Cryptography

**Module Description:** The intent of this Knowledge Unit is to provide students with an understanding of the concepts cryptography and its uses in in networking.

**Prerequisite Knowledge:**  Students are expected to have a basic understanding of data representations.

**Length of Completion**: 8 lecture/meeting/active learning hours, 8 hours outside of lecture reading/preparation, homework.

**Level of Instruction:** This module intended for advanced 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:** Learning activities involves group discussion and working some sample cryptography problems. More advanced task could include writing code that uses crypto libraries.

**Lab Files that are Needed:** None.

# learning outcomes

MODULE learning oUTCOMES

* Students will be able to describe the basic concepts of cryptography, including substitution and transposition.
* Students will be able to describe the basic concepts of symmetric key cryptography
* Students will be able to explain the structure of DES and AES algorithms.
* Students will be able to describe Double DES and Triple DES.
* Students will be able to describe the encipherment modes ECB, CFB, PCFB, OFB, and CTR.
* Students will be able to describe the basic concepts of asymmetric key cryptography
* Students will be able to explain RSA algorithm and its uses for secure communication and digital signatures.
* Students will be able to explain Diffie Hellman key exchange.
* Students will be able to describe the basic concepts of cryptographic protocols
* Students will be able to explain some shortfalls found in cryptographic protocols.

# module Details

**Interconnection:** This module is not directly interconnected with other modules.

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

* Lesson 1: Lesson\_1\_Cryptography.pptx
* Lesson 2: Lesson\_2\_Cryptography\_Symmetric.pptx
* Lesson 3: Lesson\_3\_Cryptography\_Aymmetric.pptx
* Lesson 4: Lesson\_3\_Prudent\_Engineering.pptx

**Assessment:** This provides a reference of what is included in the assessment guide and a mapping of how the assessment items cover all module and lesson learning outcomes.

# lessons

**Overview of Lessons**

* Lesson 1: Cryptography Overview
* Lesson 2: Symmetric Key Cryptography, DES and AES, Encipherment Modes
* Lesson 3: Asymmetric Key Cryptography, RSA and Diffie Hellman
* Lesson 4: Cryptographic Protocols, Prudent Engineering Practices for Cryptographic Protocols

**Lesson 1: Cryptography Overview**

Lesson 1 Learning Outcomes:

Upon completion of this lesson:

* Students will be able to describe the basic concepts of cryptography, including substitution and transposition.

Lesson 1 Details:

**Warm Up:** Ask the students to define cryptography. Ask how it works. Ask if anyone uses it. (If they say no, ask about https – mention it uses cryptography).

**Active Learning Activity:** Work some sample substitution and transposition ciphers. Can provide some cryptogram puzzles for decipherment.

**Lesson 2: Symmetric Key Cryptography**

Lesson 2 Learning Outcomes:

Upon completion of this lesson:

* Students will be able to describe the basic concepts of symmetric key cryptography
* Students will be able to explain the structure of DES and AES algorithms.
* Students will be able to describe Double DES and Triple DES.

Students will be able to describe the encipherment modes ECB, CFB, PCFB, OFB, and CTR.

Lesson 2 Details:

**Warm Up:** This lesson should take a few lectures. Start with a recall of the previous lesson. Ask the student some questions about the previous material. For first lection discuss uses of cryptography, especially public and private key as introduced in lesson 1.

**Lesson:** The lesson here is based on the PowerPoint slides and is a standard lecture. Allow time for questions and discussion during the lecture.

**Active Learning Activity:** Have students use python pycryptodome library. Note that it is dangerous to use public libraries unless they are certified by NIST cryptographic Validation Program (<https://csrc.nist.gov/projects/cryptographic-module-validation-program>). To date there are not python validated crypto modules.

**Lesson 3: Asymmetric Key Algorithms**

Lesson 3 Learning Outcomes:

Upon completion of this lesson:

* Students will be able to describe the basic concepts of asymmetric key cryptography
* Students will be able to explain RSA algorithm and its uses for secure communication and digital signatures.
* Students will be able to explain Diffie Hellman key exchange.

Lesson 3 Details:

**Warm Up:** This lesson should take a couple of lectures. For the first lecture, ask students about potential short falls in symmetric key algorithms. For later lectures, ask about lessons learned in the previous lecture.

**Lesson:** The lesson here is based on the PowerPoint slides and is a standard lecture. Allow time for questions and discussion during the lecture.

**Active Learning Activity:** Continue experimenting with pycryptodome features.

**Lesson 4: Cryptographic Protocols**

Lesson 4 Learning Outcomes:

Upon completion of this lesson:

* Students will be able to describe the basic concepts of cryptographic protocols
* Students will be able to explain some shortfalls found in cryptographic protocols.

Lesson 4 Details:

**Warm Up:** This lesson should take a couple of lectures. In the first lecture ask students about potential short falls Diffie Hellman key exchange. The idea is to lead to concerns about authenticating Alice and Bob’s identities to each other. Subsequent lectures, talk about lessons learned in the previous lecture.

**Lesson:** The lesson here is based on the PowerPoint slides and is a standard lecture. Allow time for questions and discussion during the lecture.

**Active Learning Activity:** Continue experimenting with pycryptodome features.

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.