Section 4 Lecture 28 – AES Implementation - Solutions

Q1)

(i) 2^{128}

(ii) There are all the previous keywords with either a 0 or 1 at the end, so twice as many possibilities

(iii) Doubling computer power will mean we can brute force 1 extra bit (twice as many keywords). Therefore to get 128 – 56 = 72 extra bits means we need to double power 72 times, which is 144 years according to Moore's Law. 144 years on from 1998 is the year 2142.

Q2)

(i) Split into bytes the keyword is

10101111 01011110 01110011 10011101 01010000 10100100 10010101 00101010
10101010 11110010 01010010 11101011 01001010 11101010 11001010 10011101

In hexadecimal this is AF 5E 73 9D 50 A4 95 2A AA F2 52 EB 4A EA CA 9D

Hence the initial AES state is the matrix

AF	50	AA	4A
5E	A4	F2	EA
73	95	52	CA
9D	2A	EB	9D

(ii) Just look up the values in the table to get the matrix

79	53	AC	D6
58	49	89	87
8F	2A	00	74
5E	E5	E9	5E

(iii) *ShiftRows* just keeps the first row as it is, shifts the second row left by 1, the third row left by 2 and the fourth row left by 3, to get

79	53	AC	D6
49	89	87	58
00	74	8F	2A
5E	5E	E5	E9

(iv)

First column:

We need to multiply (using our definitions of multiplying and adding)

$$\begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} 79 \\ 49 \\ 00 \\ 5E \end{pmatrix}$$

2 x 79: 79 in binary is 01111001, which shifts as in the definition to give 11110010 (no need to XOR as first bit was 0)
3 x 49: 49 in binary is 01001001, which shifts to give 10010010, then XOR this with the original byte 01001001 to get 11011011
1 x 00: 00 in binary is 00000000 which just stays the same
1 x 5E: 5E in binary is 01011110 which just stays the same

Hence the first element is the XOR of 11110010, 11011011, 00000000, 01011110 which gives 01110111 which is 77 in hexadecimal

Similarly,

1 x 79 = 01111001, 2 x 49 = 10010010, 3 x 00 = 00000000, 1 x 5E = 01011110
XOR gives 10110101 = B5

1 x 79 = 01111001, 1 x 49 = 01001001, 2 x 00 = 00000000, 3 x 5E = 10111010
XOR gives 10001010 = 8A

3 x 79 = 10001011, 1 x 49 = 01001001, 1 x 00 = 00000000, 2 x 5E = 11100100
XOR gives 00100110 = 26

Hence the first column is $\begin{pmatrix} 77 \\ B5 \\ 8A \\ 26 \end{pmatrix}$

Other columns

The other columns follow similarly. Just remember that when multiplying a byte that begins with 1 by 2, you need to shift and then take the XOR with 00011011 (and similarly when you do the first part of multiplying by 3).

For example, to work out the element in the second row and second column, you need:

1 x 53 = 01010011
2 x 89: In binary, 89 is 10001001. Shifting gives 00010010. Since the original byte begins with 1, we need to XOR this with 00011011 to get 00001001

3 x 74 = 10011100
1 x 5E = 01011110

Taking the XOR gives 10011000 = 98

If you complete it all, I believe the answer is this!

77	0C	BB	1D
B5	98	D6	3C
8A	20	56	89
26	44	7A	28

Q3) Open to you!