Justin Cabral

ECE/CS 578

Assignment #3

## 1- AES

Compute the given steps below. You can use AES specification for more explanation. Show your work and present the results in a table to make it easy to follow.

1. a- Convert the given 128-bit input to Hexadecimal form.

| Input Byte # | Binary | Hex |
|---|---|---|
| Byte 1 | 0101 0110 | 56 |
| Byte 2 | 1110 0010 | E2 |
| Byte 3 | 0001 1001 | 19 |
| Byte 4 | 1011 0010 | B2 |
| Byte 5 | 0100 0100 | 44 |
| Byte 6 | 1011 0011 | B3 |
| Byte 7 | 1101 1011 | DB |
| Byte 8 | 0100 0011 | 43 |
| Byte 9 | 1000 0001 | 81 |
| Byte 10 | 0001 1110 | 1E |
| Byte 11 | 1001 1101 | 9D |
| Byte 12 | 0011 1010 | 3A |
| Byte 13 | 1001 1110 | 9E |
| Byte 14 | 1000 0101 | 85 |
| Byte 15 | 1111 0011 | F3 |
| Byte 16 | 0100 1111 | 4F |

2. b- Write the input in a state diagram (4 by 4 matrix).

| Input State Matrix | | | |
|---|---|---|---|
| 56 | 44 | 81 | 9E |
| E3 | B3 | 1E | 85 |
| 19 | DB | 9D | F3 |
| B2 | 43 | 3A | 4F |

3. c- Apply SubBytes Step: use AES S-box to substitute the input.

| Apply SubBytes | | | |
|---|---|---|---|
| B1 | 1B | 0C | 0B |
| 98 | 6D | 72 | 97 |
| D4 | B9 | 5E | 0D |
| 37 | 1A | 80 | 84 |

4. d- Apply ShiftRows Step.

| Apply ShiftRow | | | |
|---|---|---|---|
| B1 | 1B | 0C | 0B |
| 6D | 72 | 97 | 98 |
| 5E | 0D | D4 | B9 |
| 84 | 37 | 1A | 80 |

5. e- Apply Mixcolumns Step: use Irreducible polynomial $P(x) = x^8 + x^4 + x^3 + x +$

**Blue = Use of irreducible polynomial in answer**
**Black = No reduction needed in answer**

**C0 = $(x^8+x^6+x^5+x) + (x^7+x^5+x^4+x^2+x+1) + (x^6+x^4+x^3+x^2+x) + (x^7+x^2) = x^4+x^2$ = [14]**
**C1 = $(x^7+x^5+x^4+1) + (x^7+x^6+x^4+x^3+x) + (x^7+x^6+x^5+x) + (x^7+x^2)$ = x^3 + x^2 + 1 = [0D]**
**C2 = $(x^7+x^5+x^4+1) + (x^6+x^5+x^3+x^2+1) + (x^7+x^5+x^4+x^3+x^2) + (x^8+x^7+x^3+x^2) = x^7+x^6+x^5+x^4+x^2+x+1$ = [F7]**
**C3 = $(x^8+x^7+x^6+x^4+x+1) + (x^6+x^5+x^3+x^2+1) + (x^6+x^4+x^3+x^2) + (x^8+x^3) = x^7+x^6+x^5+x^3+x$ = [EA]**

| Mixed Column 1 |
|---|
| 14 |
| 0D |
| F7 |
| EA |

**C4 = $(x^5+x^4+x^2+x) + (x^7+x^4+x^2+x) + (x^3+x^2+1) + (x^5+x^4+x^2+x+1) = x^7 + x^4 + x^3 + x$ = [9A]**
**C5 = $(x^4+x^3+x+1) + (x^7+x^6+x^5+x^2) + (x^4+x^2+x+1) + (x^5+x^4+x^2+x+1) = x^7 + x^6 + x^4 + x^3+x^2+x+1$ = [DF]**
**C6 = $(x^4+x^3+x+1) + (x^6+x^5+x^4+x) + (x^4+x^3+x) + (x^6+x^4+x^3+1) = x^5 + x^3 + x$ = [2A]**
**C7 = $(x^5+x^3+x^2+1) + (x^6+x^5+x^4+x) + (x^3+x^2+1) + (x^6+x^5+x^3+x^2+x) = x^5 + x^4 + x^3 + x^2$ = [3C]**

| Mixed Column 2 |
|---|
| 9A |
| DF |
| 2A |
| 3C |

**C8 = $(x^4+x^3) + (x^8+x^7+x^5+x^4+x^3+1) + (x^7+x^6+x^4+x^2) + (x^4+x^3+x) = x^6+x^5+x^4+x^2$ = [74]**
**C9 = $(x^3+x^2) + (x^8+x^5+x^3+x^2+x) + (x^8+x^6+x^5+x^4+x^3+x^2) + (x^4+x^3+x) = x^6 + x^2$ = [44]**
**C10 = $(x^3+x^2) + (x^7+x^4+x^2+x+1) + (x^8+x^7+x^5+x^3) + (x^5+x^3+x^2+x) = x^2+x$ = [06]**
**C11 = $(x^4+x^2) + ( x^7+x^4+x^2+x+1) + (x^7+x^6+x^4+x^2) + (x^5+x^4+x^2) = x^6 + x^5+x+1$ = [63]**

| Mixed Column 3 |
|---|
| 74 |
| 44 |
| 06 |
| 63 |

**C12 = $(x^4+x^2+x) + (x^8+x^7+x^5+x^3) + (x^7+x^5+x^4+x^3+1) + (x^7) = x^7+x^4+x^3+x^2$ = [9C]**
**C13 = $(x^3+x+1) + (x^8+x^5+x^4) + (x^8+x^7+x^6+x^3+x+1) + (x^7) = x^6 + x^5 + x^4$ = [70]**
**C14 = $(x^3+x+1) + (x^7+x^4+x^3) + (x^8+x^6+x^5+x^4+x) + (x^8+x^7) = x^6+ x^5 + 1$ = [61]**
**C15 = $(x^4+x^3+x^2+1) + (x^7+x^4+x^3) + (x^7+x^5+x^4+x^3+1) + (x^8) = x^8+x^5+x^4+x^3+x^2 = x^5+x^2+x+1$ = [27]**

| Mixed Column 4 |
|---|
| 9C |
| 70 |
| 61 |
| 27 |

| Input State After Mix Column | | | |
|---|---|---|---|
| 14 | 9A | 74 | 9C |
| 0D | DF | 44 | 70 |
| F7 | 2A | 06 | 61 |
| EA | 3C | 2 | 27 |

6. f- Apply AddRoundKey Step: use the given round key.

| Round Key Hex Conversion | | |
|---|---|---|
| Input Byte # | Binary | Hex |
| Byte 1 | 0011 0100 | 34 |
| Byte 2 | 0000 1001 | 09 |
| Byte 3 | 1010 0110 | A6 |
| Byte 4 | 1101 0110 | D6 |
| Byte 5 | 0111 0110 | 76 |
| Byte 6 | 1001 0011 | 93 |
| Byte 7 | 0010 1000 | 28 |
| Byte 8 | 0100 0011 | 43 |
| Byte 9 | 1101 0101 | D5 |
| Byte 10 | 0000 0100 | 04 |
| Byte 11 | 1011 1000 | C8 |
| Byte 12 | 1011 1101 | CD |
| Byte 13 | 1111 0001 | F1 |
| Byte 14 | 1011 0101 | B5 |
| Byte 15 | 0111 0010 | 72 |
| Byte 16 | 0111 0010 | 72 |

- Perform the XOR with State and Round Key Table

| State After Round Key XOR | | | |
|---|---|---|---|
| 20 | EC | A1 | 6D |
| 04 | 4C | 40 | C5 |
| 51 | 02 | CE | 13 |
| 3C | 7F | AE | 55 |

- Convert Hex to Binary for our Cipher Output

**Cipher Text:**
00100000000001000101000100111100110110001001100000000100111111101000010100000001100111010101110011011011100010100010011010101010101

**2- Modular Arithmetic** is the basis of many cryptosystems. As a consequence, we will address this topic with several problems in this and upcoming chapters.

**Compute the results:**

1. $37 \cdot 3\ mod\ 23$

37 * 3 = 111
111/23 = 4 R 19
37 * 3 ≡ 19 mod 23

2. $19 \cdot 13\ mod\ 23$

19 * 13 = 247
247/23 = 10 R 17
19 * 13 ≡ 17 mod 23

3. $18 \cdot 15\ mod\ 12$

15 mod 12 ≡ 3 mod 12

18 * 3 ≡ 24 mod 12 ≡ 0 mod 12

4. $15 \cdot 29 + 11 \cdot 15\ mod\ 23$

29 mod 23 ≡ 6 mod 23
15 * 6 = 90/23 = 3 R 21
15 * 6 mod 23 ≡ 21 mod 23
11 * 15 = 165/23 = 7 R 4
11 * 15 mod 23 ≡ 4 mod 23
21 + 4 mod 23 ≡ 25 mod 23 ≡ 2 mod 23

**Find the inverses in the given modular spaces:**

v. $8^{-1}\, mod\ 17$

GCD(8, 17) = 1. Thus, a modular multiplicative inverse exists.

$15 \equiv 8^{-1}$ mod 17
$15 * 8 \equiv 1$ mod 17

Therefore, the inverse of $8^{-1}$ mod 17 is <u>15</u>

vi. $5^{-1}\, mod\ 17$

GCD(5, 17) = 1. Thus, a modular multiplicative inverse exists.

$7 \equiv 5^{-1}$ mod 17
$7 * 5 \equiv 1$ mod 17

Therefore, the inverse of $5^{-1}$ mod 17 is <u>7</u>

vii. $5^{-1}\, mod\ 37$

GCD(5, 37) = 1. Thus, a modular multiplicative inverse exists.

$15 \equiv 5^{-1}$ mod 37
$15 * 5 \equiv 1$ mod 37

Therefore, the inverse of $5^{-1}$ mod 37 is <u>15</u>

viii. $10^{-1}\, mod\ 15$

GCD(10, 15) != 1. Thus, <u>**NO**</u> modular multiplicative inverse exists.

**List all elements of modulo 216 with no multiplicative inverse.**

Any element N of modulus 216 will have a multiplicative inverse if and only if the GCD of N and 216 is equal to 1.

Any element N of modulus 216 will **NOT** have a multiplicative inverse if and only if it is divisible by 2 or 3.

Therefore, our list is the total of the elements N divisible by 2 and 3

Elements Divisible by 2:
0, 2 , 4 , 6 , 8 , 10 , 12 , 14 , 16 , 18 ,20 ,22 ,24 , 26 , 28 , 30 , 32 , 34 , 36 ,38 , 40 , 42 , 44 , 46 , 48 , 50 , 52 , 54 , 56 , 58 , 60 , 62 , 64 , 66 , 68 , 70 , 72 , 74 , 76 , 78 , 80 , 82 , 84 , 86 , 88 , 90 , 92 , 94 , 96 , 98 , 100 , 102 , 104 , 106 , 108 , 110 , 112 , 114 , 116 , 118 ,120 ,122 ,124 , 126 , 128 , 130 , 132 , 134 , 136 ,138 , 140 , 142 , 144 , 146 , 148 , 150 , 152 , 154 , 156 , 158 , 160 , 162 , 164 , 166 , 168 , 170 , 172 , 174 , 176 ,178 , 180 , 182 , 184 , 186 , 188 , 190 , 192 , 194 , 196 , 198 , 200 ,202, 204 , 206 , 208 , 210 , 212 , 214

Elements Divisible by 3:
3, 9, 15, 21 , 27 , 33 , 39 , 45 , 51 , 57 , 63 , 69 , 75 , 81 , 87 , 93 , 99 , 105 ,111 , 117 , 123 , 129 , 135 , 141 , 147 , 153 , 159 , 165 , 171 , 177 , 183 , 189 , 195 , 201 , 207 , 213.