# IT 6823 LM 6. Cryptography

# Learning Material

**Note**: The learning material is composed of a list of web links, videos, and other materials screened and/or created by the instructor. The material is organized by student outcomes. Essential information is included in this document and students are recommended to go to the links to learn more about a specific topic.

## Overview

The module covers the principles of cryptography. Topics includes classical cryptography and public key cryptography, and digital signature. There are a lot of concepts and algorithms introduced in the module. You don’t need to know all the mathematics behind the algorithm. Just focus on how those algorithm work and their applications.

Cryptography is a part of Protect phase in the NITS security framework.

## Student Learning Outcomes

* **Define cryptography and its main concepts**
* “The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification”. Source: <https://csrc.nist.gov/glossary/term/cryptography>
* Focus on protecting confidentiality. Can protect integrity too with modern algorithms.
* Cryptography terms plaintext, “encryption, ciphertext, encryption algorithms, encryption key, decryption algorithm. <https://en.wikipedia.org/wiki/Cryptography> Terminology section.
* Two classical cipher types: transposition ciphers and substitution cipher -<https://en.wikipedia.org/wiki/Cryptography> Classic cryptography section.
* Classification of cipher on how the data is processed: stream cipher and block cipher. Need to know the pros and cons of each type. The main difference between Block cipher and Stream cipher is that block cipher converts the plain text into cipher text by taking plain text’s block at a time. While stream cipher converts the plain text into cipher text by taking 1 byte of plain text at a time. Source:

<https://www.geeksforgeeks.org/difference-between-block-cipher-and-stream-cipher/>

* **Describe the Caesar Cipher and Vigenère Cipher**
* Both algorithms focus on confidentiality.
* Caesar Cipher - Focus on the introduction, example, and breaking the cipher section.

Source: <https://en.wikipedia.org/wiki/Caesar_cipher>

* Vigenère Cipher – Focus on the introduction and description section. Source: <https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher>
* **Discuss AES algorithm and its applications**
* Widely used symmetric cipher. Block cipher. For confidentiality.
* Focus on “why AES is the Standard” and “How Strong is AES section”

Source: <https://securityboulevard.com/2020/04/advanced-encryption-standard-aes-what-it-is-and-how-it-works/>

A web service to check encryption and certificates used by a website: <https://www.ssllabs.com/ssltest/>

* **Explain Public Key Cryptography**
* A pair of keys. Asymmetric cryptography. For confidentiality and integrity.
* Need to know how PKC works. The pros and cons of symmetric key and asymmetric system. Introduction and Hybrid Cryptography sections of the source: <https://en.wikipedia.org/wiki/Public-key_cryptography>
* Hash- used for digital signature and integrity. Need to know the basics of cryptographic hash function. The introduction section of the source: <https://en.wikipedia.org/wiki/Cryptographic_hash_function>
* Digital signature. For authentication and integrity. Source: <http://nic.af/en/page/what-we-do/pki/digital-signature> This is a short article. Read it all.
* **Describe the RSA algorithm**
* One of the widely used public key cryptosystem
* Need to know the operation of RSA algorithm. Don’t need to perform the mathematic calculation but should know the steps. Source: [https://en.wikipedia.org/wiki/RSA\_(cryptosystem)](https://en.wikipedia.org/wiki/RSA_%28cryptosystem%29)
* RSA online calculator: <https://www.cs.drexel.edu/~jpopyack/IntroCS/HW/RSAWorksheet.>[html](https://www.cs.drexel.edu/~jpopyack/IntroCS/HW/RSAWorksheet.html)
* **Discuss security through obscurity**

Focus on the “Advantage of secret keys”, “Maintaining security”, and “Security through obscurity” sections of the source:

<https://en.wikipedia.org/wiki/Kerckhoffs%27s_principle#Security_through_obscurity>

* **Explain what’s cryptanalysis and cryptographic attacks.**

Just need to know what those attacks are. Don’t need to know the details.

<https://www.experts-exchange.com/articles/12460/Cryptanalysis-and-Attacks.html>

ciphers