Romel Cabiling

Home

Home > My courses > 121 - ITSP2B > 07 Deep Diving into Cryptography > Lesson Proper for Week 7

Lesson Proper for Week 7

WHAT IS CRYPTOGRAPHY?

The history of cryptography dates back to ancient times when messages were sent between two parties in a secure manner. In the modern age of technology, information security plays a vital role in everyday life, from entering your login information on a Facebook website to just chatting on the WhatsApp messenger platform.

Have you ever wondered whether, while chatting with someone on WhatsApp, the messages you send and receive could be intercepted and read by another person who is not authorized to view them? In the past, WhatsApp did not provide an end-to-end encryption service, which means that, if a malicious user were performing a **Man-in-the-Middle** (MITM) attack or even sniffing the traffic between the victim and the other person, they could see all the messages that were exchanged between the two parties in plain text. Some people think that they have nothing to hide when they send a message across an insecure platform, but what we have to remember is that time-sensitive information may be sent over, whether it's a password, telephone number, email address, residential address, or even something which is private to a user.

With cryptography, organizations are now able to protect their data and their customers' data securely using the appropriate algorithms and technologies. An example of cryptographic technology is the use of a **Virtual Private Network** (VPN) for connecting branch sites together over an unsecure network such as the internet, a remote access VPN for a teleworker employee, or even a field engineer who needs to access the corporate network while not in the office at the time.

Cryptography is the scrambling of data that is to be sent over an unsecure channel. Cryptography focuses on the confidentiality of data in different states: data at rest, data in motion, and data in use.

· **Data at rest:** Data at rest is data that's not in use and resides on a storage device such as a hard drive, CD/DVD ROM, flash/thumb drive, and so on. In this state, the data is dormant and encryption can be applied to ensure it kept private. Even if it's stolen or lost, confidentiality is still maintained.

· **Data in motion:** Data in motion or data in transit is when the data is moving between devices. In this state, it's more vulnerable to cyber-attacks such as MITM and sniffing. Technologies such as a VPN assist by ensuring a secure channel is used to transport the data over the untrusted or unsecure network connection. **The use of Secure Sockets Layer (SSL)/Transport Layer Security (TLS)** can secure data between a user's computer browser and a website.

· **Data in use:** Data is in its most vulnerable state as it is unencrypted and is currently being accessed by a user or multiple users at the same time. Because it's unencrypted, it's exposed to any type of cyber-attack or threat

OBJECTIVES OF CRYPTOGRAPHY

In this section, we'll take a look at the four objectives of cryptography.

1. Confidentiality

It is also referred to as the privacy or secrecy of information. It maintains information and keeps it safe from unauthorized people. This can be attained through various means, such as by physical methods or through mathematical algorithms. Confidentiality in cryptography can be achieved by using scrambled text, cipher text, or encrypted text.

2. Data Integrity

This helps to identify the alteration of data services. Data or information may get altered due to attacks by unauthorized people. This service should make sure that the information received by the receiver has not been altered or changed by any means while the information is in transit. Integrity in cryptography is achieved by using hashing.

3. Authentication

This helps to identify the source of the originator and other fields such as the date and time of creation of the information. This confirms that the receiver of the information is the one who is identified and verified by the sender. Authentication works based on credentials or keys. Only if the credentials match each other will the user who is accessing the file be authorized/allowed to access the information. Authentication can be enabled with the help of pre-shared private and public keys.

4. Non – Repudiation

Non-repudiation is when you provide reassurance that an action has taken place. As a typical example, let's say it's lunchtime and you decide to head out of your office to buy lunch at a nearby restaurant. When you pay for your meal, the cashier issues you a receipt. The receipt usually contains the time, location, items purchased, and the person who received the payment, and so on. The receipt/bill ensures and proves that the transaction took place.

TERMINOLOGIES

During the course of this chapter, we will be using certain terms which you may be a bit unfamiliar with or even heard about. Here, we are going to provide a short list of terms and their meanings:

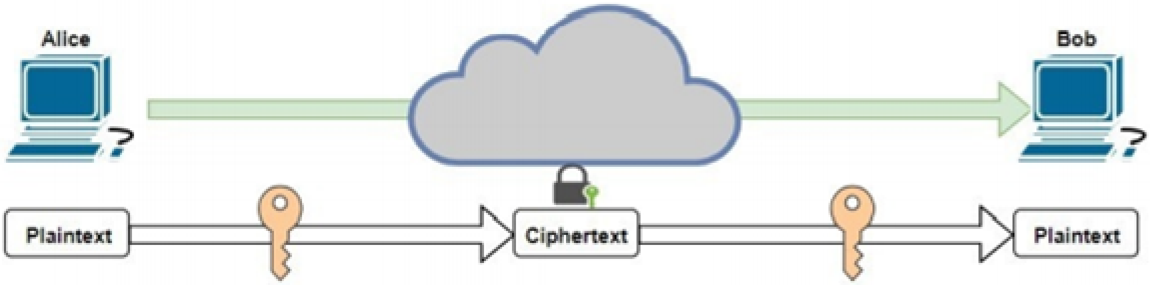
- Message Digest 5 (MD5).
- Secure Hashing Algorithm (SHA).
- Advanced Encryption Standard (AES).
- Data Encryption Standard (DES).
- Triple Data Encryption Standard (3DES).
- Rivest Cipher 4 (RC4).
- Rivest, Shamir, and Adleman (RSA). They are the creators of the RSA encryption technology.
- Virtual Private Network (VPN).
- Secure Sockets Layer (SSL) used to secure data over TCP connections.
- Transport Layer Security (TLS) is the successor to SSL and also secures TCP connections.
- Hypertext Transfer Protocol Secure (HTTP).
- Internet Protocol Security (IPSec).

TYPES OF ENCRYPTION

Here, we will discuss the main differences between symmetric and asymmetric encryption algorithms.

1. Symmetric Encryption

Let's observe the following diagram. There are two devices wanting to exchange a message over an unsecure network such as the internet. Both Bob and Alice are worried that someone in between their machines may be monitoring their traffic and that their privacy is at risk:

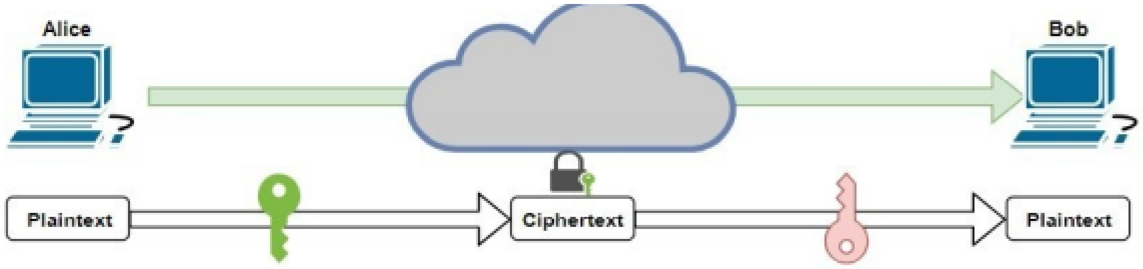


With symmetric encryption, Alice would use a secret key to encrypt or scramble her message for Bob. When Bob receives the Ciphertext (encrypted message), he would use the same secret key as Alice to decrypt the Ciphertext to obtain the actual message.

To describe symmetric encryption simply, this method uses the same key (secret) to encrypt and decrypt a message. If the key is lost or stolen, the message is vulnerable or compromised.

2. Assymetric Encryption

With asymmetric encryption, the main difference is that Alice would use a secret key to encrypt the message before sending it to Bob. When Bob receives the Ciphertext, he would use a different key to decrypt the message and read its contents:



◀ Preliminary Activity for Week 7

Jump to...

Analysis, Application, and Exploration for Week 7 ▶

Navigation

Home
Dashboard
Site pages
My courses
121 - CC106
121 - BPM101 / DM103
121 - OAELEC2
121 - ITE3
121 - MUL101

- 121 - ITSP2B
  - Participants
  - Grades
  - General
  - 01 Exploring Security Threats
  - 02 Delving into Security Toolkits
  - 03 Intrusion Prevention System
  - 04 Understanding Security Policies I
  - 05 Understanding Security Policies II
  - 06 - Preliminary Examination
  - 07 Deep Diving into Cryptography
    - Preliminary Activity for Week 7
    - **Lesson Proper for Week 7**
    - Analysis, Application, and Exploration for Week 7
    - Generalization for Week 7
    - Evaluation for Week 7
    - Assignment for Week 7
  - 08 Deep Diving into Cryptography: Types of Cipher
  - 09 Implementing the AAA Framework
  - 10 Implementing the AAA Framework: Implementing A...
  - 11 Securing the Control and Management Planes
  - 12 - Midterm Examination
  - 13 Protecting Layer 2 Protocols
  - 14 Protecting the Switch Infrastructure
  - 15 Exploring Firewall Technologies I
  - 16 Exploring Firewall Technologies II
  - 17 Cisco ASA
- 121 - WEB101 / CCS3218
- Courses

Fair Warning

NOTICE: Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission***.

PROSECUTION: Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

COURSE OF ACTION: Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

2nd Semester Enrollment

visit www.bcp.edu.ph

Enrollment registration is now Ongoing

For 2nd Semester SY 2021 - 2022

We are accepting new students, returnees and transferees.

"Be trained to be the best,
Be linked to success"

bcp-inquire@bcp.edu.ph

(8)442-8601 | (8)518-8050

Activities

- Assignments
- Forums
- Quizzes
- Resources

Bestlink College of the Philippines
College Department

Powered byeLearning Commons