Lesson Plan

LESSON TITLE: **Module 3: Cryptography**

SUMMARY:

Topic Outline

- Cryptography concepts, theory, and techniques
- Symmetric and asymmetric encryption
- Caesar, Vigenère, and Transposition ciphers
- Public key cryptosystems
- Information Hiding Protocols
- Digital Certificates
- Digital Signatures
- File, Directory, and Email Encryption

GRADE BAND:

☐ K-2
☒ 6-8
☐ 3-5
☒ High School

Time Required:

60 minutes

Lesson Learning Objective/Outcomes: Upon completion of this lesson, students will be able to:

- Understand basic cryptographic concepts, analysis, techniques, and tools;
- Gain familiarization of applied cryptography in cyberspace.

Materials List:

Software tools: GnuGPG4 and DiskCryptor

How will you facilitate the learning?

- Describe the Warm-up Activity/Focused Activity/Closure and/or Reflection
- Describe the Teacher Instruction

We adopt the following best instructional practices and strategies to facilitate learning:

- Multimodal presentation of information
- Cooperative active learning
- Team building
- Periodic checking for understanding

This lesson includes:

☒ Mapping to Cyber Security First Principles
☒ Learning Objectives
☒ Assessments

Mapping to Cyber Security First Principles:

☒ Domain Separation
☒ Abstraction
☐ Process Isolation
☒ Data Hiding
☐ Resource Encapsulation
☐ Layering
☒ Modularity
☒ Simplicity
☒ Least Privilege
☒ Minimization

Assessment of Learning:

TYPE (Examples Listed Below)	NAME/DESCRIPTION
Quiz/Test Presentation Oral Questioning Observation Other Choose an item. Choose an item.	Online pop-quiz/survey using gosoapbox.com will be utilized to check understanding of key indicators. Key Indicators of Understanding • Familiarity with key concepts of cryptography • Recognition of Cyber Security Principle involved • Being able to differentiate Symmetric and asymmetric encryption • Being able to perform basic encryption and decryption • Being able to implement message authentication and confidentiality Hands-on exercises will be conducted to reinforce learning. Participants will be asked to present their observations on pertinent case studies.

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

We provide digital videos with closed captions of software tools and hands-on exercises.

Description of Extension Activity(ies):

Background Materials

Cryptography

Cryptography is the practice and study of techniques for secure communications. It involves the design, implementation, and analysis of protocols that enforces the authentication, confidentiality, non-repudiation, and integrity of information that is transmitted. The earliest forms of message hiding (also known as steganography) dates back to the time when Greeks would send messages that are tattooed on the unshaven heads of messengers. The hair was grown before the messenger was dispatched so as to hide the message. The Roman emperor Julius Caesar was attributed the Caesar cipher which is essentially the alphabet shifted left or right by a constant number of positions. Thus if the alphabet is shifted right by 3 positions, the letter A is written as C, B as D, C as E, and so on. This is called substitution cipher.

Symmetric-key and Asymmetric-key Cryptography

Symmetric-key cryptography is a technique that utilizes the same key for both encryption od plaintext and decryption of cipher text. In essence, a secret key is being shared by both parties to enable secure exchange of information. Examples of this cryptographic technique are the RC4, AES, and DES algorithms.

Asymmetric-key cryptography (also known as public-key cryptography) uses a pair of keys: one public and the other private. The public key is widely known while the private key is held undisclosed by the owner. This pair of keys are complementary, i.e. they can only work together. To enforce the confidentiality of the message, the public key is used to encrypt and only the owner, who holds the secret private key, is the only one who can decrypt the cipher text. For the purpose of non-repudiation, the sender of the message encrypts the message with his/her own private key which is tantamount to digitally signing the message. The only way that the cipher text (the digitally signed message) can be decrypted is by using the owner's public key. Examples of this cryptographic technique are the RSA cryptosystem, the Diffie-Hellmann key exchange, and various elliptic curve systems.

Digital Certificate

A digital certificate is an electronic document used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents. A valid signature and a trusted signer indicate that they key to communicate with its owner is legitimate. In a typical Public-Key Infrastructure (PKI) scheme, the signer is known as a Certificate Authority (CA) which provides the certificate issuing services.

Associated Problem-based Laboratory Exercises:

I. Hands-on Public Key Cryptography with OpenPGP

1. Open Notepad and create a file named **TextFile_ToEncrypt.txt** on the C:\ drive. Write your name and a simple message in the file and save it.
2. Create a new certificate (public and private keys)
    - Start **Kleoptra** on your Desktop. On the menu bar, click on **File →New Certificate.**
    - The **Certificate Creation Wizard** should pop up. Click on **"Create a personal OpenPGP key pair."**
    - Complete the form entries.
    - Click Next. Then click Create Key. Enter a passphrase.
    - Click Finish.
3. Save your public key
    - Right click on the key and click **"Export Certificates."**
    - Save it on your USB drive using the filename format **YourLastname_Public**
4. Save your private key

    Right click on the key and click **"Export Secret Keys."**

    Check "ASCII armor"

Save it on the C: drive using the filename format **YourLastname_Private**

5. Exchange with your partner your USB drives and copy the file that contains the public key
6. Open the file with your partner's public key, copy the entire public key starting at the line
   ----BEGIN PGP PUBLIC KEY BLOCK---
   Up until the line
   ----END PGP PUBLIC KEY BLOCK---
   Go back to the Kleopatra application and click on Clipboard→Certificate import
7. Click on File→Sign/Encrypt Files and find the text file named **TEXTFILE_ToEncrypt.txt**
8. On **"What do you want to do**" select **Encrypt** and the check box **"text output (ASCII armor)"**
9. On **"For whom do you want to encrypt?"** select both certificates (your partner and yours) and click on the **"Add"** button. Click on **Encrypt.**
10. You should see a file named T**EXTFILE_ToEncrypt.txt.asc** on the C:\ drive. Copy that file on the USB drive.
11. Exchange USB drives with your partner and decrypt the encrypted file with Kleopatra.

II. Hands-on encryption of a USB drive using Diskcryptor

1. Launch DiskCryptor
2. Select the USB drive to encrypt, on the right side, you should see "Encrypt" enabled.
3. Click on "Encrypt" and a menu pops up. Click Next, then type in the password for the encryption authentication.
4. Please note, it'll ask you to format drive. Do not format drive. You'll just have to unlock it through DiskCryptor to open it.

III. Hands-on paper and pen encryption using Vignere Cipher

1. Using the Vignere Cipher, encrypt the following phrase:
   I NEVER TEACH MY PUPILS. I ONLY ATTEMPT TO PROVIDE THE CONDITIONS IN WHICH THEY CAN LEARN --Albert Einstein

IV. Hands-on paper and pen encryption using Playfair Cipher

1. Encrypt the following sentence using the ***Playfair Cipher*** and the keyword "forensic."
   "Ask not what your country can do for you, ask what you can do for your country."

Acknowledgements: