# ITAS363 Unit 4 Lab

## Introduction

LabSim Security Pro is used to provide a simulated, hands-on laboratory for the purposes of learning about important security concepts. In an online environment it is impossible for students to work directly with security mechanisms in administrative scenarios. Therefore, LabSim is the tool that supports students in their pursuit to understand difficult concepts in an online environment.

Use of LabSim Security Pro requires a one-time registration process. You should have received an activation code from the bookstore (Words of Wisdom). Notify the bookstore immediately if you have not yet received your activation code. Contact them at aiuonlinebooks@wordsofwisdombooks.com.

Instructions for accessing LabSim can be found in the Course Materials section. You can also contact your instructor with any questions. You will have access to Security Pro for 36 months (3 years) from the date of registration.

Note that LabSim Security Pro is aligned with CompTIA’s Security+ certification. CompTIA suggests that individuals pursuing certification in this area have approximately two years of experience in IT administration with Security focus. Completing this lab will not qualify you to complete the exam. One must complete several courses in order to cover all the concepts included in the certification exam. Further, completing the coursework does not conclude with automatic certification. Those students who wish to pursue certification may do so outside the classroom. For those students that qualify, they may contact the Registrar’s office for receipt of a discounted certification voucher honored by CompTIA.

LabSim Security Pro is aligned with (ISC)2 SCCP (Systems Security Certified Practitioner )certification exam. Completing this lab will not qualify you to complete the exam. One must complete several courses in order to cover all the concepts included in the certification exam. Further, completing the coursework does not conclude with automatic certification. Those students who wish to pursue certification may do so outside the classroom.

***Hardware Requirements***: Refer [here](http://www.testout.com/home/support/quick-start-guides/system-requirements) to verify that you meet the necessary Hardware Requirements. Note that you will need speakers.

***Expected Time for Completion*: six and a half (6.5) hours or more depending on time necessary to familiarize yourself with tool**. You may complete the tasks in numerous iterations. You do not need to complete all the lab tasks in one sitting.

## Lab Description

Upon completion, you will:

* Compare and contrast basic concepts of cryptography
* Given a scenario, implement secure systems design
* Compare and contrast types of attacks
* Crack a symmetric encryption key
* Encrypt files with EFS and GPG
* Configure BitLocker with a TPM
* Manage certificates
* Configure a subordinate CA
* Use hashes
* Add SSL to a website
* Allow SSL connections
* Require IPsec for communications
* Install and configure network components, both hardware- and software-based, to support organizational security

## Lab Tasks

Each Module contains numerous Sections. The last section in each Module is a Practice Exam. The Practice Exam is **not** required. Taking the Practice Exam is **optional**. The results of the Practice Exam do **not** impact your course grade one way or the other.

All Module Sections (excluding the last Section – Practice Exam) are required unless otherwise designated.

### Module 2.0 Security Basics

Section 2.4 Cryptography (Review video only: 2.4.1)

### Module 9.0 Data

Section 9.2 Advanced Cryptography

Section 9.3 Cryptography Implementations

Section 9.4 Cryptographic Attacks

Section 9.5 Symmetric Encryption

Section 9.6 Asymmetric Encryption

Section 9.7 File Encryption

Section 9.8 Public Key Infrastructure (PKI)

Section 9.9 Hashing

Section 9.10 Data Transmission Security

Section 9.11 Data Loss Prevention (DLP)

The above Section includes one hands-on activity. Be sure to complete them.