CS-364: Introduction to Cryptography and Network Security LAB

LAB Assignment III

Course Instructor: Dr. Dibyendu Roy Due: Mar 26, 2023, 11:59 pm

Instructions: Code must be written in C and well commented. Submission of code in any other file extension (.pdf, .docx etc) will not be considered. Write your name and roll number on the top of your code. The file name of the code will be YOUR ROLL NO.c

Implement the encryption as well as the decryption of AES′ block cipher.

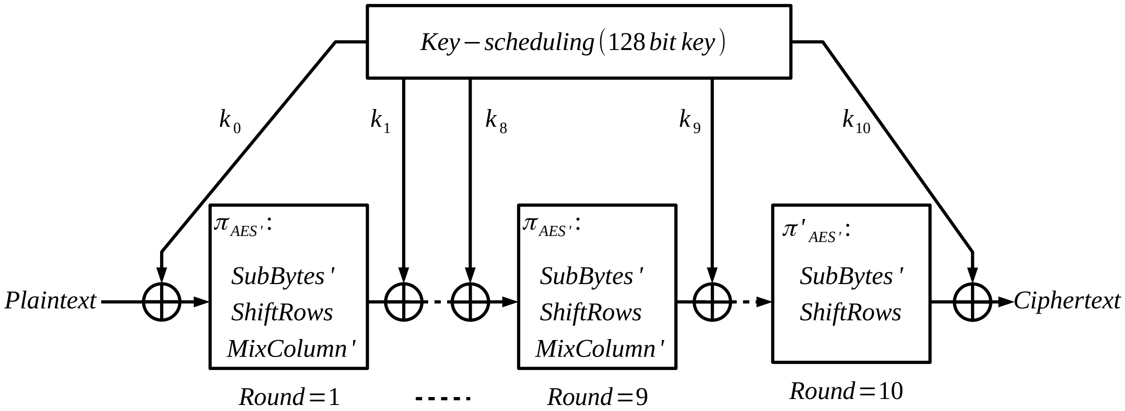

Figure 1: AES′

	Y															
X	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	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
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	C8	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

Figure 2: AES-Subbytes

Consider the Subbyte function Sub (given in Figure 2) of AES. Using the Sub (Figure 2) define a Subbyte′ function $\text{Subbyte}' : \{0,1\}^8 \rightarrow \{0,1\}^8$ as per the following rule,

$$\text{Subbyte}'(x) = Sub(2 * x + 1). \tag{1}$$

Here $+, *$ are the two binary operations of the field $\mathbb{F}_2[x]/ < x^8 + x^4 + x^3 + x + 1 >$.
Consider the following matrix M (given in Equation (2), in integer) instead of original mixcolumn matrix

of AES.

$$M = \begin{bmatrix} 1 & 4 & 4 & 5 \\ 5 & 1 & 4 & 4 \\ 4 & 5 & 1 & 4 \\ 4 & 4 & 5 & 1 \end{bmatrix} \tag{2}$$

The inverse of M is given in Equation (3) (in integer).

$$M^{-1} = \begin{bmatrix} 165 & 7 & 26 & 115 \\ 115 & 165 & 7 & 26 \\ 26 & 115 & 165 & 7 \\ 7 & 26 & 115 & 165 \end{bmatrix} \tag{3}$$

Using M we will perform our Mixcolumn$'$ operation. We will use the same key-scheduling as in AES-128 encryption algorithm. With this setup implement 10 rounds of AES$'$. The pictorial design of AES$'$ is given in Figure 1.

1. Input (scanf): plaintext of 128 bits. Input will be 16 hexadecimal e.g., `a1 12 ...ca 45 ec`

2. Input (scanf): key of 128 bits: Input will be 16 hexadecimal e.g., `b1 32 ...ef 3a cb`

3. Output (printf): encrypt the plaintext using the encryption algorithm of AES$'$ and print the ciphertext of 128 bits: Output will be 16 hexadecimal.

4. Output (printf): decrypt the generated ciphertext using the decryption algorithm of AES$'$ and print the decrypted text of 128 bits: Output will be 16 hexadecimal.

If your code is correct the output in item (4) will match with input in item (1) for all possible random inputs in item (1) and (2).