The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260/COMP6360 Data Security

Week 9 Workshop – 3rd and 5th May 2021

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

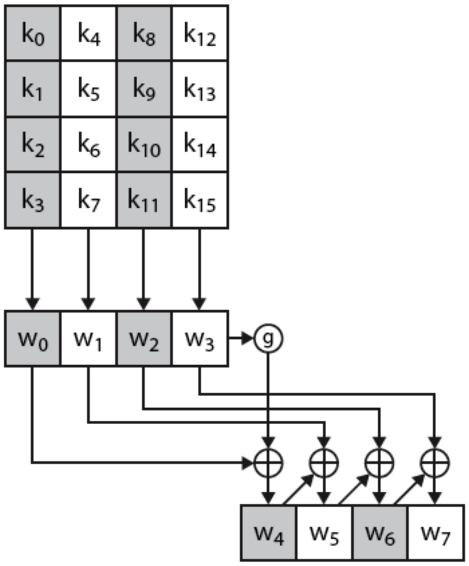
47
37
94
ED

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.

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.

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.)

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 $d=e$.

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?

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?

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