CEN448 – Semester 322 – Homework 3

# Review Questions

1. What is the purpose of the State array?

2. What is the rationale behind SubBytes and ShiftRows?

3. Which parts of AES that are affected by the key length? Explain.

4. What are the block cipher modes that are suitable for transmission over noisy channel? Why?

5. Mention the advantages and disadvantages of CBC mode.

6. How does 3DES maintain backward compatibility with DES?

7. If you have a slow CPU (e.g. embedded system), would you use block cipher or stream cipher? How to ensure that your choice is secure?

# Problems

1. a. Perform SubBytes on the following State array

|  |  |  |  |
| --- | --- | --- | --- |
| 67 | 37 | 24 | FF |
| AE | A5 | C1 | EA |
| F8 | B4 | 0C | 4C |
| E8 | 21 | 97 | BC |

b. Perform ShiftRows on the following State array

|  |  |  |  |
| --- | --- | --- | --- |
| 59 | 86 | 57 | D3 |
| F7 | 92 | C6 | 7A |
| A3 | 52 | 4A | FF |
| 36 | F3 | 93 | DE |

c. Show the output of **second column** of the State array **after** MixColumns when the input State array is

|  |  |  |  |
| --- | --- | --- | --- |
| 41 | 8D | FE | 29 |
| 9A | 36 | 16 | 85 |
| 78 | 87 | E4 | 06 |
| 65 | 9B | FD | 88 |

**Show all steps** or no score will be given.

2. For the AES key 8C16A62518F868634EE4092BA1E24BBA, calculate AES round keys from w0 up to w7. Show the steps.

3. Show by example how stream cipher can be broken if key is reused.