Year and Semester	2018 FALL
Course Number	CS-336
Course Title	Intro. to Information Assurance
Work Number	HA-04
Work Name	Symmetric Encryption
Work Version	Version 1
Long Date	Sunday, 16 September 2018
Author(s) Name(s)	Zane Durkin

Abstract

In this article I will be going over the steps of AES, and a few review questions from the book [1].

1 AES Shift Cipher

For this section I will encrypt and decrypt "ZANE" using a shift cipher. The shift cipher I will be using is a more common one known as the Cesare Cipher. For this cipher I will shift each letter down the alphabet (and then looping back around at the end) by a set number of characters.
I will be using the number 15 as my key, so the letter A will become the letter 15 characters down the alphabet: P
So with this cipher, "ZANE" becomes: "OPCT".

to decrypt the cipher, simply shift the letters the opposite direction in the alphabet with the same key. so P becomes A.
so "OPCT" will decrypt to "ZANE".

2 AES Round

A single round of AES (Not including the first or last round), have four main steps.

1. The first setup is Substitute Bytes. This step is a substitution steps since it takes the values found in the S-box and substitutes the data values with the S-box values.

2. The second step is Shit Rows. This step is a permutation step since it doesn't require data to be replaces, but rather moved around in the matrix.

3. The third step is Mix Columns. This step is a permutation since it replaces data in the matrix with values that have been shifted (multiplied) from their original values, but data itself has not been substituted for another value.

4. The fourth and final step is Add Round Key. This step is a substitution since it require the use of an external matrix (the key) to exchange the values in the data matrix. Each value in the data matrix is xORed with the corresponding value in the key matrix, and the result is substituted for the original value in the data matrix.

3 AES S-Box

Assuming I have the starting state block:

A1	49	FF	00
56	2C	00	FF
C9	3B	FF	00
3B	51	00	FF

I can run it through the Substitute Bytes set of AES, and swap out the data values with their corresponding value in the S-box. This will look like:

32	3B	16	63
B1	71	63	16
DD	BE	16	63
E2	D1	63	16

4 AES Add Round Key

Assuming I have a Key block as shown:

AA	54	B1	85
00	00	00	00
00	00	00	00
00	00	00	00

I can apply the Add Round Key method to the Data Block from the previous section. To do this I will XOR each box in the key block with the corresponding box in the data box. The output will look as follows:

98	6F	A7	E6
B1	71	63	16
DD	BE	16	63
E2	D1	63	16

5 Review Questions

5.1 Question 20.1

5.2 Question 20.2

5.3 Question 20.3

5.4 Question 20.4

5.5 Question 20.5

5.6 Question 20.6

5.7 Question 20.7

5.8 Question 20.8

5.9 Question 20.9

5.10 Question 20.10

5.11 Question 20.11

5.12 Question 20.12

References

[1] Stallings, W., and Brown, L. *Computer Security Principles and Practice*, 3 ed. Pearson Education, One Lake Street, Upper Saddle River, New Jersy 07458, 7 2014.