rotated column:

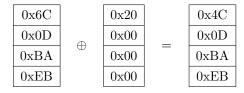
Last Column Before Substitution Last Column After Substitution

> 0xB80x6C0xF30x0D0xC00xBA0x3C0xEB



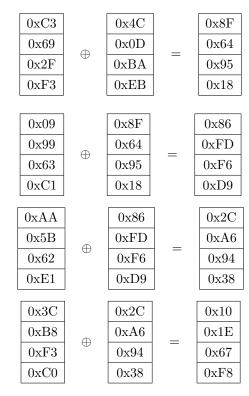
## Step 4: Apply Round Constant

XOR the substituted column with the round constant.



#### Step 5: Generating the next round key

The new key word is generated by XORing the resulting column with the previous column.



Step 6: Next round Key(Sixth Round Key)

Sixth Round Key:

0x8F	0x86	0x2C	0x10
0x64	0xFD	0xA6	0x1E
0x95	0xF6	0x94	0x67
0x18	0xD9	0x38	0xF8