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 2
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 [2].

1 AES Shift Cipher [1]

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 [1]

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, p. 645].

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 [2, p. 645].

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 [2, p. 646].

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 [2, p. 646].

3 AES S-Box [1]

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 [2, p. 649]. 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 [1]

Assuming I have a Key block as shown:[1]

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 [2, p. 651]. 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 [2, p. 664]

A symmetric cipher requires a few main ingredients [2, p. 638]:

- plaintext, There must be something that needs to be encrypted.
- Encryption Algorithm, The process which will encrypt the plain text.
- secret key, The key is used in the encryption algorithm to determine which substitutions or transformation are needed.
- Ciphertext, The output of the encryption algorithm after it has accepted the key and plaintext.
- Decryption Algorithm, The reverse of the encryption algorithm.

5.2 Question 20.2 [2, p. 664]

The two basic functions used in encryption algorithms are substitution and transposition [2, p. 639].

5.3 Question 20.3 [2, p. 664]

Only one key is required for two people to communicate via a symmetric cipher. The same key is used for the encryption and decryption process [2, p. 639].

5.4 Question 20.4 [2, p. 664]

Block ciphers and stream ciphers differ by their algorithm, block ciphers encrypt a set amount of bits at a time, while stream ciphers encrypt a continuous stream of bits [2, p. 651].

5.5 Question 20.5 [2, p. 664]

The two general approaches to attacking a cipher are brute forcing, and cryptanalysis [2, p. 639].

5.6 Question 20.6 [2, p. 664]

Some block ciphers use encryption and decryption to enhance the security of the algorithm [2, p. 644].

5.7 Question 20.7 [2, p. 664]

Triple encryption is running the same algorithm three times on the same string, feeding the output of the first encryption into the input of the second and so on [2, p. 644].

5.8 Question 20.8 [2, p. 664]

The middle portion of 3DES is decryption to allow for the decryption of the old single encrypted DES [2, p. 644].

5.9 Question 20.9 [2, p. 664]

Link encryption is used in a network to secure traffic coming from a user to a network relay. Each relay will have it's own encryption for communication to help prevent the tracking of a packet as it moves throughout the network. End-to-End encryption is used to encrypt data from the original send to the intended final receiver, so each relay cannot determine what is in the packet has it is relayed throughout the network [2, p. 661].

5.10 Question 20.10 [2, p. 664]

There are many ways in which two parties can share secret keys [2, p. 663]:

- A key can be selected by the first party, and physically given to the second party
- A key can be selected by a third party and physically given to both the first and second party.
- The two parties could share a new key using an old key to encrypt the message.
- If the two parties have an encrypted connection to a third party, they could share a secret key using the third party as a medium.

5.11 Question 20.11 [2, p. 664]

The difference between a session key and a master key is that a session key is only used for the current session, while a master key is used to share session keys [2, p. 663].

5.12 Question 20.12 [2, p. 664]

A Key Distribution Service (KDS) is used as a third party to generate and transmit session keys between two parties [2, p. 663].

References

[1] Dr. Conte de Leon, D. Intro to information assurance, 2018.

[2] 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.