Introduction to Cryptography

**Module Description:** This module provides an overview of cryptography. Students will be given an overview at first, such as different encryption methods. Then more details will be provided on symmetric cryptography and asymmetric cryptography, such as DES, AES, RSA. Another micro module talks about cryptographic applications that are widely used in the real world.

**Prerequisite Knowledge:**  Students are expected to understand the introduction to cybersecurity concepts module and know how to do modular arithmetic.

**Length of Completion:** This module includes 3 micro modules. The total length of the module is around 7 hours.

**Level of Instruction:** This module intended for upper division undergraduate students majoring in computer science or computer engineering.

**Learning Setting:** This module is suitable for many forms of delivery: online/in-class/hybrid.

**Lab Environment:** None

**Activity/Lab Tasks:** There will be in-class discussion and an out-of-class written assignment.

**Lab Files that are Needed:** None

# learning outcomes

MODULE learning oUTCOMES

• Students will be able to list the elements of a cryptographic system.

* Students will be able to understand the differences between symmetric and asymmetric algorithms.
* Students will be able to demonstrate which cryptographic techniques are appropriate for a given situation.
* Students will be able to state how cryptography can be used, strengths and weaknesses.
* Students will be able to describe the cryptographic applications, such as message authentication, public key certificates, digital signature.

# module Details

**Instructional Files and Online Resources that are Needed:**

Slides:

Lesson 1: Cryptography Overview (CSP-M2-L1.pptx)

Lesson 2: Symmetric and Asymmetric Cryptography (CSP-M2-L2.pptx)

Lesson 3: Cryptographic Applications (CSP-M2-L3.pptx)

**Assessment:**

Written homework questions (CSP-HW2.docx)

# lessons

**Overview of Lessons:**

Lesson 1: Cryptography Overview

Lesson 2: Symmetric and Asymmetric Cryptography

Lesson 3: Cryptographic Applications

**Lesson 1 Learning Outcomes:**

Upon completion of this lesson:

* Students will be able to list the elements of a cryptographic system.

**Lesson 1 Details:**

**Warm Up:** Ask students how the cryptography being used in our daily life.

**Lesson:**

Topics to be covered in this lesson include:

* Basic concepts of cryptography (encryption, decryption, plaintext, ciphertext, key)
* Different methods of encryption (substitution, Transposition, diffusion, permutation, symmetric encryption, asymmetric encryption, block encryption, stream encryption)

**Active Learning Activity:**

In-class exercise:

After discussing Caesar Cipher, give students an encrypted sentence using Caesar Cipher, then ask students to decrypt it.

**Lesson 2 Learning Outcomes:**

Upon completion of this lesson:

* Students will be able to understand the differences between symmetric and asymmetric algorithms.
* Students will be able to demonstrate which cryptographic techniques are appropriate for a given situation.

**Lesson 2 Details:**

**Warm Up:**

Ask students what is the length of the key in AES (or DES), let them guess the number. Show them an example of the key.

**Lesson:**

Topics to be covered in this lesson include:

* DES, Double DES, Triple DES, AES

**Active Learning Activity:**

Discussion:

What are the advantages and disadvantages of symmetric cryptography and asymmetric cryptography?

**Lesson 3 Learning Outcomes:**

Upon completion of this lesson:

* Students will be able to state how cryptography can be used, strengths and weaknesses.
* Students will be able to describe the cryptographic applications, such as message authentication, public key certificates, digital signature.

**Lesson 3 Details:**

**Warm Up:**

Give students an example of using checksum to validate the integrity of a letter.

**Lesson:**

Topics to be covered in this lesson include:

* Diffie-Hellman, Hash, Message authentication, Digital Signature, Public key certificates, digital envelopes.

**Active Learning Activity:**

Discussion:

What are the advantage and disadvantage of using public key certificates?

In-class activity: (After discussing Diffie-Hellman key exchange)

Ask students to pair with each other (2-person groups). Give students an easy prime number to do the Diffie-Hellman. Then in the group, each person pick a number, do the calculation, share the calculated value with the partner and figure out the secret key by using Diffie-Hellman.

Please attribute Dr. Jim Alves-Foss and Dr. Jia Song, University of Idaho  
  
  
  
Except where otherwise noted, this work is licensed under <https://creativecommons.org/licenses/by-nc-sa/4.0/>  
  
Notwithstanding the non-commercial license terms, non-profit educational institutions are granted a non-exclusive, royalty-free license to adapt and use this material, with attribution.  
  
Creative Commons and the double C in a circle are registered trademarks of Creative commons in the United States and other countries. Third party marks and brands are the property of their respective holders.

Project sponsored by the National Security Agency under grant Number H98230-17-1-0199. The United States Government is authorized to reproduce and distribute reprints notwithstanding any copyright notation herein.