Lesson Plan for: Cybersecurity & Cryptography

Tutor: Omar Choudhry Tutor's Email: O.Choudhry@leeds.ac.uk

Colour codes: Assessment, Lectures, Practicals/Debates/Discussions/Workshops

Lesson Date	Learning Objectives				
	Course topic (according to course outline)	**Type of class (e.g. format, specific skills taught)**	**Description of class (e.g. sub-topics, key questions)**	**Location**	**Time**
WEEK 1 30 June Sunday	a) Course Introduction		Students should begin by writing down answers to a few basic questions, such as goals for the next 1-, 5- and 10 years, including plans for future studies and employment.	Computer Lab	8:30-9:00
	b) Career Paths in Cybersecurity	Lecture	Begin by potentially instilling additional motivation in students. I would discuss certifications, courses, competitions and potential jobs and salaries. This should be in the first lecture (immediately following my introduction to students).	Computer Lab	9:00:9:15
	c) Career Paths in Cybersecurity	Practical activity + Q&A	Give students an opportunity to refine their original goals and read them out. Use this time for a question-and-answer session, too.	Computer Lab	9:15-9:30
	d) Critical Cybersecurity Case Studies	Lecture	This is to provide additional motivation and to refer back to it as we teach future core topics. This way, students will clearly understand that the theory they are learning is entirely applicable in practice and potentially give some	Computer Lab	9:30-10:00

			excitement at the beginning (I mean, how does the US Pentagon get hacked?…). As a side point, the rest of this lecture can be used to discuss some bases around security, hackers and threats and perhaps authentication (including entropy, physical tokens, two-factor authentication (2FA) and biometrics).		
	e) Assessment	Critical Cybersecurity Case Studies Assessment	Given a case study, answer some relevant questions. **Closed-book assessment worth 5%.**	Computer Lab	10:00-10:15
	f) Basic Coding	Coding Lab: IDE Setup	Get students to set up the VSCode IDE on their devices/computers with Python, pip, and relevant packages. If there are issues, focus on setting up with Google Colab.	Computer Lab	10:15-10:30
	g) Basic Coding	Coding Lab: Learn Python	Begin going through Codecademy. Students who did not manage to set up in the previous session can do so now.	Computer Lab	11:00-11:45
	h) Assessment	Basic Coding Assessment	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 worth 5%.**	Computer Lab	11:45-12:00
	i) Specialist Topic: Advanced Coding	Coding Lab: Version Control	Half an hour to introduce and use version control. Students would make *GitHub* accounts, create repositories using the IDE, attempt to create branches, make commits, and perform push and pull requests. All students could use this repository to store all	Computer Lab	12:15-12:45

			their previous work and future work from this point on. Though this is a specialist topic, it will be useful to have this done early on to help with the rest of the course.		
1 July Monday	a) Architecture of Computers	Architecture of Computers Workshop	Discussing computer architecture (*Boolean logic*, *truth tables*, *number systems*, *memory*, *operating systems*, *CPUs*, *GPUs*). We will provide some assembly code examples and show buffer overflow in action. There will be a supplied worksheet (a Python interactive workbook) they will be able to complete throughout this 2 hour session (providing an exact breakdown may not be feasible here).	Computer Lab	8:30-10:30
	b) Architecture of Computers	Practical Lab: Dissecting a PC	Show students how real computers are built from beginning to end, including how to install an operating system. We will not actually build the computer – instead, we will focus on removing certain components and showing its insides.	Computer Lab	11:00-12:00
	c) Assessment	Architecture of Computers Assessment	Pick a computer component and explain its role. Describe its inputs and outputs and what it interfaces with. Take a question with some logic gates and describe what they do, as well as a complete truth table. **Open-book assessment worth 10%.**	Computer Lab	12:15-12:45
2 July Tuesday	a) Database Systems	Practical Database Systems Workshop	We will go over database systems (*database architecture, relational algebra, ER modelling, normalisation,* and *database design*). To	Computer Lab	8:30-10:00

			supplement this workshop, we will use online modelling software.		
	b) Database Systems	Lecture: The Data in Database	Discussions on *big data*, *database management systems*, maintaining *data privacy regulations*, and *visualising*.	Computer Lab	10:00-10:15
	c) Database Systems	Lecture: Data Ethics and Case Studies	We will discuss ethics and look at cyber case studies.	Computer Lab	10:15-10:30
	d) Database Systems	Practical SQL Lab	We will examine relational data in SQL, learn how to exploit vulnerabilities, perform SQL injections, and supplement this with exercises in SQL and Python.	Computer Lab	11:00-12:00
	e) Assessment	Database Systems Assessment	Design an SQL schema from a list of requirements and perform ER modelling. Question on SQL query. **Open-book assessment worth 10%.**	Computer Lab	12:15-12:45
3 July Wednesday	a) Cryptographic Techniques	Lecture: Introduction to Cryptographic Techniques	Introduction to this area. This would give an overview of what happens in the entire encryption/decryption process. We will mention public and private cryptography.	Computer Lab	8:30-9:00
	b) Cryptographic Techniques	Lecture: Encryption	Explain how we perform encryption and different forms of encryption.	Computer Lab	9:00-9:30
	c) Cryptographic Techniques	Practical Encryption Lab	Showing how we can actually **encrypt** a message **mathematically**.	Computer Lab	9:30-10:00
	d) Cryptographic Techniques	Practical Encryption Lab	Showing how we can actually **encrypt** a message in **Python**.	Computer Lab	10:00-10:30
	e) Cryptographic Techniques	Lecture: Decryption	Explain how we perform decryption and then discuss issues regarding different cryptographic techniques.	Computer Lab	11:00-11:30

	f) Cryptographic Techniques	Practical Decryption Lab	Showing how we can actually **decrypt** a message **mathematically**,	Computer Lab	11:30-12:00
	g) Cryptographic Techniques	Practical Decryption Lab	Showing how we can actually **decrypt** a message in **Python**,	Computer Lab	12:15-12:45
4 July Thursday	a) Cryptographic Techniques	Advanced Cryptography Workshop	We will discuss *symmetric cyphers*, the *RSA algorithm*, *advanced encryption standards* (AES), *electronic code books* (ECB), and issues with *randomness*. An interactive Python notebook will supplement this to discuss and play around with the aforementioned concepts.	Computer Lab	8:30-9:30
	b) Assessment	Cryptographic Techniques Assessment	A pair activity to encrypt and decrypt a message. This will involve research on the students' side. **Open-book assessment worth 15%.**	Computer Lab	9:30-10:30
	c) Basic Coding	Practical Coding Lab	Working through Codecademy to finish off the week.	Computer Lab	11:00-12:00
	d) Basic Coding	Practical Coding Lab	Continue working through Codecademy.	Computer Lab	12:15-12:45
	e) Week 1 survey			Computer Lab	12:30-12:45
WEEK 2 7 July Sunday	a) Network Security Concepts	Lecture: Introduction to Network Security	One of the most important topics. Introduction to the Internet infrastructure and network architecture.	Computer Lab	8:30-9:00
	b) Network Security Concepts	Practical: Design Practical	Students should design a theoretical system interacting with the internet and research potential vulnerabilities.	Computer Lab	9:00-9:15
	c) Network Security Concepts	Lecture: Network Security Concepts	Discuss *TCP/IP networking threats* and *architecture*, *network defences (TLS and firewalls)* and *packet filtering*.	Computer Lab	9:15-10:00

	d) Network Security Concepts	Practical: Identifying and Mitigating Vulnerabilities	Analyse your designed system in the previous practical and identify the vulnerabilities. Research ways to fix the problems online. Prepare a lightning talk to present.	Computer Lab	10:00-10:30
	e) Network Security Concepts	Group Discussion	Lightning talks of all students.	Computer Lab	11:00-12:00
	f) Network Security Concepts	Lecture: Network Security Concepts Continued	Continue discussing network security concepts. Focus on *defence against man-in-the-middle attacks, firewalls* and *domain name systems (DNS)*.	Computer Lab	12:15-12:45
8 July Monday	a) Basic Coding	Practical Coding Lab	Working through Codecademy to begin the day and week.	Computer Lab	8:30-9:30
	b) Network Security Concepts	Practical Wireshark Lab	Look at how we can use the Wireshark software tool.	Computer Lab	9:30-10:00
	c) Network Security Concepts	Practical Cisco Packet Tracer Lab	Look at how we can use the Cisco Packet Tracer software tool.	Computer Lab	10:00-10:30
	d) Cybersecurity Legislation and Regulation	Lecture: Cybersecurity Legislation and Regulation	Based on all the information we have covered so far, we should discuss legislation and regulations (including those in Saudi Arabia, the United Kingdom, the United States, and the EU).	Computer Lab	11:00-11:30
	e) Cybersecurity Legislation and Regulation	Group Debate	Allow students to choose from a list of questions. Then, divide them into two groups, each arguing its own side.	Computer Lab	11:30-12:00
	f) Assessment	Network Security Concepts Assessment	Describe how the internet works, why we need security and how we implement it. **Open-book assessment worth 15%.**	Computer Lab	12:15-12:45

9 July Tuesday	a) Cyber Attacks	Lecture: Cyber Attacks	Many core topics revolve around attacks. We would combine this all under *Hacking and Cyber Attacks*, initially beginning with an introduction, followed by analysing case studies for **Brute Force Attacks** and **DDoS Attacks.**	Computer Lab	8:30-9:00
	b) Cyber Attacks	Practical Brute Force Lab	Look at how we can actually perform brute force attacks using Python.	Computer Lab	9:00-10:00
	b) Cyber Attacks	Lecture: Buffer Overflows	This lecture will cover **Buffer Overflows** and issues faced with memory. There will be a short reminder about **SQL injections**.	Computer Lab	10:00-10:30
	c) Cyber Attacks	Research DDoS Lab	Reseach task to find an example of a DDoS attack, how it occurred and why, consequences and following preventative/safeguarding measures. Students to work in groups and present at the end of the session.	Computer Lab	11:00-12:00
	d) Cyber Attacks	Practical Buffer Overflow Lab	Practical activity investigating buffer overflows in the C programming language and how it can be avoided.	Computer Lab	12:15-12:45
10 July Wednesday	**Field Trip**	**See the STEM Field Trip Proposal below.**			**All Day**
11 July Thursday	a) Malware and Viruses	Lecture: Malware and Viruses	This is similar to the previous area but involves much more detail. Thus, I suggest more time dedicated to this. Malware discussed would be **logic bombs, backdoors, viruses, supply chain tracks, Trojan horses** and **worms**.	Computer Lab	8:30-9:00

			This would also include methods to prevent malware and viruses, such as **anti-viruses, command injections** and **input validation**.		
	b) Malware and Viruses	Research Malware Lab	This will be a practical lab with research-task-based exercises focusing on implementing the theory learnt in the malware and viruses session. It will be similar to the DDoS lab, but this time, it will focus on malware and viruses.	Computer Lab	9:00-9:30
	c) Threat-Vectors and Threat Agents	Lecture: Threat-Vectors and Threat Agents	Vector-based threats involve **Cross-Site Scripting, Insider Threats, and Social Engineering**. Agent-based threats involve **Hacktivists, Script Kiddies, Cyber Crime Gangs,** and **Black-and-White Hat Hackers.**	Computer Lab	9:30-10:00
	d) Threat-Vectors and Threat Agents	Practical Hacking Lab	Practical lab with exercises focusing on implementing the theory learnt in the threat-vectors session.	Computer Lab	10:00-10:30
	e) Assessment	Written Assessment	There will be one question on each previous major topic. We will not include hacking or cyber-attacks here, as this will be in the following assessment. The decision to move this written assessment to week 2 was due to the potential lack of time marking. This closed-book assessment is **worth 20%.**	Computer Lab	11:00-12:00
	f) Assessment	Hacking and Cyber Attacks Assessment	The mid-term (end of week 2) test will ask questions about different attacks and potential mitigations. **Open-book assessment worth 20%.**	Computer Lab	12:15-12:45

WEEK 3 14 July Sunday	a) Specialist Topics	Lecture: Introducing Specialist Topics	**Advanced Coding:** Integrated development environments, multiple programming languages, procedural programming, object-oriented programming, web development, coding libraries and packages, version control. **Data Science and Artificial Intelligence (AI):** (data processing, data visualisation, machine learning, deep learning). Essentially, it is a crash course that gives a strong foundation in this field of computer science. 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 show how we can apply ML and AI to cybersecurity and cryptography.	Computer Lab	8:30-8:45
	b) Specialist Topics: Advanced Coding	Lecture: Multiple Programming Languages	Explain different programming languages, their uses and the best places to learn them. This would include *C* for briefly explaining procedural programming and *C++* for object-oriented programming.	Computer Lab	8:45-9:15
	c) Specialist Topics: Advanced Coding	Lecture: Web Development	I would touch on web development (*HTML*, *CSS* and *JavaScript*) and the different libraries and packages used (with examples in *React*).	Computer Lab	9:15-9:45
	d) Specialist Topics: Data Science	Practical Data Processing Lab	A crash course on data processing, learning about collecting data online, using existing	Computer Lab	9:45-10:30

			datasets, types of data, and issues with data, with a final focus on data cleaning and manipulation with practical exercises. All of this will be supplemented with the Python programming language. We will focus on datasets we can use for data visualisation and ML.		
	e) Specialist Topics: Data Science	Practical Data Visualisation Lab	This is another crash course on data visualisation. I will discuss different visualisation libraries in Python and methods of understanding how to use them. We will focus on data visualisation methods using datasets they collected in the previous crash course on data processing. We will learn how to create nice visualisations and components of plots and graphs.	Computer Lab	11:00-12:00
	f) Specialist Topics: AI – Machine Learning	Lecture: Machine Learning	As this field is vast, the main focus will be to introduce Machine Learning (ML) and actually understand this domain. There will be a discussion of loss functions and how we develop, train, test, and evaluate ML models. I would provide students with excellent resources they can use to continue learning about this field.	Computer Lab	12:15-12:45
15 July Monday	a) Specialist Topics: AI – Machine Learning	Practical Machine Learning Lab	We will focus on some basic fundamentals and then examine different Python models with practical examples. Models will include *linear regression, lasso regression*, and *decision trees* (including *random forest models*). We will also	Computer Lab	8:30-10:30

			consider applying ML models to the data we worked on in the Data Section labs.		
	b) Specialist Topics: AI – Deep Learning	Practical Deep Learning Lab	A deep learning (DL) crash course. Like the previous ML course, we will operate similarly in the approach. The main focus will be *neural networks* and using *backpropagation* and *gradient descent*. We will look at practical examples using the *MNST* dataset to classify hand-written numbers.	Computer Lab	11:00-12:00
	c) Specialist Topics: AI – Deep Learning	Practical Deep Learning Lab	Continuing DL course. We will introduce more models, such as *transformers* (how models like *ChatGPT* work) and *convolution neural networks* (for operating on images with a practical exercise on image segmentation). We will conclude by presenting DL applications within the cryptography and cybersecurity field.	Computer Lab	12:15-12:45
16 July Tuesday (half day)	a) Specialist Topic: AI – Deep Learning	Practical Deep Learning Lab + Q&A	The actual final 90 minutes will be kept for extension activities and as a buffer in case circumstances lead to the planned classes not being completed. I would expect this set of topics to be interesting for the students, so it should be more interactive and have more questions and answers from students.	Computer Lab	8:30-10:15
	b) Final survey			Computer Lab	10:15-10:30

STEM group project: 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 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 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).

STEM Field trip proposal: 1. **Mishkat Interactive Centre**: This centre raises awareness of renewable energy sciences, which makes it a perfect option for inspiring students to do their group projects. They offer various programs we could do: The Wind Challenge (45 minutes), Inventor Zone (30 minutes) and Robotics Lab (45 minutes). 2. **Cybersecurity Firms**: The idea would be to visit a cybersecurity firm. The interest is clear - to give students a more practical experience and insight into the real world. If the company is happy to host for a longer time, including a tour, talks and a Q&A. This could take up to 2 hours in total. For both field trips, up to 1 hour would be spent on the transportation (there and back). This would leave 30 minutes to split between the introduction and debrief.

Mishkat Interactive Centre: https://maps.app.goo.gl/Nu1soQp8twR4GRWu8 (Maps), https://en.mishkat.org.sa/programs/ (Website)

Cybersecurity Forms:

1. **Wattlecorp Cybersecurity Labs**: https://maps.app.goo.gl/CYXStq1B1WaGT9MA7?g_st=ic (Maps), https://www.wattlecorp.com/sa/ (Website)

2. **Cipher Company for Cybersecurity**: (https://maps.app.goo.gl/US5Zkzovm5EgVmDu7?g_st=ic (Maps), https://cipher.com.sa/ (Website)
3. **Looptech**: https://maps.app.goo.gl/Bk2QQ38LvJ5LELhd6?g_st=ic (Maps), https://looptech.com.sa/ (Website)
4. **National Museum** (if issues with other options): https://maps.app.goo.gl/TZFkvTbkS9JB5Faf7?g_st=ic (Maps)