

# WM187-15 Programming for Cyber Security

**25/26**

**Department**

WMG

**Level**

Undergraduate Level 1

**Module leader**

Harjinder Lallie

**Credit value**

15

**Module duration**

30 weeks

**Assessment**

Multiple

**Study location**

University of Warwick main campus, Coventry

---

## Description

### Introductory description

Fluency in the process of software development is a prerequisite to the study of much of the remainder of this programme. In order to use computers to solve cyber security problems effectively, students must be competent at reading and writing programs in multiple programming languages. In addition, they must be able to design and analyse algorithms, select appropriate paradigms, and utilize modern development and testing tools. This module brings together those fundamental concepts and skills related to the software development process. As such, this module provides a foundation for other software-oriented aspects of the programme: programming languages for cyber security, data science for algorithms and complexity in the cyber context, and the cyber context of software engineering. This module focuses on the cyber context of the entire software development process, identifying those concepts and skills that should be mastered in the first year of the programme. This includes the design and simple analysis of algorithms, fundamental programming concepts and data structures, and basic software development methods and tools. A significant feature of the module is the use of group development projects. A single programming language and development environment will be used to exemplify the abstract concepts being developed. There will necessarily be some significant proportion of the module's independent study time being spent gaining familiarity with the language and its associated environment.

## Module aims

To introduce, develop, and affirm fundamental programming knowledge and skills  
Outline and affirm secure coding principles

## Outline syllabus

This is an indicative module outline only to give an indication of the sort of topics that may be covered. Actual sessions held may differ.

### Outline content

Fundamentally this module develops core programming concepts aimed at assisting the learner progress through further modules which requires this key skill.

The language is likely to be Python, but could change depending on the tutor. Learners will be taken through fundamental concepts to being able to design, develop, and test programs.

The content of this module will be taught from a cyber security perspective.

Key topics include but are not limited to:

- algorithms and design
- fundamental programming concepts
- fundamental data structures
- secure software development
- development methods
- Testing strategies

## Learning outcomes

By the end of the module, students should be able to:

- Understand and apply basic programming principles
- Develop a software component that meets a given problem
- Analyse the behaviour of a program in response to various combinations of interesting inputs
- Utilise standard algorithms and data structures in the solution to well defined problems

## Indicative reading list

The Python Book, Rob Mastrodomenico, Wiley, 2022

Practical Python Security, Dennis Byrne, Manning Publications, 2021

Building Python Programs, Reges et al, Pearson, 2019

[View reading list on Talis Aspire](#)

## Subject specific skills

Simple object oriented terminology, including classes, objects, inheritance and methods

Good programming style

Basic programming constructs including sequence, selection and iteration, the use of identifiers, variables and expressions, and a range of data types

Analyse a problem in a systematic manner and model in an object oriented approach

Use simple programming environments to aid the above process

Design a short program, compile the program, debug the program and test the program

## Transferable skills

Problem solving, teamwork, ability to solve problems using a range of sources and techniques

---

## Study

### Study time

Type	Required
Lectures	18 sessions of 1 hour (12%)
Supervised practical classes	18 sessions of 1 hour (12%)
Private study	54 hours (36%)
Assessment	60 hours (40%)
Total	150 hours

### Private study description

Combination of lab continuation work and online study

## Costs

No further costs have been identified for this module.

---

## Assessment

You must pass all assessment components to pass the module.

### Assessment group A

	Weighting	Study time	Eligible for self-certification
Introductory app development	50%	30 hours	Yes (extension)

	<b>Weighting</b>	<b>Study time</b>	<b>Eligible for self-certification</b>
Report on the development of a program which demonstrates the development, testing and reporting of the tool.			
Building a security app	50%	30 hours	Yes (extension)
Build an app/tool which meets specific given requirements which may include a tool that simulates a security feature, a tool that tests a security feature, or other tool			

## **Assessment group R**

	<b>Weighting</b>	<b>Study time</b>	<b>Eligible for self-certification</b>
Building a security app (Resit)	100%		Yes (extension)
Build an app/tool which meets specific given requirements which may include a tool that simulates a security feature, a tool that tests a security feature, or other tool			

## **Feedback on assessment**

Written feedback for each assignment  
 Verbal feedback during tutorial sessions  
 Solutions provided to tutorial questions  
 Summative feedback on assignments

---

## **Availability**

### **Courses**

This module is Core for:

- UWMA-H651 Undergraduate Cyber Security
  - Year 1 of H651 Cyber Security
  - Year 1 of H651 Cyber Security
  - Year 1 of H651 Cyber Security