Year and Semester	2018 FALL
Course Number	CS-336
Course Title	Intro. to Information Assurance
Work Number	HA-03
Work Name	Selected Problems from Textbook: Chapter 02 (Stallings and Brown, 2015)
Work Version	Version 1
Long Date	Sunday, 9 September 2018
Author(s) Name(s)	Zane Durkin

Abstract

In this article I will be going over a few problems from the Textbook [1]. I'll be solving 4 problems from the end of Chapter 02, and I'll being going through review questions 2.1 to 2.13.

1 Problems from the end of Chapter 02

1.1 Problem 1

1.2 Problem 2

1.3 Problem 3

1.4 Problem 4

2 Review questions from Chapter 02

2.1 Problem 2.1

The essential ingredients of a symmetric cipher are:

- Plain Text
- The Encryption Algorithm
- The Secret Key
- The Cipher Text
- The Decryption Algorithm

2.2 Problem 2.2

Only a single key is required for two people to communicate via a symmetric cipher.

2.3 Problem 2.3

The two principal requirements for the secure use of a symmetric encryption are

- The secret key must be shared privately between only the two members before communication.
- The algorithm must be strong enough to not be reversed without the key

2.4 Problem 2.4

The Three approaches to message authentication are:

- The message is sent with a message authentication tag to all machines that need the data. There is one machine on the network that is responsible for authenticating the message using the attached message authentication tag. If there is a problem with the message, the authenticating device will broadcast to all machines that the message was not authenticated.
- For systems that have a heavy load and cannot authenticate each message, they can authenticate on a selective basis. So messages are selected at random to be authenticated.
- Authentication with the program in plaintext. To reduce the resources required to decrypt the program every time. The message could contain an additional authentication tag to be used fro integrity checking whenever needed.

2.5 Problem 2.5

A Message Authentication code is a one way hashing of a message using a secret key that has been shared before hand in a secure fashion. The MAC is attached with the message, and authenticity can be assured by the client by re-hashing the message with the same secret key and then comparing with the MAC.

2.6 Problem 2.6

Figure 2.3 is a diagram of the use of a Message Authentication Code. The figure shows that the message is combined with a key 'K' to produce a MAC. The MAC is then attached to the end of the message and transmitted to the receiver. The receiver then spates the message from the MAC and re-generated the MAC with the message and key. After generating the new MAC, it is compared with the given MAC to verify the message's authenticity.

2.7 Problem 2.7

In order for a hash function to be useful for message authentication it must have the following functions:

- It can be applied to any block size of data.
- It produces a fixed length output
- H(x) is relatively easy to compute for any x.
- It is computationally in feasible to find a value x that will match a given h in H(x)=h
- When H(x)=H(y) is computationally in feasible to not have y=x. (second preimage resistant)
- For any value of x, it is computationally in feasible to find a value y that will match H(x)=H(y). (collision resistant)

2.8 Problem 2.8

The principle ingredients of public-key cryptography are

- Plain text
- Encryption Algorithm
- Public and Private key
- Cipher text
- Decryption Algorithm

2.9 Problem 2.9

Three uses of a public key cryptosystem are:

- Digital Signature. A public key cryptosystem can be used to sign a message to verify that the message came from the person who has the private key.
- Symmetric key Distribution. Public key cryptosystems can be used to confidentially distribute symmetric keys by encrypting the message with the public key, so only the owner of the private key can view the message.
- Encryption of Secret keys. The use of the Private key to encrypt a message can be done. The encrypted message can then be decrypted by the public key pair.

2.10 Problem 2.10

2.11 Problem 2.11

2.12 Problem 2.12

2.13 Problem 2.13

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.