# LM 6. Cryptography

### 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.

### To Do List

* 1. Study the learning material of this module - security frameworks. Use the learning material document and PowerPoint slides as a guide.
  2. Quiz 2 - 10 multiple choice/true false questions from LM5 and LM6. Open book and open notes. One attempt only - must be **completed by xx.**

### Learning Outcomes

After this module, student will be able to:

* Define cryptography and its main concepts
* Describe the Caser cipher and Vigenère cipher
* Discuss AES algorithm and its applications
* Explain Public Key Cryptography
* Describe the RSA algorithm
* Discuss security through obscurity
* Explain what’s cryptanalysis and cryptographic attacks