**Mawhiba-Oxmedica**
**Universal Enrichment Program**
**29 June - 18 July 2024**

موهبة

# Pre-Course Student Handout
*for*
# Cybersecurity & Cryptography

Tutor: Mr. Omar Choudhry

Student's Name:

Cover Page Photo: https://www.eenewseurope.com/en/automated-test-system-to-strengthen-post-quantum-cryptography/

This is your pre-course student handout for the **Cybersecurity and Cryptography** summer course – part of a joint program with *Mawhiba* and *Oxmedica*. Some of the information in this document may have or will be shared with you.

# 1 Programme Information

This is the 8th annual collaboration between Mawhiba and Oxmedica, a testament to the exclusivity and prestige of our flagship summer program. Held in the Kingdom of Saudi Arabia since 2016, this year's program boasts a record number of enrolled students, approximately 500 across the male and female programs. As students, you are not just participants, but part of an elite group within the top 1% of aspirational and ambitious high school students. Mawhiba is a programme established by King Saud رحمه الله. Education is a cornerstone of Prince Salman's حفظه الله Vision 2030, and this program is a key part of it. A core ambition of Vision 2030 is to build an independent economy away from the petroleum industry. Part of that is to educate children to grow up to have thriving businesses and careers in wider industries – of which education is an integral foundation.

As part of Oxmedica, we are committed to making a lasting impact on STEM (scientific, technological, engineering, and mathematical) knowledge. We aim to inspire the next generation and offer them a unique experience that will shape their future. We are a global team of experienced academic, research, and career professionals. This will be a high-intensity, bespoke academic program aimed at aspirational high school students spanning an extremely important core STEM discipline – Cybersecurity and Cryptography. You will not only gain theoretical knowledge but also have a series of immersive, impactful and academically rigorous lectures and workshops specially designed to enhance every student's personal character and subject knowledge, setting you up for a successful future in the field.

Through Mawhiba, you will have a teaching assistant who will assist throughout this programme. They will assist with lessons, field trips, and equipment planning. You will also have a residential assistant (between each student group of 8-10 students). They are university students who will help manage logistics such as getting to/from classrooms and restaurants, dealing with accommodation matters, checking in, and any enrichment and weekend activities.

> *"It was absolutely fantastic. I've never learned and had fun at the same time. It was challenging, interesting, and something new." – Oxmedica KSA Student.*

# 2 Tutor Information

Your tutor, Mr Omar Choudhry, is a PhD candidate in the **UKRI CDT AI-Medical** (*Artificial Intelligence for Medical Diagnosis and Care* in the *Centre for Doctoral Training* funded by the *United Kingdom's Research and Innovation* group) programme and recipient of a scholarship, the fully-funded **ESPRC Studentship Award** (*Engineering and Physical Sciences Research Council*). He achieved a **BSc in Computer Science with Artificial Intelligence** (*2020-2023*), winning various prizes throughout his degree.

He is a **student representative** for the UKRI CDT for Artificial Intelligence for Medical Diagnosis and Care, a **postgraduate representative** for students in the *School of Computing* and a **teaching assistant** for all levels of undergraduate computer science students. He serves on the CDT's *Engagement Committee* to help connect the cohorts' research to the wider public, schools, industry and more.

He has industry experience with the United Nations International Computing Centre (UNICC), Discover Financial Services, and Chelsea and Westminster Hospital NHS Foundation Trust. He is the Director of *Handle Academy Ltd* and *OC Solutions Ltd*. He also has *extensive teaching, tutoring, and volunteer experience* in schools and other organisations.

## 2.1 Teaching Pedagogies

We expect you as students, individually and collectively, to be well-mannered and well-behaved, trying your best to do the work to the best of your ability. We expect you to listen when tutors and instructors speak and only speak when instructed. There will be no assigned homework – please maintain a good work/life balance, and there is no need to do extra work outside of the classroom.

Lectures will not be very long unless necessary. There will be many substantial activities – lab work, demonstrations, group discussions, competitions, creative work, debates, workshops and potentially a guest lecture. You are expected to engage in scheduled debates, complete worksheets, pay attention to and make notes to lectures, present in group and individual presentations, and ask questions in question-and-answer sessions. Lessons will always end with key messages and learning points. Regarding classroom management, please be prompt and punctual. Breaks will be provided where necessary.

The focus is on having a clear trajectory and strong motivation from the outset. The goal is not to impart as much theoretical knowledge as possible but on skills, building in practical and applied elements where possible. We aim to inspire, intrigue, and encourage dialogue in one of the most forefront fields in the tech world.

# 3 Cybersecurity and Cryptography Course

## 3.1 Introduction

This course will introduce you to fundamental components of computer science with a particular focus on key tenets of cybersecurity and cryptography. Students will begin by understanding the basic language and architecture of computers, networks, and database systems and will investigate the different possible security threats that computer systems confront. You will consider what value your private data might hold for organisations and how organisations might use this data in nefarious ways without seeking your permission. Students will then look at social engineering techniques cybercriminals use to trick users into giving away their personal data. The course then turns its attention to more common cybercrimes such as hacking, DDoS attacks, and malware and considers methods to protect themselves and our networks against these attacks. You will also learn the basics of cryptography and how to encode and decode using ancient and modern cyphering techniques. Students will undergo regular individual/group-based class exercises to implement their learning in various cyber threat scenarios.

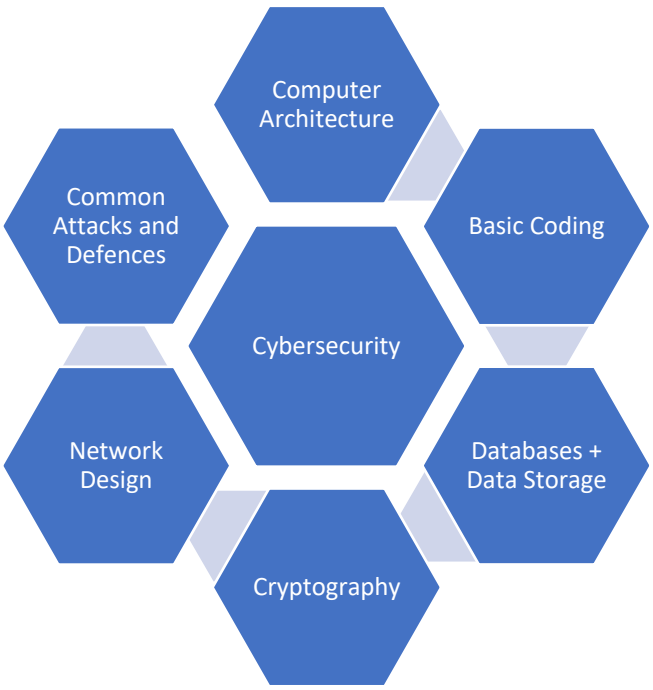
After taking this course, students will be able to:

- Encrypt and decrypt messages using a variety of cyphering techniques
- Describe the basic structure of computer networks and the most common ways in which these networks may be attacked
- Code and debug simple cybersecurity software without assistance
- Understand the role of cybersecurity in business and government
- Project themselves into the day-to-day lifestyle of a cybersecurity professional and have a sense of whether a career in cybersecurity is right for them

This course will approach computer security through a systems thinking lens. Each lesson will build on the previous to construct a complete understanding of how the Internet works and how it can be exploited. Starting with the application level, we will fully understand the systems that support the Internet infrastructure.

## 3.2 Course Trajectory

Cybersecurity is a discipline within computer science that identifies weaknesses and develops defences for systems, networks, and programs against attacks.[1] The primary objective of cybersecurity specialists is to develop technologies into robust systems that protect the user. This course is designed to provide an introduction to the discipline of cybersecurity complimented with a foundational understanding of computing necessary to deeply understand security. The course is structured to first address the components and architecure of computers such as your laptop or mobile phones. Within each class period, we will expand the scope to include another component of a complete system such as the internet. With each topic, the class will utilise an attacker mindset to execute attacks and identify vulnerabilities in technologies in order to create more robust defences.




[1] https://csrc.nist.gov/glossary/term/cybersecurity

The goal of this course is to ignite the student's interest in cybersecurity and increase computational competency. In addition to technical skills, this course will provide greater information about the cybersecurity career pathway which offer highly dynamic and in-demand opportunities.

## 3.3 Assessment

You will be assessed using different methods (note that all assessments are open-book except the first and last).

| *No.* | **Assessment description** | **Weight** | **Week** |
|---|---|---|---|
| *1* | **Case Study Practical:** Given a case study, answer some relevant questions. **Closed-book assessment**. | 5% | 1 |
| *2* | **Coding Practical:** Simple exercises in Python. The main form of assessment is not to see correct answers but rather to observe the students and monitor their effort and focus. **Open-book assessment**. | 5% | 1 |
| *3* | **Architecture Practical:** Pick a component in a computer and explain its role. Describe its inputs and outputs and what it interfaces with. Take a question with some logic gates and describe what it does and a complete truth table. **Open-book assessment**. | 10% | 1 |
| *4* | **Databases Practical:** Design an SQL schema from a list of requirements and perform ER modelling. Question on SQL query. **Open-book assessment**. | 10% | 1 |
| *5* | **Cryptographic Techniques Practical:** A pair activity to encrypt and decrypt a message. This will involve research on the students' side. **Open-book assessment**. | 15% | 1 |
| *6* | **Network Security Concepts Practical:** Describe how the internet works, why we need security and how we implement it. **Open-book assessment**. | 15% | 2 |
| *7* | **Hacking & Cyber Attacks Practical:** The mid-term (end of week 2) test will ask questions about different attacks and potential mitigations. **Open-book assessment**. | 20% | 2 |
| *8* | **Written Assessment:** Open-book assessment This is the final test, but we will keep it at the end of week 2 to make week 3 lighter. **Closed-book assessment**. | 20% | 2 |

You will be given a final detailed student report at the end of the programme.

## 3.4 Pre-Course Preparation

This is the most important part of this document, so please read it carefully. We understand you have limited time before the programme, however, you can always look at these things after the course to continue nurturing your interest in this field.

An important concept in cybersecurity is ***defence in depth***, which is a strategy where layers of independent security controls, people, or technologies are applied to defend an asset against

attack.[2] Foundationally, each layer of defence provides redundancy that can help detect and prevent attacks. Different tools, such as firewalls and anti-virus software, are used at different layers to provide the most effective defences to suite the organisations needs and design specifications.

Traditionally, defence in depth is explained using the metaphor of a medieval castle defending against invasion. Read the Medium article linked below and answer the following questions.

https://medium.com/@rukhsarkhan4198/the-art-of-cybersecurity-mastering-defense-in-depth-1be91a061c90

Alternatively, use the QR Code.link below:

https://bit.ly/OxmedicaCC

1. Detail three levels of protection that exist to defend money in a vault at the bank.

2. What technologies were listed in the article? Rank the technologies from most to least familiar to you.

3. Explain defence in depth using an example from your life.

4. Find an article online that reports on a specific cyber attack. Identify some of the defensive layers at play in the incident. (*Reference Operation Aurora: A Lesson in Layered Defense*)

[2] https://csrc.nist.gov/glossary/term/defense_in_depth

## 3.5 Further Preparation

One helpful resource is a YouTube playlist I created (the link is in Google Docs, which you can access with the QR Code or the link on the previous page) containing a list of YouTube videos related to this field. Some are technical and will teach you concepts, while others are story-based and will expose you to this vast field's history.

**Then try to watch online tutorials on YouTube or search for articles on Google online on how to use specific software**. Play around with these and think about why these tools exist and how exactly they are useful:

- **Wireshark** (https://www.wireshark.org/)
- **Cisco Packet Tracer** (https://www.packettracernetwork.com/download/download-packet-tracer.html)

In the second week, we will hopefully dissect a real computer إن شاء الله to physically understand how a computer is put together and what the different components do. It is a good idea to **start looking at the different computer parts**—search on Google or watch different YouTube videos (e.g., Linus Tech Tips: https://www.youtube.com/@LinusTechTips). You can also go online to a website like https://pcpartpicker.com/ to see what kinds of components exist and are the latest in the market.

Also, try **downloading some software** before we begin on your own computers (we will be going through **Codecademy's Python course** throughout this program (https://www.codecademy.com/learn/learn-python-3) – if you are able to get ahead, you will really be able to benefit more and take much advantage of the course). Use the links below or search on Google:

- **Google Chrome** (https://www.google.com/intl/en_uk/chrome/dr/download/)
- **Python 3.12.3** (https://www.python.org/downloads/)
- **pip** (package manager for Python may already be included, so check this) (https://www.liquidweb.com/kb/install-pip-windows/)
- **VSCode** (https://code.visualstudio.com/download)

Some of the core topics we will cover are as follows (I have provided some recommendations on what you could do – remember, this is just a potential set of things you could do to get the most out of the experience; it is not by any means required, rather simply encouraged):

- **Course Introduction** (for this, prepare by thinking about and writing goals for the next 1-, 5- and 10 years, including plans for future studies and employment).
- **Career Paths in Cybersecurity** (for this, look online at different jobs which exist in the industry. Look at what is required as part of the job descriptions and what you could do to achieve those things, e.g. a BSc degree in a computer science-related field).
- **Critical Cybersecurity Studies** (browse YouTube for different cyber attack and crime videos).
- **Architecture of Computers** (for this, look at some YouTube videos covering truth tables and Boolean logic).
- **Database Systems** (for this, take a look at the https://www.drawio.com/ website. Search for different "ER diagrams" or "UML diagrams" on Google and attempt to recreate them).

- **Cryptographic Techniques** (for this, you could look at YouTube videos for "encryption" and "decryption". It is quite mathematical, and we will cover this in detail).
- **Network Security Concepts** (for this, look at videos on YouTube on "TCP/IP" and "TLS")
- **Hacking and Cyber Attacks** (for this, try to create a mind map of as many cyber attacks, malware, and viruses online as possible and try to connect them – be creative, don't try to make it perfect).
- **Machine Learning** (this is a specialist topic, which will be mentioned later. If you are interested, go through the Machine Learning Specialisation course by Andrew Ng from DeepLearning.AI on YouTube: https://www.youtube.com/playlist?list=PLkDaE6sCZn6FNC6YRfRQc_FbeQrF8BwGI).

There are some extra resources you can look at:

- HackTheBox: https://www.hackthebox.com/
- CompTIA Security+ Essential Textbook: https://books.google.co.uk/books?id=veXvEAAAQBAJ
- Meta Purple Llama: https://llama.meta.com/purple-llama/
- Andress, J. (2019). Foundations of information security: a straightforward introduction. No Starch Press. , Supplementary Textbook
- Anderson, R. (2020). Security engineering: a guide to building dependable distributed systems. John Wiley & Sons. , Supplementary Textbook

## 3.6 STEM Final Group Project

You will work for roughly 75 minutes daily on a final project of about 4 or 5 students. You will be paired up with students from the Mechanical Engineering course.

You will be designing a **secure, sustainable power grid**. This project will involve two core aspects: designing a sustainable power grid using renewable energy sources and a relevant, robust cybersecurity framework. The cybersecurity aspect will consider secure communication channels, encryption of data transmissions, and authentication protocols for grid access and control. The engineering aspect will focus on creating a sustainable energy source that could be developed within the Kingdom of Saudi Arabia. It will consider the process of collecting, storing, and converting energy to electricity, but mainly transportation of the energy, thinking about the required physical infrastructure.

Certain aspects need to be considered, such as what happens in the case of an actual attack and what fail-safes are in place, energy-specific issues such as solar only working during clear day-time or safety and economic challenges for nuclear power plants, geographical locations, challenges with integration into any existing electrical grid and political challenges. Also, evaluate if a distributed power grid is better than a single large power plant (a grid generally has more redundancy, but the probability of a successful attack increases due to the increased connections in the notebooks and with a larger number of physical locations). This project will hopefully be interesting for the students as it combines both disciplines in an extremely relevant field, constituting various principles and ideas from both courses.

The main deliverables and forms of assessment will be a 4-page report (50%, based on application of technical knowledge, relevance to the real world, novelty and innovation, organisation, and clarity), a set of slides (25%, based on clarity, conciseness, use of media and

diagrams), and the physical presentation (25%, based on delivery and communication skills, time management, and answering questions).

Remember that the final product must have a strong oral component with visual aids (pitch, proposal, presentation, …) with a maximum time limit of 10 minutes per group. We will have combined in-class group project presentations on **16 July,** and then the best groups from all courses (just 1 group for our course) will showcase their projects on **17 July**.

The timeline looks as follows:

- Class 1: Project brief + brainstorming
- Class 2: Research
- Class 3: Research
- Class 4: Research
- Class 5: Consolidation
- Class 6: Deck prep
- Class 7: Deck prep
- Class 8: Deck prep
- Class 9: Practice rounds 1
- Class 10: Incorporation of feedback
- Class 11: Practice rounds 2
- Class 12: Final edits

### 3.7 Specialist Topics

You will have the opportunity to benefit from some of my specialisms in this course in the final week of the programme. As mentioned in my tutor information, my key areas are within artificial intelligence.

Machine learning and the whole artificial intelligence field are so important that it is integral to teach students what this is and how it works so that it isn't just a mystery. The applications are endless, and we will make sure to show how we can apply ML and AI to cybersecurity and cryptography with practical examples.

Given that only 9 hours of course time is available to teach these topics, the goal would be to equip students with the most practical knowledge and develop their skills within this limited time. Even though there are many, it is essential to discuss aspects of each so that students are aware of what exists in the real world and what is used in industry.

## 4 Other Information

### 4.1 MBA/Tech Summit

In addition to academic learning, you will also have an opportunity to attend an MBA Bootcamp and Tech Summit. The Tech Summit addresses the foremost relevant tech themes today: AI, disruptive technologies, ethics and policy-making, impact on sustainability, and maximum exposure to crucial tech issues and innovations in diverse fields.

The MBA Bootcamp focuses on turning scientific discoveries into useful technologies, mastering interconnected fields, and identifying critical problems that need to be solved. It will also focus on utilising key themes from leading MBA programs (e.g., the Harvard MBA case method), varied topics, and quick acquisition and understanding of key business concepts.

As your tutor, I will deliver a talk at the Tech Summit, "*A New Age Of Fabrication*". I will hope to cover 3 main topics: *Fake News* (how AI algorithms can generate realistic but entirely

fabricated news articles and videos, influencing public opinion and potentially swaying elections), *Social Media Echo Chambers* (amplification of misinformation and creating polarised communities) and *Deepfakes* (from explicit content to professional theft sand falsified religious verdicts).

The MBA Bootcamp will be on **Saturday, July 6**, during Week 1, and the Tech Summit on **Saturday, July 13**, during Week 2.

## 4.2 Schedule

We have approximately 11.5 days of teaching. We will also have specific days for an MBA Bootcamp, a Tech Summit, a Field Trip Excursion, and Final Presentations. Within these teaching days, we will have approximately 30 hours to teach the core cybersecurity and cryptography topics and 9 hours to teach the specialist topics.

| | |
|---|---|
| 29 June | Set-up and student orientation |
| 30 June | First day of classes |
| 16 July | Final day of classes and project presentations |
| 17 July | Best projects showcase, course Open Day & certificates. |
| 18 July | Closing ceremony |

| | | |
|---|---|---|
| 07:15 | Breakfast | 60 mins |
| 08:30 | STEM | 2 hours |
| 10:30 | Break | 30 mins |
| 11:00 | STEM | 60 mins |
| 12:00 | Prayer | 15 mins |
| 12:15 | STEM | 30 mins |
| 12:45 | Lunch | 90 mins |
| 14:15 | Group project | 75 mins |
| 15:30 | Prayer | 15 mins |
| 18:00 | Phone and relaxation time | 90 mins |
| 19:30 | Dinner | 60 mins |

**This concludes the pre-course student handout for the Cybersecurity & Cryptography course.**