Project:

Software Implementation of Advanced Encryption Standard

Group Info submission due: 5pm, Monday, June 19, 2017
Project report submission due: 5pm, Monday, July 24, 2017

Table of Contents:

Objective: Implementation of the contemporary symmetrical key cryptographic system.

Forming A Group:

- The project is group based. A group can consist of up to **two** students.
- Find your group code (A, B)
  - Adding up **the last digit in all group members' IDs** to obtain S1. Adding up **the second-to-last digit in all group members' IDs** to obtain S2.
    Let A = S1 mod 5, B = (S2 mod 5) + 5.
  - For example, Alice and Bob form a group with
    Alice's ID: **103 555 456**
    Bob's ID**: 103 555 678**.
    Then A = **6+8** mod 5 = 4, and B = [(**5+7**) mod 5] + 5 = 2+5 =7.
    So Group code: (A, B) = (4, 7).
  - If Alice herself alone forms a group, then
    Group code (A, B) = (1, 5) since A = 6 mod 5 = 1, B = (5 mod 5) +5 = 5.

Project Procedure:

1. Choose a language and implement AES (Round 0 to Round 10, with 128-bit key, refer to the lecture notes on Chapter 4, and a diagram is shown in Appendix A). Programming language is required to be C or C++.
2. Execute your AES program with the sample input and key, and make sure your results match the sample results (refer to Appendix B).
3. Modify all the S-Box in AES as follows and the resultant AES will be called the modified AES:
   a. View A and B in your group code (A, B) as two decimal numbers.
   b. Find Row A and Row B in the S-Box (Page 15, Lecture notes on Chapter 4).
   c. Switch Row A and Row B in the S-Box to obtain the modified S-Box.
   d. AES algorithm with the modified S-Box is called the modified AES.
   e. An example showing how to modify S-Box is given in Appendix C.

4. Use number A in your Group Code (A, B) to select a pair of plaintext and key (Appendix D). Then execute your modified AES program with the assigned plaintext and key to generate the results for each round (refer to Appendix E for result format).

Project files to submit:

1. Report file: Format/edit your results in two pages as shown in Appendix E. Note that you should indicate the language and version, and execution platform. Screenshot of your program results is **NOT** required.
2. Source Code file: Submit your source code for the modified AES.
3. File format:
    a. Report in either PDF or MS Word format.
    b. Source code in either PDF, MS Word, or txt format

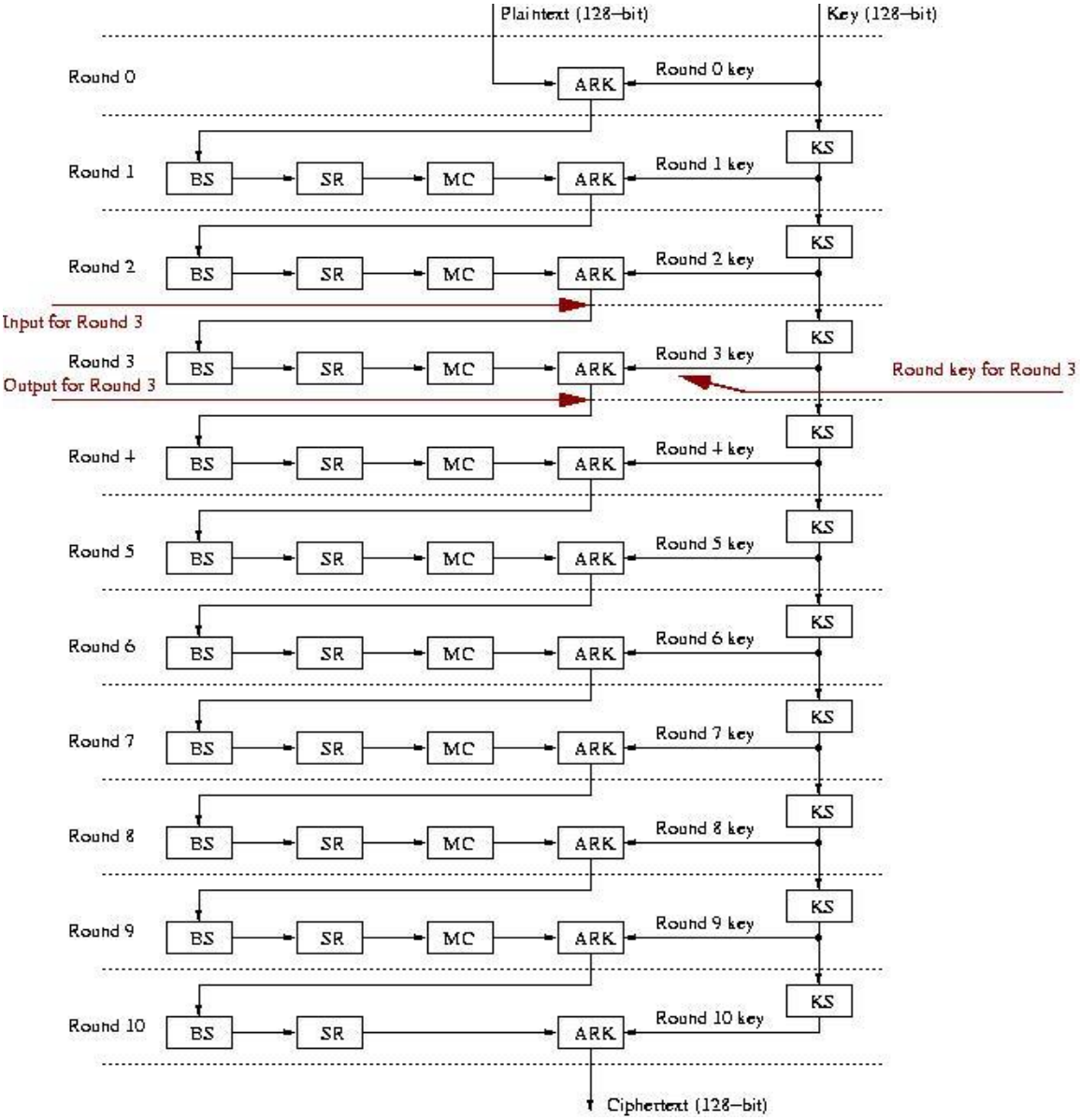
Submission Method:

1. On Blackboard course webpage, go to Resources=>Project and Labs, and then you can find a link for uploading your project report.

Project Grading:

1. The full marks for the project are 100, which has 15% of course weight.
2. Only one copy of submitted project files is required and marked for each group.
3. There will be a deduction of up to 50 marks regardless the quality of your coding, if one of the following is true:
    (a). Your results are different from the correct ones, or (b). you used a pair of plaintext and key different from the ones assigned to you based on the group code.
4. Note: This course is not a programming course. Grading is based on the results. We do not differentiate "minor" and "major" programming errors, as one bit error in ciphertext will lead to total failure in decryption attempt to recover the plaintext.

Appendix A. AES diagram showing input, output, and round keys for each round



Appendix B. Sample Result Page (for testing your program with the original S-Box):

```
------------------------------------------------------------
Original Plaintext and Key:
Input      00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff
Key:       00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
------------------------------------------------------------
Key Schedule Results for Each Round:
------------------------------------------------------------
Round 1:
      Key: d6 aa 74 fd d2 af 72 fa da a6 78 f1 d6 ab 76 fe
Round 2:
      Key: b6 92 cf 0b 64 3d bd f1 be 9b c5 00 68 30 b3 fe
Round 3:
      Key: b6 ff 74 4e d2 c2 c9 bf 6c 59 0c bf 04 69 bf 41
Round 4:
      Key: 47 f7 f7 bc 95 35 3e 03 f9 6c 32 bc fd 05 8d fd
Round 5:
      Key: 3c aa a3 e8 a9 9f 9d eb 50 f3 af 57 ad f6 22 aa
Round 6:
      Key: 5e 39 0f 7d f7 a6 92 96 a7 55 3d c1 0a a3 1f 6b
Round 7:
      Key: 14 f9 70 1a e3 5f e2 8c 44 0a df 4d 4e a9 c0 26
Round 8:
      Key: 47 43 87 35 a4 1c 65 b9 e0 16 ba f4 ae bf 7a d2
Round 9:
      Key: 54 99 32 d1 f0 85 57 68 10 93 ed 9c be 2c 97 4e
Round 10:
      Key: 13 11 1d 7f e3 94 4a 17 f3 07 a7 8b 4d 2b 30 c5
------------------------------------------------------------
Data Results for Each Round:
------------------------------------------------------------
Round 0:
-----Start: 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff
----Output: 00 10 20 30 40 50 60 70 80 90 a0 b0 c0 d0 e0 f0
Round 1:
-----Start: 00 10 20 30 40 50 60 70 80 90 a0 b0 c0 d0 e0 f0
```

```
-----S-Box: 63 ca b7 04 09 53 d0 51 cd 60 e0 e7 ba 70 e1 8c
--ShiftRow: 63 53 e0 8c 09 60 e1 04 cd 70 b7 51 ba ca d0 e7
----MixCol: 5f 72 64 15 57 f5 bc 92 f7 be 3b 29 1d b9 f9 1a
----Output: 89 d8 10 e8 85 5a ce 68 2d 18 43 d8 cb 12 8f e4
Round 2:
----Output: 49 15 59 8f 55 e5 d7 a0 da ca 94 fa 1f 0a 63 f7
Round 3:
----Output: fa 63 6a 28 25 b3 39 c9 40 66 8a 31 57 24 4d 17
Round 4:
----Output: 24 72 40 23 69 66 b3 fa 6e d2 75 32 88 42 5b 6c
Round 5:
----Output: c8 16 77 bc 9b 7a c9 3b 25 02 79 92 b0 26 19 96
Round 6:
----Output: c6 2f e1 09 f7 5e ed c3 cc 79 39 5d 84 f9 cf 5d
Round 7:
----Output: d1 87 6c 0f 79 c4 30 0a b4 55 94 ad d6 6f f4 1f
Round 8:
----Output: fd e3 ba d2 05 e5 d0 d7 35 47 96 4e f1 fe 37 f1
Round 9:
----Output: bd 6e 7c 3d f2 b5 77 9e 0b 61 21 6e 8b 10 b6 89
Round 10:
-----Start: bd 6e 7c 3d f2 b5 77 9e 0b 61 21 6e 8b 10 b6 89
-----S-Box: 7a 9f 10 27 89 d5 f5 0b 2b ef fd 9f 3d ca 4e a7
--ShiftRow: 7a d5 fd a7 89 ef 4e 27 2b ca 10 0b 3d 9f f5 9f
----Output: 69 c4 e0 d8 6a 7b 04 30 d8 cd b7 80 70 b4 c5 5a
--------------------------------------------------------
```

Appendix C. An example on how to modify the original S-Box to obtain the modified S-Box with Group Code (A, B)=(4, 7)

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

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

```
e1  f8  98  11  69  d9  8e  94  9b  1e  87  e9  ce  55  28  df    14
8c  a1  89  0d  bf  e6  42  68  41  99  2d  0f  b0  54  bb  16    15
```

Appendix D. Select Plaintext and Key (both in hexadecimal form):

- Group Code (A, B) = (0, 5)
  - 0000 0000 0000 0000 0000 0000 0000 abc0 (plaintext)
  - 1a0c 24f2 8754 93bc b708 0e43 930f 5670 (key)
- Group Code (A, B) = (0, 6)
  - 0000 0000 0000 0000 0000 0000 0000 abc1 (plaintext)
  - 1a0c 24f2 8754 93bc b708 0e43 930f 5671 (key)
- Group Code (A, B) = (0, 7)
  - 0000 0000 0000 0000 0000 0000 0000 abc2 (plaintext)
  - 1a0c 24f2 8754 93bc b708 0e43 930f 5672 (key)
- Group Code (A, B) = (0, 8)
  - 0000 0000 0000 0000 0000 0000 0000 abc3 (plaintext)
  - 1a0c 24f2 8754 93bc b708 0e43 930f 5673 (key)
- Group Code (A, B) = (0, 9)
  - 0000 0000 0000 0000 0000 0000 0000 abc4 (plaintext)
  - 1a0c 24f2 8754 93bc b708 0e43 930f 5674 (key)
- Group Code (A, B) = (1, 5)
  - 0000 0000 0000 0000 0000 0000 0000 abc5 (plaintext)
  - 1a0c 24f2 8754 93bc b708 0e43 930f 5675 (key)
- Group Code (A, B) = (1, 6)
  - 0000 0000 0000 0000 0000 0000 0000 abc6 (plaintext)
  - 1a0c 24f2 8754 93bc b708 0e43 930f 5676 (key)
- Group Code (A, B) = (1, 7)
  - 0000 0000 0000 0000 0000 0000 0000 abc7 (plaintext)
  - 1a0c 24f2 8754 93bc b708 0e43 930f 5677 (key)
- Group Code (A, B) = (1, 8)
  - 0000 0000 0000 0000 0000 0000 0000 abc8 (plaintext)
  - 1a0c 24f2 8754 93bc b708 0e43 930f 5678 (key)
- Group Code (A, B) = (1, 9)
  - 0000 0000 0000 0000 0000 0000 0000 abc9 (plaintext)
  - 1a0c 24f2 8754 93bc b708 0e43 930f 5679 (key)
- Group Code (A, B) = (2, 5)
  - 0000 0000 0000 0000 0000 0000 0000 abca (plaintext)
  - 1a0c 24f2 8754 93bc b708 0e43 930f 567a (key)
- Group Code (A, B) = (2, 6)
  - 0000 0000 0000 0000 0000 0000 0000 abcb (plaintext)
  - 1a0c 24f2 8754 93bc b708 0e43 930f 567b (key)
- Group Code (A, B) = (2, 7)

    - 0000 0000 0000 0000 0000 0000 0000 abcc (plaintext)
    - 1a0c 24f2 8754 93bc b708 0e43 930f 567c (key)
- Group Code (A, B) = (2, 8)
    - 0000 0000 0000 0000 0000 0000 0000 abcd (plaintext)
    - 1a0c 24f2 8754 93bc b708 0e43 930f 567d (key)
- Group Code (A, B) = (2, 9)
    - 0000 0000 0000 0000 0000 0000 0000 abce (plaintext)
    - 1a0c 24f2 8754 93bc b708 0e43 930f 567e (key)
- Group Code (A, B) = (3, 5)
    - 0000 0000 0000 0000 0000 0000 0000 abcf (plaintext)
    - 1a0c 24f2 8754 93bc b708 0e43 930f 567f (key)
- Group Code (A, B) = (3, 6)
    - 0000 0000 0000 0000 0000 0000 0000 abd0 (plaintext)
    - 1a0c 24f2 8754 93bc b708 0e43 930f 5680 (key)
- Group Code (A, B) = (3, 7)
    - 0000 0000 0000 0000 0000 0000 0000 abd1 (plaintext)
    - 1a0c 24f2 8754 93bc b708 0e43 930f 5681 (key)
- Group Code (A, B) = (3, 8)
    - 0000 0000 0000 0000 0000 0000 0000 abd2 (plaintext)
    - 1a0c 24f2 8754 93bc b708 0e43 930f 5682 (key)
- Group Code (A, B) = (3, 9)
    - 0000 0000 0000 0000 0000 0000 0000 abd3 (plaintext)
    - 1a0c 24f2 8754 93bc b708 0e43 930f 5683 (key)
- Group Code (A, B) = (4, 5)
    - 0000 0000 0000 0000 0000 0000 0000 abd4 (plaintext)
    - 1a0c 24f2 8754 93bc b708 0e43 930f 5684 (key)
- Group Code (A, B) = (4, 6)
    - 0000 0000 0000 0000 0000 0000 0000 abd5 (plaintext)
    - 1a0c 24f2 8754 93bc b708 0e43 930f 5685 (key)
- Group Code (A, B) = (4, 7)
    - 0000 0000 0000 0000 0000 0000 0000 abd6 (plaintext)
    - 1a0c 24f2 8754 93bc b708 0e43 930f 5686 (key)
- Group Code (A, B) = (4, 8)
    - 0000 0000 0000 0000 0000 0000 0000 abd7 (plaintext)
    - 1a0c 24f2 8754 93bc b708 0e43 930f 5687 (key)
- Group Code (A, B) = (4, 9)
    - 0000 0000 0000 0000 0000 0000 0000 abd8 (plaintext)
    - 1a0c 24f2 8754 93bc b708 0e43 930f 5688 (key)

Appendix E. Format for Result Pages (for format template only):

- **Example Result Page 1:**

```
------------------------------------------------------------
ID1 = 103 555 123 (Alice Smith)
ID2 = 103 555 876 (Bob Jones)
Group Code (A,B) = (4,7)
Assigned Plaintext and Key:
    0000 0000 0000 0000 0000 0000 0000 abd6 (plaintext)
    1a0c 24f2 8754 93bc b708 0e43 930f 5686 (key)

The program is written in C for operating system Fedora (Linux).
------------------------------------------------------------
Key Schedule Results for Each Round with the modified AES:
------------------------------------------------------------
Round 0:
      Key: 2a 0c 24 f2 87 54 93 bc b7 08 0e 43 93 0c 53 0c
Round 1:
      Key: d6 aa 74 fd d2 af 72 fa da a6 78 f1 d6 ab 76 fe
Round 2:
      Key: b6 92 cf 0b 64 3d bd f1 be 9b c5 00 68 30 b3 fe
Round 3:
      Key: b6 ff 74 4e d2 c2 c9 bf 6c 59 0c bf 04 69 bf 41
Round 4:
      Key: 47 f7 f7 bc 95 35 3e 03 f9 6c 32 bc fd 05 8d fd
Round 5:
      Key: 3c aa a3 e8 a9 9f 9d eb 50 f3 af 57 ad f6 22 aa
Round 6:
      Key: 5e 39 0f 7d f7 a6 92 96 a7 55 3d c1 0a a3 1f 6b
Round 7:
      Key: 14 f9 70 1a e3 5f e2 8c 44 0a df 4d 4e a9 c0 26
Round 08:
      Key: 47 43 87 35 a4 1c 65 b9 e0 16 ba f4 ae bf 7a d2
Round 9:
      Key: 54 99 32 d1 f0 85 57 68 10 93 ed 9c be 2c 97 4e
Round 10:
```

```
Key: 13 11 1d 7f e3 94 4a 17 f3 07 a7 8b 4d 2b 30 c5
```

- **Example Result Page 2:**

```
------------------------------------------------------------
Data Results for Each Round with the modified AES:
------------------------------------------------------------
Round 0:
-----Start: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 16
----Output: 00 10 20 30 40 50 60 70 80 90 a0 b0 c0 d0 e0 f0
Round 1:
----Output: 89 d8 10 e8 85 5a ce 68 2d 18 43 d8 cb 12 8f e4
Round 2:
----Output: 49 15 59 8f 55 e5 d7 a0 da ca 94 fa 1f 0a 63 f7
Round 3:
----Output: fa 63 6a 28 25 b3 39 c9 40 66 8a 31 57 24 4d 17
Round 4:
----Output: 24 72 40 23 69 66 b3 fa 6e d2 75 32 88 42 5b 6c
Round 5:
----Output: c8 16 77 bc 9b 7a c9 3b 25 02 79 92 b0 26 19 96
Round 6:
----Output: c6 2f e1 09 f7 5e ed c3 cc 79 39 5d 84 f9 cf 5d
Round 7:
----Output: d1 87 6c 0f 79 c4 30 0a b4 55 94 ad d6 6f f4 1f
Round 8:
----Output: fd e3 ba d2 05 e5 d0 d7 35 47 96 4e f1 fe 37 f1
Round 9:
----Output: bd 6e 7c 3d f2 b5 77 9e 0b 61 21 6e 8b 10 b6 89
Round 10:
----Output: 69 c4 e0 d8 6a 7b 04 30 d8 cd b7 80 70 b4 c5 5a
------------------------------------------------------------
```