Cryptography Introduction

Any system created to work in today’s environments need to be secure. Not only do these ever increasingly complex systems need to function correctly under extreme conditions, they also need to be protected from malicious attack. Generally, designing and accessing a secure system is difficult. The acronym “CIA” is generally striven for:

**Confidentiality**: data is accessible only to authorized parties

**Integrity**: data is from the party claimed, without modification

**Availability**: authorizedparties can access data when and where needed

The goal of the exercises contained in this learning section is to explain a brief overview of cryptography concepts. One should understand a few techniques and algorithms used in security today after completing these exercises.

As a primer, please view the following video lecture supplied by the microcontroller manufacturer, Microchip. The lecture provides an excellent overview of cryptography and the techniques important to creating reliable security. It is an enormous amount of information at once, and it may benefit to watch multiple times or watch in sections.

[Microchip- Complete Crypto Primer](https://www.dropbox.com/s/ofjk7a7zf93dzu4/00%20-%20Complete%20Crypto%20Primer.mp4?dl=0)

After viewing the video, please review the following:

* What is the “CIA” triad and why is it important in secure systems?
* When should security be considered in the design process of a system?
* What are a few real-world examples when creating a secure system is important?
* When may encryption itself not be necessary?
* What is a hash algorithm?
* What is symmetric encryption/authentication?
* What is asymmetric encryption/authentication?
* What is Diffie Hellman Algorithm?
* What is entropy?