The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260/COMP6360 Data Security

Week 8 Workshop – 2 & 3 May 2019

Solutions

1. Mix Column transformation of AES operates on each column of the State individually and can be defined as follows:

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} = \begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}$$

Verify that the *State* column

87
6E
46
A6

is transformed into

47
37
94
ED

Solution: see text

Remember AES operates in GF(2^8) with irreducible polynomial $x^8 + x^4 + x^3 + x + 1$. What we want to verify is the following:

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} 87 \\ 6E \\ 46 \\ A6 \end{bmatrix} = \begin{bmatrix} 47 \\ 37 \\ 94 \\ ED \end{bmatrix}$$

For the first element in the output, we have:

$$[02 \quad 03 \quad 01 \quad 01] \begin{bmatrix} 87 \\ 6E \\ 46 \\ A6 \end{bmatrix} = 47$$

Expanded out, this is: $(02 \cdot 87) + (03 \cdot 6E) + 46 + A6$.

Looking at $(02 \cdot 87)$, the first thing to do is to convert to binary:

$$02 \rightarrow 0000\ 0010$$
$$87 \rightarrow 1000\ 0111$$

We can carry out multiplication as introduced earlier, applying the modulo operator using long division with the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$:

```
  1000 0111    (87)
x 0000 0010    (02)
  0000 0000
1 0000 1110
1 0000 1110 -> 10E
```

Now applying the modulo operator using long division:

```
                1
           _________
1 0001 1011(1 0000 1110
            1 0001 1011
            0 0001 0101 -> 15
```

When implementing the Mix Column transformation, note that multiplication by 2 in GF(2^8) is equivalent to a left shift, dropping the top bit and conditionally applying XOR with (0001 1011) if the multiplication causes an overflow. We can verify if this is equivalent in this case: left shifting 87 and dropping the leftmost bit, we get:

$$0000\ 1110 \rightarrow 0E$$

Then applying XOR, because the dropped bit was a 1:

```
  0000 1110
+ 0001 1011
  0001 0101 -> 15
```

Which is the same result as using multiplication followed by the modulo operator.

Next, we will solve $(03 \cdot 6E)$. Converting 6E to binary we get:

$$6E \rightarrow 0110\ 1110$$

```
  0110 1110   (6E)
x 0000 0011   (03)
  0110 1110   (6E)
0 1101 1100   (DC)
0 1011 0010 -> B2
```

For implementation, note that this is equivalent to $(02 \cdot 6E) + (01 \cdot 6E)$, which means we can use the left shift technique described above followed by an addition to implement a multiplication by 3. Since the Mix Columns transformation only uses multiplication by 1, 2 and 3, this is enough to implement this transformation, without needing to implement general multiplication between any two elements of GF(2^8).

So, putting this back in to the original sum, we have $15 + B2 + 46 + A6$:

```
  0001 0101   (15)
  1011 0010   (B2)
  0100 0110   (46)
+ 1010 0110   (A6)
  0100 0111 -> 47
```

Which gives us 47 as expected.

For the second element, we have:

$$[02 \quad 03 \quad 01 \quad 01] \begin{bmatrix} 87 \\ 6E \\ 46 \\ A6 \end{bmatrix} = 37$$

For the third element, we have:

$$[02 \quad 03 \quad 01 \quad 01] \begin{bmatrix} 87 \\ 6E \\ 46 \\ A6 \end{bmatrix} = 94$$

For the fourth element, we have:

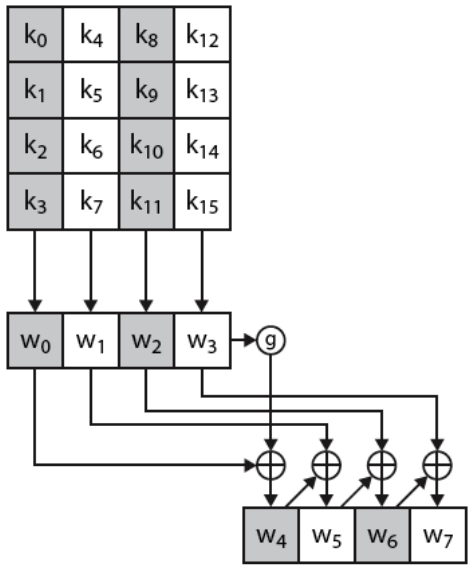
$$[02 \quad 03 \quad 01 \quad 01] \begin{bmatrix} 87 \\ 6E \\ 46 \\ A6 \end{bmatrix} = ED$$

2. AES takes as input a 4 word (16 bytes, 128bits) key and expends it into 44 words according to the following algorithm:

```
KeyExpansion (byte key[16], word w[44])
{     word temp
      for (i=0; i<4; i++)
            w[i]=(key[4×i], key[4×i+1], key[4×i+2], key[4×i+3]);
      for (i=4; i<44; i++)
      {     temp=w[i-1];
            if (i mod 4 = 0) temp=SubWord(RotWord(temp))⊕ Rcon[i/4];
            w[i]=w[i-4] ⊕ temp
      }
}
```

where SubWord is a byte substitution using S-box and RotWord is a one byte circular left shift. Round constant Rcon[j]=(RC[j],0,0,0) where RC[1]=1, RC[j]=2RC[j-1]:

j	1	2	3	4	5	6	7	8	9	10
RC[j]	01	02	04	08	10	20	40	80	1B	36



Show the first eight words of the key expansion for a 128-bit key of all zeroes.

Solution:

W(0)= [00 00 00 00]
W(1)= [00 00 00 00]
W(2)= [00 00 00 00]
W(3)= [00 00 00 00]
W(4)= [62 63 63 63]
W(5)= [62 63 63 63]
W(6)= [62 63 63 63]
W(7)= [62 63 63 63]

Note: Putting 00 in the s-box gives 63, {63 63 63 63} ⊕ {01 00 00 00} = {62 63 63 63}
The "g" in the diagram refers to `SubWord(RotWord(temp))⊕ Rcon`

The first four words are simply the given key, which in this case are all zeros:

$$w(0) = [k_0 k_1 k_2 k_3]$$
$$w(1) = [k_4 k_5 k_6 k_7]$$
$$w(2) = [k_8 k_9 k_{10} k_{11}]$$
$$w(3) = [k_{12} k_{13} k_{14} k_{15}]$$

The fifth word (i.e. w4) is calculated by applying XOR to the first word and the output of the "g" function. The "g" function rotates the bytes to the left, puts them though the S-box, then applies an XOR to that with the round constant (RC_j, 0, 0, 0)

$$w(4) = [k_0 k_1 k_2 k_3] \oplus ([S(k_{13})\ S(k_{14})\ S(k_{15})\ S(k_{12})] \oplus [01\ 00\ 00\ 00])$$

The sixth word (w5) is calculated as the fifth word XORed with the second word (w1). The seventh word (w6) is calculated as the sixth word (w5) XORed with the third word (w2). The eighth word (w7) is calculated as the seventh word (w6) XORed with the fourth word (w3).

3. Show that $x^i \bmod (x^4+1) = x^{i \bmod 4}$. (Look at Lecture 7, or how AES defines polynomial arithmetic for polynomials of degree less than 4 in GF(2^8) to see the context of this equation)

Solution:

We want to show $x^i \bmod (x^4+1) = x^{i \bmod 4}$ when operating using polynomials in in GF(2^8).

First, we can start with $i = 4$, so we need to show $x^4 \bmod (x^4+1) = x^0 = 1$.

We can show this is the case by writing x^4 in the following form:

$$x^4 = [1 \times (x^4+1)] + 1$$

Note that 1+1 =0 due to addition being the XOR operation

When $i = 4a$ (i.e. a multiple of 4), then we can always break it down into components to get 1. For example:

$$\begin{aligned} x^8 \bmod (x^4+1) &= x^4 \bmod (x^4+1) \times x^4 \bmod (x^4+1) \\ &= 1 \times 1 \\ &= 1 \end{aligned}$$

When i is not a multiple of 4, we can always separate out the multiples of 4, and write i in the form: $i = 4a + (i \bmod 4)$, and then we can simplify this to the expected form:

$$\begin{aligned} x^i \bmod (x^4+1) &= x^{4a+(i \bmod 4)} \bmod (x^4+1) \\ &= (x^{4a} \times x^{(i \bmod 4)}) \bmod (x^4+1) \\ &= x^{4a} \bmod (x^4+1) \times x^{(i \bmod 4)} \bmod (x^4+1) \\ &= 1 \times x^{(i \bmod 4)} \bmod (x^4+1) \\ &= x^{(i \bmod 4)} \bmod (x^4+1) \\ &= x^{(i \bmod 4)} \end{aligned}$$

As required.

4. In the discussion of mixed columns and inverse mixed columns it was stated that b(x)=a^{-1}(x) mod (x^4+1), where
a(x) = {03}x^3 + {01}x^2 + {01}x + {02} and
b(x) = {0B}x^3 +{0D}x^2 + {09}x + {0E}.
Show that this is true.

Solution:

This notation comes from the polynomial arithmetic description of the Mix Columns step. a(x) is the polynomial used for the forwards transform, b(x) is the polynomial used for the inverse transform. Notice how the coefficients of the polynomials match the elements in the matrix multiplication.

For this question, we want to show $b(x) = (a^{-1}(x))\text{mod}(x^4 + 1)$, or equivalently $\big(a(x) \cdot b(x)\big)\text{mod}(x^4 + 1) = 1$.

Note that $a(x)$ and $b(x)$ are not themselves polynomials in GF(2^8), but rather polynomials with coefficients which are elements in GF(2^8). They are elements in a polynomial ring where the elements have a degree of less than 4 and have coefficients which are elements of GF(2^8). The main observation we'll need for this ring is the following:

$$x^i \text{mod}(x^4 + 1) = x^{i \bmod 4}$$

Now we can multiply $a(x)$ and $b(x)$:

$$\begin{aligned}
&\big(a(x) \cdot b(x)\big)\text{mod}(x^4 + 1) \\
&\quad = [(a_3x^3 + a_2x^2 + a_1x + a_0)(b_3x^3 + b_2x^2 + b_1x + b_0)]\text{mod}(x^4 + 1) \\
&\quad = [c_6x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x^1 + c_0]\text{mod}(x^4 + 1) \\
&\quad = [c_3x^3 + (c_2 + c_6)x^2 + (c_1 + c_5)x^1 + (c_0 + c_4)]\text{mod}(x^4 + 1)
\end{aligned}$$

Where:

$$\begin{aligned}
a_0 &= 02, a_1 = 01, a_2 = 01, a_3 = 03 \\
b_0 &= 0E, b_1 = 09, b_2 = 0D, b_3 = 0B
\end{aligned}$$

$$\begin{aligned}
c_0 &= a_0b_0 \\
c_1 &= a_1b_0 + a_0b_1 \\
c_2 &= a_2b_0 + a_1b_1 + a_0b_2 \\
c_3 &= a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3 \\
c_4 &= a_3b_1 + a_2b_2 + a_1b_3 \\
c_5 &= a_3b_2 + a_2b_3 \\
c_6 &= a_3b_3
\end{aligned}$$

And we used $x^i \text{mod}(x^4 + 1) = x^{i \bmod 4}$ to go from the second last line to the last line. If we substitute the values back in, we can verify that $\big(a(x) \cdot b(x)\big)\text{mod}(x^4 + 1) = 1$.

Calculating c_0:

$$\begin{aligned} c_0 &= a_0 b_0 \\ &= 02 \cdot 0E \\ &= 1C \end{aligned}$$

```
  0000 1110   (0B)
x 0000 0010   (02)
  0000 0000
  0001 1100
  0001 1100 -> 1C
```

Calculating c_4:

$$\begin{aligned} c_4 &= a_3 b_1 + a_2 b_2 + a_1 b_3 \\ &= 03 \cdot 09 + 01 \cdot 0D + 01 \cdot 0B \\ &= 1B + 0D + 0B \end{aligned}$$

```
  0000 1001   (09)
x 0000 0011   (03)
  0000 1001
  0001 0010
  0001 1011 -> 1B
```

```
  0001 1011   (1B)
  0000 1101   (0D)
+ 0000 1011   (0B)
  0001 1101 -> 1D
```

Calculating $c_0 + c_4$:

$c_0 + c_4 = 1C + 1D)$

$$= 01$$

```
  0001 1101   (1D)
+ 0001 1100   (1C)
  0000 0001 -> 01
```

And the rest can be found in like manner.

We want to show that d(x) = a(x) x b(x) mod $(x^4 + 1) = 1$. Substituting into Equation (5.12) in Appendix 5A, we have:

$$\begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} 0E \\ 09 \\ 0D \\ 0B \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

But this is the same set of equations discussed in the subsection on the MixColumn transformation:

$$(\{0E\} \bullet \{02\}) \oplus \{0B\} \oplus \{0D\} \oplus (\{09\} \bullet \{03\}) = \{01\}$$
$$(\{09\} \bullet \{02\}) \oplus \{0E\} \oplus \{0B\} \oplus (\{0D\} \bullet \{03\}) = \{00\}$$
$$(\{0D\} \bullet \{02\}) \oplus \{09\} \oplus \{0E\} \oplus (\{0B\} \bullet \{03\}) = \{00\}$$
$$(\{0B\} \bullet \{02\}) \oplus \{0D\} \oplus \{09\} \oplus (\{0E\} \bullet \{03\}) = \{00\}$$

The first equation is verified in the text. For the second equation, we have {09} • {02} = 00010010; and {0D} • {03} = {0D} ⊕ ({0D} • {02}) = 00001101 ⊕ 00011010 = 00010111. Then

$$\begin{aligned} \{09\} \bullet \{02\} &= 00010010 \\ \{0E\} &= 00001110 \\ \{0B\} &= 00001011 \\ \{0D\} \bullet \{03\} &= \underline{00010111} \\ & \quad 00000000 \end{aligned}$$

For the third equation, we have {0D} • {02} = 00011010; and {0B} • {03} = {0B} ⊕ ({0B} • {02}) = 00001011 ⊕ 00010110 = 00011101. Then

$$\begin{aligned} \{0D\} \bullet \{02\} &= 00011010 \\ \{09\} &= 00001001 \\ \{0E\} &= 00001110 \\ \{0B\} \bullet \{03\} &= \underline{00011101} \\ & \quad 00000000 \end{aligned}$$

For the fourth equation, we have {0B} • {02} = 00010110; and {0E} • {03} = {0E} ⊕ ({0E} • {02}) = 00001110 ⊕ 00011100 = 00010010. Then

$$\begin{aligned} \{0B\} \bullet \{02\} &= 00010110 \\ \{0D\} &= 00001101 \\ \{09\} &= 00001001 \\ \{0E\} \bullet \{03\} &= \underline{00010010} \\ & \quad 00000000 \end{aligned}$$

5. Consider the RSA encryption scheme with $n = p \times q$ where p=5 and q=7. Prove that all keys d and e in the range [0,$\phi(n)$-1] must satisfy the quality d=e.

Solution

Recall that e and d are multiplicative inverses modular $\phi(n)$:
$\phi(n) = (p-1)(q-1) = 4 \times 6 = 24$
$e \times d \bmod \phi(n) = 1$
$e \times d \bmod 24 = 1$

Recall that d is chosen in such a way that $\gcd(d, \phi(n)) = 1$. Now $24 = 2^3 \times 3$, thus d can only be one of: 5, 7, 11, 13, 17, 19, 23 and trivially 1. We prove by inspection that d = e in all cases.
$5 \times 5 \bmod 24 = 1$
$7 \times 7 \bmod 24 = 1$
$11 \times 11 \bmod 24 = 1$
$13 \times 13 \bmod 24 = 1$
$17 \times 17 \bmod 24 = 1$
$19 \times 19 \bmod 24 = 1$
$23 \times 23 \bmod 24 = 1$

6. In a public-key system using RSA, you intercept the ciphertext C=9 sent to a user whose public key is e=5, n=35. What is the plaintext M?

Solution

$n = 35 = 5 \times 7$
$\phi(n) = (5-1)(7-1) = 4 \times 6 = 24$
$e \times d \bmod \phi(n) = 1$
$5 \times d \bmod 24 = 1$
Using Euler's theorem, we get $d = 5^{(\phi(24)-1)} \bmod 24 = 5^7 \bmod 24 = 5 \times 5^6 \bmod 24 = 5 \times 25^3 \bmod 24 = 5 \times 1^3 \bmod 24 = 5$. (Otherwise use Euclid's extended algorithm)

So $M = C^d \bmod n = 9^5 \bmod 35 = 9 \times 9^4 \bmod 35 = 9 \times 81^2 \bmod 35 = 9 \times 11^2 \bmod 35 = 9 \times 121 \bmod 35 = 9 \times 16 \bmod 35 = 144 \bmod 35 = 4$.

7. Suppose we have a set of blocks encoded with the RSA algorithm and we do not have the private key. Assume n=$p \times q$, e is the public key. Suppose also that someone tells us they know one of the plaintext blocks has a common factor with n. Does this help us in any way?

Solution:

In general if a and b have a factor in common, then a mod b is also a multiple of that same factor. This is the basic idea underlying the Euclid's algorithm for finding the

Greatest Common Divisor (gcd). If the plaintext M has a common factor with n, then M^e also has the same factor, and so does the ciphertext $C = M^e \bmod n$.

Therefore, the ciphertext has a common factor with n – we just need to find a greatest common divisor $\gcd(C, n)$ of ciphertext C and n and that will be either p or q.

8. Suppose that in a RSA cryptosystem n= 98537 and e=1573. Encipher the message 25776 and break the system by finding d.

Solution:

$C = M^e \bmod N = 25776^{1573} \bmod 98537 = 87893.$
To find d, we need to find multiplicative inverse of e modulo Φ(n).
Φ(98537) = Φ(467*211) = 466*210 = 97860.
Thus 1573d mod 97860 = 1

i	y	u	v	g
0		1	0	97860
1		0	1	1573
2	62	1	-62	334
3	4	-4	249	237
4	1	5	-311	97
5	2	-14	871	43
6	2	33	-2053	11
7	3	-113	7030	10
8	1	146	-9083	1
9	10	-1573	97860	0

d = 97860 – 9083 = 88777