UNIVERSITY OF GLOUCESTERSHIRE
at Cheltenham and Gloucester

Business School
Cyber and Technical Computing
www.glos.ac.uk

CT5046
Cryptography & Security
Module Guide

2023/24
Semester One
Park Campus Cheltenham

Module Leader | Madhu Khurana
Module Tutor | Madhu Khurana

Table of Content

1. Learning Outcomes

A student passing this module should be able to:

1. Understand and synthesize the essential components and principles of cryptography;
2. Understand the fundamental principles and application of symmetric encryption and cryptographic hashing to provide an improved cyber security posture;
3. Understand the fundamental principles and application of asymmetric and public-key encryption to provide an improved cyber security posture;
4. Understand the application of cryptographic techniques and protocols to protect the transmission and storage of information, provide confidentiality, integrity, protected message exchanges, data origin authentication, entity authentication and non-repudiation;
5. Identify and explain key management, digital signatures, digital certificates and a Public-Key Infrastructure (PKI);
6. Identify and understand the requirements to implement cryptographic applications. Recognise the importance of cryptanalysis and cryptographic backdoors.

2. Prerequisites

Students need to have a good understanding on the basics of computing and as well as Python programming. There is no need for knowledge on cryptography before starting this module.

3. Module Evaluation

3.1. Evaluation for 22/23

The module was well-received by the students. However, the following observations were made:

1. Students struggled to understand the mathematics principles and concepts behind the cryptographic techniques;
2. They were not able to identify the organisational assets in the case study;
3. There was a lack of depth in terms of their understanding of cryptography in their assessments.

3.2. Responses for the Current Year

In order to address the aforementioned issues, the following actions will be undertaken:

1. Provide a two-week session on “Introduction to cryptography”, which covers the fundamental mathematics and number theory together with appropriate examples;
2. Provide post-sessional work consisting of a combination of case studies and technical work, and discuss them at the beginning of each lecture session;
3. Provide relevant reading materials on Moodle to facilitate student understanding.

4. Reading List

a) William Stalling. Cryptography and Network Security: Principles and Practice
b) Nielson, Seth James and Christopher K. Monson. 2019. Practical Cryptography in Python : Learning Correct Cryptography by Example. Berkeley, CA: Apress L.P.
c) Zheng, Zhiyong. 2022. Modern Cryptography. Vol. Volume 1, a Classical Introduction to Informational and Mathematical Principle /. Singapore: Springer.
d) Kraft, James and Lawrence Washington. 2018. An Introduction to Number Theory with Cryptography, Second Edition. First ed. Boca Raton, FL: CRC Press.
e) Holden, Joshua. 2017. The Mathematics of Secrets : Cryptography from Caesar Ciphers to Digital Encryption. Princeton: Princeton University Press.

5. Scheme of Work

Detailed in the table below are the semester week numbers, commencing dates, lecture topics and practical sessions, with the associated lecturer. This is an indicative scheme of work.

Date w/c	Topic	Practical work	Lecturer	CyBok Mapping
Week 1 Week 2	An overview of the module. **Introduction to cryptography:** Principles of cryptography; Cryptography terms and meanings; Confidentiality, integrity, non-repudiation, data origin authentication and entity authentication; A history of cryptography.	Review and analyse a number of case studies on cryptography.	MK	9.2.1
Week 3	**Introduction to cryptography I:** Basic information theory; Essential number theory, algebra and discrete mathematics	Exercises on number theory and classical ciphers	MK	9.4.1 9.4.2 9.4.4
Week 4	**Introduction to cryptography II:** Classical, symmetric and asymmetric encryption techniques and algorithms; Steganography; Cryptanalysis.	Number theory/classical cipher follow-up and encryption exercises	MK	9.4.1 9.4.2 9.4.4
	Symmetric encryption: The purpose and operation of symmetric encryption; Block and stream ciphers; Feistel networks; S-Boxes; Substitution and permutation. Data Encryption Standard (DES); Triple DES (3DES); Advanced Encryption Standard (AES).	Perform symmetric encryption. Investigate cryptanalysis on a number of symmetric encryption algorithms.	MK	19.2.2 19.2.3 19.2.7

Week 5 Week 6	**Symmetric encryption:** Data Encryption Standard (DES); Triple DES (3DES); Advanced Encryption Standard (AES). **Cryptographic hashing:**	Perform symmetric encryption. Investigate cryptanalysis on a number of symmetric encryption algorithms.	MK	9.1.1 9.1.3
	The purpose and operation of cryptographic hashing; Message Authentication Message (MAC); Hashed MACs (HMACs).	Perform cryptographic hashing. Investigate a number of hashing algorithms.	MK	19.2.1 19.2.4 19.2.8
Week 7 Week 8	**Asymmetric encryption:** The purpose and operation of asymmetric encryption; Diffie-Hellman key exchange; Elliptic Curve Cryptography (ECC);	Perform asymmetric encryption. Investigate cryptanalysis on a number of asymmetric encryption algorithms.	MK	9.3.1 9.3.2 9.6.1 9.6.2
Week 9	**Asymmetric encryption:** RSA Public-Key encryption; Key negotiation and distribution; Message exchanges, data origin authentication, entity authentication and the provision for non-repudiation.	Perform asymmetric encryption. Investigate cryptanalysis on a number of asymmetric encryption algorithms.	MK	9.3.1 9.3.2 9.5.1 9.5.2
	Applications of Cryptography I Digital Signatures; Key Management; Key Distribution.	Implementation of digital signatures with key management and distribution	MK	19.2.8 19.3.1 19.3.3
Week 10	**Applications of Cryptography II** The concept and operations of Digital Certificates; Public Key Infrastructure; Data at Rest; Data in Motion; VPN; Tunnelling.	Setting up Client/Server Programs Communication in VPN	MK	19.2.8 19.3.1 19.3.3
Week 11	**Assignment Workshop**		MK	

Week

Assignment submission

12		

6. Assignment

1. Module code and Title:	**CT5046 Cryptography and Security**
2. Module Tutor:	Madhu Khurana
3. Tutor with Responsibility for this Assessment:	Madhu Khurana
4. Assignment:	1: 100% Coursework: Individual, standard written: 2,500 words or equivalent. You will be penalised according to the Academic Regulations for Taught Provision if you exceed the size limit.
5. Submission Deadline:	**Tuesday 12th December 2023** Your attention is drawn to the penalties for late submission; *see Academic Regulations for Taught Provision.*
6. Arrangements for Submission:	Moodle
7. Date and location for return of work:	Written feedback and provisional mark will be within 20 working days.
8. Students with Disabilities:	Alternative assessment arrangements may be made, where appropriate, for disabled students. However, these will only be implemented upon the advice of the disability advisor. Disabled students wishing to be considered for alternative assessment arrangements must give notification of the disability (with evidence) to the Disability Advisor by the published deadlines.
9. University Regulations for Assessment:	All assessments are subject to the **Academic Regulations for Taught Provision**. These include regulations relating to errors of attribution and assessment Offences. In exercising their judgement, examiners may penalise any work here the standard of English, numeracy or presentation adversely affects the quality of the work, or where the work submitted exceeds the published size or time limits, or where the work fails to follow normal academic conventions for acknowledging sources.
10. The Requirements for the Assessment:	Titan Industries, a multinational security and defence organization, operates primarily in the field of AI-powered cybersecurity through its subsidiary, Titan AI. Titan AI's primary functions are research and development, headquartered in New York, with branch offices in Singapore and Cheltenham. The

Singapore office focuses on innovating AI-powered cybersecurity tools and consists predominantly of research personnel. Conversely, the Cheltenham office primarily handles sales and support, serving both local and EU markets and comprising marketing and accounting personnel.

Currently, Titan Industries maintains centralized email and file servers located at the Cheltenham office. The email server stores staff emails, while the file server is used by Cheltenham staff for sales and marketing data storage. Additionally, a dedicated file server serves the Singapore branch office for field trials and research data. All Titan offices are equipped with computers, granting staff access to these file servers. Moreover, wireless access points are available to enable staff to bring their own devices and access these files. Remote access support is also provided for staff working remotely.

Despite accessibility by relevant staff, security audits have recently exposed vulnerabilities in both data-at-rest and data-in-transit encryption. Specifically, data transmitted to and from the offices via wireless access points remain largely unencrypted and susceptible to interception. While classified information on the Singapore server is protected by a web-based login, usernames and passwords, as well as the files on the server, lack encryption.

As a cybersecurity consultant, your task is to recommend and design data protection measures within the organization, including encryption for:

1. Network, email, and internet traffic.
2. Files on the file servers in both the Singapore and Cheltenham offices.
3. Traffic used for remote access to the files.

Your report should include:

1. Definition and explanation of data-at-rest and data-in-transit in the context of this case study.
2. Identification and justification of appropriate encryption techniques and their functionality.
3. A comprehensive assessment of the advantages and disadvantages of the selected encryption techniques.
4. A detailed plan outlining how these encryption methods will be applied to safeguard the identified data categories.

You are allowed to make assumptions in your analysis, but it is essential to clearly outline these assumptions within your report. You should also ensure that your assumptions do not contradict with the original requirements of the assessment.

11. Special Instructions:	None.	
12. Assessment One Criteria:	**Grade**	**Content**
	To achieve <30	Some requirements met, but very limited and not recoverable. Copyright violation.
	To achieve <40	Deliverables partially complete. An inadequate design for safeguarding the data within the company. Inadequate identification and evaluation of how the company can protect all the necessary data at rest and in-transit. An inadequate report structure and layout.
	To achieve 40+	A limited design for safeguarding the data within the company. Limited identification and evaluation of how the company can protect all the necessary data at rest and in-transit. An inadequate report structure and layout.
	To achieve 50+	A partial design for safeguarding the data within the company. Partial identification and evaluation of how the company can protect all the necessary data at rest and in-transit. A reasonable report structure and layout.
	To achieve 60+	Good design for safeguarding the data within the company. Good identification and evaluation of how the company can protect all the necessary data at rest and in-transit. A good report structure and layout.
	To achieve 70+	A very good design for safeguarding the data within the company. Very good identification and evaluation of how the company can protect all the necessary data at rest and in-transit. A very good report structure and layout.