The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260/COMP6360 Data Security

Week 9 Workshop – 3rd and 5th May 2021

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

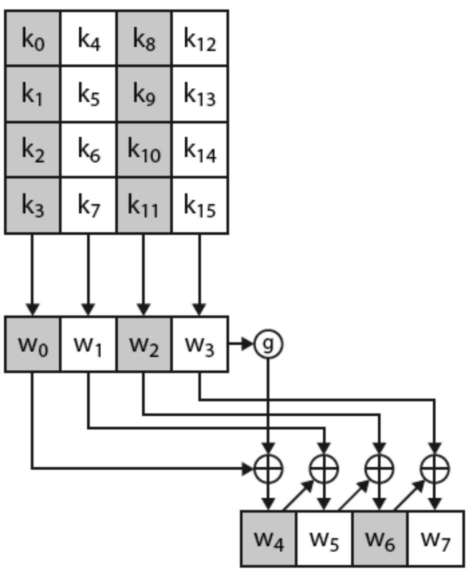
Solution: See text.

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}

3. In the discussion of mixed columns and inverse mixed columns it was stated that
$b(x) = a^{-1}(x) \bmod (x^4+1)$, 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:

We want to show that $d(x) = a(x) \times b(x) \bmod (x^4 + 1) = 1$. 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:

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

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

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

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

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

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

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

4. 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:

It is easy to see that $x^4 \bmod (x^4 + 1) = 1$. This is so because we can write:

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

Recall that the addition operation is XOR. Then,

$$x^8 \bmod (x^4 + 1) = [x^4 \bmod (x^4 + 1)] \times [x^4 \bmod (x^4 + 1)] = 1 \times 1 = 1$$

So, for any positive integer a, $x^{4a} \bmod (x^4 + 1) = 1$. Now consider any integer i of the form $i = 4a + (i \bmod 4)$. Then,

$$x^i \bmod (x^4 + 1) = [(x^{4a}) \times (x^{i \bmod 4})] \bmod (x^4 + 1)$$
$$= [x^{4a} \bmod (x^4 + 1)] \times [x^{i \bmod 4} \bmod (x^4 + 1)] = x^{i \bmod 4}$$

The same result can be demonstrated using long division.

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 = 5×7
$\phi(n)$ = (5-1)(7-1) = 4×6 = 24
$e \times d \bmod \phi(n) = 1$
$5 \times d \bmod 24 = 1$
Using Euler's theorem, we get $d = 5^{(\phi(24)-1)} \bmod 24 = 5^7 \bmod 24 = 5\times5^6 \bmod 24 = 5\times25^3 \bmod 24 = 5\times1^3 \bmod 24 = 5$. (Otherwise use Euclid's extended algorithm)

So $M = C^d \bmod n = 9^5 \bmod 35 = 9\times9^4 \bmod 35 = 9\times81^2 \bmod 35 = 9\times11^2 \bmod 35 = 9\times121 \bmod 35 = 9\times16 \bmod 35 = 144 \bmod 35 = 4$.

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 $\Phi(n)$.
$\Phi(98537) = \Phi(467*211) = 466*210 = 97860$.
Thus $1573d \bmod 97860 = 1$

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

$d = 97860 - 9083 = 88777$