Digital Solutions Unit 4: External Assessment Preparation

This resource was developed in 2020 to assist teachers facilitating Digital Solutions Unit 4 to prepare students for external assessment. It was prepared with the help of Leigh Ferguson, Leader of Learning in Technologies, Stuartholme School; Maggie Golawska-Loye, Brisbane Girls Grammar School and resources from the Brisbane Digital Solutions Hub.

This resource was updated in 2024 by Leigh Ferguson, Leader of Learning in Technologies, Stuartholme School.

Unit 4 Digital Solutions: Preparation for the external exam

CONTENTS

Introduction

This resource was developed in 2020 to assist teachers facilitating Digital Solutions Unit 4 to prepare students for external assessment. It was prepared with the help of Leigh Ferguson, Leader of Learning in Technologies, Stuartholme School; Maggie Golawska-Loye, Brisbane Girls Grammar School and resources from the Brisbane Digital Solutions Hub.

This resource was updated in 2024 by Leigh Ferguson, Leader of Learning in Technologies, Stuartholme School.

This resource has also been designed to be a 'living document' and we encourage teacher input. If you would like to add to the document please contact highschool.engage@qut.edu.au. We will endeavour to update the resource biannually.

Disclaimer

QUT makes no representations about the suitability of this information for any purpose. It is provided "as is" without express or implied warranty.

QUT disclaims all warranties with regard to this information, including all implied warranties of merchantability and fitness, in no event shall QUT be liable or any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of this information. This information may include technical inaccuracies or typographical errors. We may make improvements and/or changes to our information at any time.

Links to external websites

This resource contains links to other sites that are external to QUT. We take care when linking to external websites, but we have no direct control over the content of the linked web sites, or to the changes that may occur to the content on those sites. It is the responsibility of the user to make their own decisions about the accuracy, currency, reliability and correctness of information contained in linked external websites.

Copyright

Assessment objectives

This assessment technique is used to determine student achievement in the following objectives:

1. Recognise and describe user-experience elements, programming features, components of data exchange systems, privacy principles and data exchange processes.
2. Symbolise and explain programming ideas, data specifications, data exchange processes, and data flow with and between systems.
3. Analyse problems and information related to a digital problem.
4. Not assessed
5. Synthesise information and ideas to develop possible low-fidelity components of secure data exchange solutions.
6. Not assessed
7. Evaluate components and solutions against criteria to make refinements and justified recommendations and evaluate impacts.
8. Not assessed

Unit 4 has three topics:

- **Topic One:** Digital Methods for Exchanging Data
- **Topic Two:** Complex Digital Data Exchange Problems and Solution Requirements
- **Topic Three:** Prototype Digital Data Exchanges

Specifications

This examination:

- consists of a number of different types of questions relating to Unit 4
- may ask students to respond using multiple choice, short and extended response in sentences or paragraphs
- may ask students to sketch, draw and / or diagrams; write and calculate using algorithms; and interpret unseen stimulus materials

Conditions

- Mode: written
- Time allowed - - Perusal time: 5 minutes Working time: 120 minutes
- Students may use a QCAA-approved non-programmable scientific calculator

Please note:

Not all subject content from Unit 4 will be assessed for the External Assessment (EA) item.

Example Exam Paper Resources

Past Exam papers from NSW

HSC Information and Digital Technology (Privacy Principles, Design Elements & Principles, data types, desk checking, recognising programming ideas)

➔ **Source:** https://educationstandards.nsw.edu.au/wps/portal/nesa/resource-finder/hsc-exam-papers/2023/information-and-digital-technology-2023-hsc-exam-pack

HSC Information Processes and Technology (networks, data transmission, data flow relationships, neural networks)

➔ **Source:** https://educationstandards.nsw.edu.au/wps/portal/nesa/resource-finder/hsc-exam-papers/2023/information-processes-and-technology-2023-hsc-exam-pack

HSC Software Design and Development

➔ **Source:** https://educationstandards.nsw.edu.au/wps/portal/nesa/resource-finder/hsc-exam-papers/2023/software-design-and-development-2023-hsc-exam-pack

Past Exam papers from Victorian Curriculum & Assessment Authority

Computing: Software Development (data structures, XML, data transmission, algorithms)

➔ **Source:** https://www.vcaa.vic.edu.au/assessment/vce-assessment/past-examinations/Pages/Computing-Software-Development.aspx

Computing Informatics

➔ **Source:** https://www.vcaa.vic.edu.au/assessment/vce-assessment/past-examinations/Pages/Computing-Informatics.aspx

Algorithmics

➔ **Source:** https://www.vcaa.vic.edu.au/assessment/vce-assessment/past-examinations/Pages/Algorithmics.aspx

Past Exam papers from Western Australia School Curriculum

Computer Science – Past ATAR Course Exams

➔ **Source:** https://senior-secondary.scsa.wa.edu.au/further-resources/past-atar-course-exams/computer-science-past-atar-course-exams

Past Exam papers from Tasmanian Assessment, Standards & Certification

Computer Science

➔ **Source:** https://www.tasc.tas.gov.au/students/years-11-and-12/preparing-for-exams/previous-exam-papers/

Information Systems and Digital Technologies

➔ **Source:** https://cma.education.tas.gov.au/api/Document/5000/ITS315118%20Information%20Systems%20and%20Digital%20Technologies%20TASC%20Exam%20Paper%202023.pdf

Practice Exam Questions

The following exam questions are from the mock sample external assessment documents available to the public on the QCAA website.

➔ **Source:** https://www.qcaa.qld.edu.au/senior/senior-subjects/syllabuses/technologies/digital-solutions

The BBC bitesize & Khan Academy sites have revision pages

Computer Science

➔ **Source:** https://www.bbc.co.uk/bitesize/examspecs/zdqy7nb

Digital Technologies

➔ **Source:** https://www.bbc.co.uk/bitesize/subjects/z9qy6yc

The revision for the American AP Computer Science exam

➔ **Source:** https://www.khanacademy.org/computing/ap-computer-science-principles

Concept One Focus: Encryption and authentication strategies

Objectives

Topic One

Recognise and describe

→ Encryption and authentication strategies appropriate for securing data transmissions and their differences e.g. two-factor or multi-factor authentication (2FA / MFA) using verification codes vs biometrics

→ Features of symmetric (Data Encryption Standard – DES, Triple DES, AES - Advanced Encryption Standard, Blowfish and Twofish) and assymetric (RSA) encryption algorithms

→ How data compression, encryption and hashing are used in the storage and transfer of data

Analyse and Evaluate

→ Caesar, Polyalphabetic (e.g. Vigenere and Gronsfield), and One-time pad encryption algorithms

Symbolise and explain

→ How application sub-systems e.g. front end, back end, work together to constitute a solution

→ Secure data transmission techniques and processes, including the use of encryption, decryption, authentication, hashing and checksums

Resources

Two-factor authentication (2FA)

Two-factor authentication (2FA) sometimes referred to as 2-step verification, is a security approach requiring users to present two factors for authentication for accessing an account.

→ **Source:** https://www.techtarget.com/searchsecurity/definition/two-factor-authentication

→ **Source:** https://www.microsoft.com/en-au/security/business/security-101/what-is-two-factor-authentication-2fa

Multi-Factor Authentication (MFA)

Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA is a core component of a strong identity and access management (IAM) policy. Rather than just asking for a username and password, MFA requires one or more additional verification factors.

➔ **Source:** https://www.onelogin.com/learn/what-is-mfa

Biometric Authentication

Biometric authentication refers to a cybersecurity process that verifies a user's identity using their biological traits such as fingerprints, voices, retinas and facial features.

➔ **Source:** https://jumpcloud.com/blog/biometric-totp-2fa

Which type of authentication is most secure - 2FA vs MFA vs Biometric?

Even though Biometric authentication is the newer technology, it's difficult to replicate for example, no two fingerprints are the same. It's considered the most secure authentication methods available today.

There are two types of biometric systems: physiological and behavioural for authentication.

➔ **Source:** https://www.aratek.co/news/which-type-of-authentication-is-most-secure
➔ **Source:** https://b-fy.com/blog/Multi-Factor-Authentication-or-Biometrics-/

Data Encryption Standard (DES)

Data encryption standard (DES) has been found vulnerable against very powerful attacks and therefore, the popularity of DES has been on a slight decline. DES is a block cipher and encrypts data in blocks of size of 64 bits each. This means 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits. DES uses a 56-bit key to encrypt any plain text which can easily be cracked using modern technologies. To prevent this from happening double DES and triple DES were introduced which are much more secure than the original DES because it uses 112-bit and 168-bit keys respectively, offering much more security than DES.

➔ **Source:** https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/

Triple DES

Triple DES was designed to replace the DES algorithm, which hackers eventually learned to defeat with relative ease. At one time, Triple DES was the recommended standard and the most widely used symmetric algorithm in the industry. Triple DES uses three individual keys with 56 bits each. The total key length adds up to 168 bits. Despite slowly being phased out, Triple DES still makes a dependable hardware encryption solution for financial services and other industries.

➔ **Source:** https://www.youtube.com/watch?v=2O4dsChgcg8

Advanced Encryption Standard

The Advanced Encryption Standard (AES) is found to be at least six times faster than triple DES. AES is an iterative rather than Feistel cipher. AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix.

➔ **Source:**
https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm
➔ **Source:** https://www.youtube.com/watch?v=IJML18Y-OKw

Blowfish

Blowfish is a symmetric encryption algorithm, meaning that it uses the same secret key to both encrypt and decrypt messages. Blowfish is also a block cipher, meaning that it divides a message up into fixed length blocks during encryption and decryption. The block length for Blowfish is 64 bits; messages that aren't a multiple of eight bytes in size must be padded.

➔ **Source:** https://www.embedded.com/encrypting-data-with-the-blowfish-algorithm/
➔ **Source:** https://www.geeksforgeeks.org/blowfish-algorithm-with-examples/
➔ **Source:** https://www.youtube.com/watch?v=gz8AV0bPaOU

Gronsfeld Cipher

Gronsfeld is essentially a Vigenere cipher but uses numbers instead of letters. So, a Gronsfield key of 0123 is the same as a Vigenere key of ABCD.

➔ **Source:** http://rumkin.com/tools/cipher/gronsfeld.php

One Time Pad Encryption

In cryptography, a one-time pad is a system in which a private key generated randomly is used only once to encrypt a message that is then decrypted by the receiver using a matching one-time pad and key. Messages encrypted with keys based on randomness have the advantage that there is theoretically no way to "break the code" by analysing a succession of messages. Each encryption is unique and bears no relation to the next encryption so that some pattern can be detected.

➔ **Source:** https://searchsecurity.techtarget.com/definition/one-time-pad

Twofish

Twofish is the successor of Blowfish. It is a symmetric key block cipher with a block size of 128 bits, with keys up to 256 bits in length. Twofish is one of the fastest of its kind and ideal for use in hardware and software environments. Twofish has some distinctive features that set it apart from most other cryptographic protocols. It uses pre-computed, key-dependent S-boxes. An S- box (substitution-box) is a basic component of any symmetric key algorithm which performs substitution.

➔ **Source:** https://www.techtarget.com/searchsecurity/definition/Twofish

Vigenère Cipher

Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using the Vigenère square or Vigenère table. The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet. At different points in the encryption process, the cipher uses a different alphabet from one of the rows. The alphabet used at each point depends on a repeating keyword.

➔ **Source:** https://www.geeksforgeeks.org/vigenere-cipher/

RSA

RSA is a public-key encryption algorithm and the standard for encrypting data sent over the internet. Unlike Triple DES, RSA is considered an asymmetric algorithm due to its use of a pair of keys. There is a public key which is what we would use to encrypt our message, and a private key to decrypt it. The result of RSA encryption is a huge batch of data that attackers quite a bit of time and processing power to break.

➔ **Source:** https://www.encryptionconsulting.com/education-center/what-is-rsa/

Data Compression, Encryption, Symmetric & Asymmetric Encryption, Hashing

This is a free computer science document covering data compression, encryption and hashing.

➔ **Source:** https://pmt.physicsandmathstutor.com/download/Computer-Science/A-level/Notes/OCR/1.3-Exchanging-Data/Advanced/1.3.1.%20Compression,%20Encryption%20and%20Hashing.pdf

Comparative Study of Different Cryptographic Algorithms

Journal of Information Security (Volume 11, No. 3, July 2020) article compares Data Encryption Standard (DES), Triple DES (3DES) also known as Triple Data Encryption Algorithm (TDEA), and Advanced Encryption Standard (AES).

➔ **Source:** https://www.scirp.org/journal/paperinformation?paperid=100754

Cybersecurity and Privacy Guide

Best practices, toolkits and templates for higher education.

➔ **Source:** https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/toolkits/encryption-101

Activities

Hacking Secret Ciphers with Python

Hacking Secret Ciphers with Python teaches complete beginners how to program in the Python programming language. The book features the source code to several ciphers and hacking programs for these ciphers. The programs include Caesar cipher, transposition cipher, simple substitution cipher, Vigenère cipher, and hacking programs for each of these ciphers. The final chapters cover the modern RSA cipher and public key cryptography.

→ **Source:** https://inventwithpython.com/hacking/

Note: The second edition of this book is available under the title *Cracking Codes with Python*

→ **Source:** https://inventwithpython.com/cracking/

Cryptography and Encryption Explained
Sweigart, A. (2016). *Invent your own computer games with Python.*

→ **Source:** https://inventwithpython.com/invent4thed/chapter14.html

Caesar Cypher worksheet

→ **Source:** http://csunplugged.mines.edu/Activities/Cryptography/Cryptography.pdf

Cryptography Activities

→ **Source:** https://sites.psu.edu/cvclab/outreach/cryptopraphy-activities-for-k-12/

→ **Source:** https://www.ahschools.us/cms/lib/MN01909485/Centricity/Domain/4557/Loads%20of%20Codes%20%20Cryptography%20Activities.pdf

Hash Function Activity

→ **Source:** https://docs.google.com/document/u/1/d/1mOPxjuo_ITfhL_cf78nGyq9Eo9SajiPaDR0jlKAnDU8/pub

Brut Force Activity

→ **Source:** https://docs.google.com/document/u/1/d/1n-8KmbLHxnsB9ZafulAc9qZ5u-X5vP6Uj3Wbs0ysJQA/pub

Authentication Activity

➔ **Source:** https://teachingsecurity.org/lesson-2-what-is-authentication-and-why-do-we-need-it/

RSA for encryption activity

➔ **Source:** https://docs.google.com/document/u/1/d/18zYaA-VrUwa82lyfCEw9bHMBqc_eqkVLZF6sX8Scl4g/pub

Information Hiding Activity

➔ **Source:** https://classic.csunplugged.org/activities/information-hiding/

Symmetric Algorithms Activity

➔ **Source:** https://docs.google.com/document/u/1/d/1QN6EZkeyYl2aQnYb1vE1fonEiGrtjSHSACm5hRZ_VWI/pub

Searching Algorithms Activity

➔ **Source:** https://classic.csunplugged.org/activities/searching-algorithms/

Concept Two Focus: Useability Principles & Elements and Principles of Visual Communication

Objectives

Topic One

Recognise and describe:

- How useability principles are used to inform solution development
- How the elements and principles of visual communication inform user interface development

Resources

Useability Principles

- Docherty, K., Graham, J., & Russell, A. (2018). *Nelson Digital Solutions for QCE Units 1-4.* Melbourne, Victoria, Australia: Cengage Learning Australia, pp. 22-28; and 230-233.

Elements and Principles of Visual Design

- Docherty, K., Graham, J., & Russell, A. (2018). *Nelson Digital Solutions for QCE Units 1-4.* Melbourne, Victoria, Australia: Cengage Learning Australia, pp. 235.

Inside Visual Communication

- Any image that is used for communicating an idea can be considered an example of visual communication.

- ➔ **Source:** https://insidevisualcommunications.weebly.com/unit-1-elements-and-principles.html

The Key Elements and Principles of Visual Design:

- To create the aesthetic style of a website or app, we work with fundamental elements of visual design, arranging them according to principles of design.

- ➔ **Source:** https://www.interaction-design.org/literature/article/the-building-blocks-of-visual-design?srsltid=AfmBOoqym4zZjW4pDdeRSBZafElqLvt5UYXF7pmlHt76chL-0mQxtkFG

10 Useability heuristics

- The 10 basic principles for designing a good user experience: these have remained true for decades, since they were introduced for heuristic evaluation of user interfaces.

→ **Source 1:** https://www.youtube.com/playlist?list=PLJOFJ3Ok_idtb2YeifXlG1-TYoMBLoG6l

→ **Source:** Jakob's Ten Usability Heuristics
https://ux247.com/usability-principles/

Activities

Activity 1:

List 5 sites or apps with good UI design, and 1-2 with bad design. For each, articulate in your own words why you believe it works or does not work.

Activity 2:

Copy the UI of a good site/app pixel-for-pixel. At the end, write down specific techniques the creator used that "expand your design vocabulary".

Activity 3:

Create 2-3 style tiles for fonts in your database that you particularly want to experiment with. Think of a concept for a site, then design out a style tile featuring:

- Realistic font choices and text elements (e.g. headers, navigational elements, body text)
- Appropriate colour palette
- Example form controls or imagery
- Logo (optional)

Activity 4:

Drawing from the style tiles you have created in Activity 4, design 1-3 screens of an app/website that you are most interested in working on.

Concept Three Focus: Security of Data

Objectives

Topic One

Explain

- Australian Privacy Principles (2014) and ethics applicable to the use of personally identifiable or sensitive data from a digital systems perspective

Describe

- Data using appropriate naming conventions, data formats and structures

Topic Two

Analyse problems and information to determine –

- Scope of given problems
- Constraints and limitations
- Requirements of the solution components
- Necessary coded modularity and features
- Factors and risks that affect data security, including confidentiality, integrity and availability, and privacy

Analyse, evaluate and make –

- Refinements to data to ensure completeness, consistency and integrity

Resources

Australian Privacy Principles
The Australian Privacy Principles (or APPs) are the cornerstone of the privacy protection framework in the *Privacy Act 1988*. They apply to any organisation or agency the Privacy Act covers. There are 13 Australian Privacy Principles.

➔ **Source:** https://www.oaic.gov.au/privacy/australian-privacy-principles/

Queensland Government Privacy Rights

➔ **Source:** https://www.qld.gov.au/law/your-rights/privacy-and-right-to-information/privacy-rights

CIA Triad

The purpose of information security is to prevent confidentiality breaches, data losses, inappropriate data deletion and inaccurate data production. The three fundamental bases of information security are represented in the CIA triad: confidentiality, integrity and availability. Put simply, confidentiality is limiting data access, integrity is ensuring your data is accurate, and availability is making sure it is accessible to those who need it. This triad can be used as a foundation to develop strong information security policies.

➔ **Source**:https://vinciworks.com/blog/what-are-confidentiality-integrity-and-availability-in-information-security/#:~:text=Put%20simply%2C%20confidentiality%20is%20limiting,develop%20strong%20information%20security%20policies.

Naming Files, Paths, and Namespaces

➔ **Source:** https://learn.microsoft.com/en-us/windows/win32/fileio/naming-a-file

File naming and folder structure

To enable you to identify, locate and use your data files efficiently and effectively you need to think about naming your files consistently and structuring your data files in a well-structured and unambiguous folder structure.

➔ **Source:** https://dmeg.cessda.eu/Data-Management-Expert-Guide/2.-Organise-Document/File-naming-and-folder-structure

Data Types and Structures

➔ **Source:** https://www.bbc.co.uk/bitesize/guides/z788jty/revision/1

Data structure and data format requirements

➔ **Source:** https://help.highbond.com/helpdocs/analytics/142/user-guide/en-us/Content/analytics/data_preparation/combining_data/data_structure_and_data_format_requirements.htm

Assessing data for accuracy and reliability

➔ **Source:** https://www.bbc.co.uk/bitesize/guides/zk89r2p/revision/1

Data Security

Data security is the process of protecting corporate data and preventing data loss through unauthorized access. This includes protecting your data from attacks that can encrypt or destroy data, such as ransomware, as well as attacks that can modify or corrupt your data.

Data security also ensures data is available to anyone in the organization who has access to it.

➔ **Source:** https://www.imperva.com/learn/data-security/data-security/

Top 10 types of information security threats

A *security threat* is a malicious act that aims to corrupt or steal data or disrupt an organisation's systems or the entire organization. A *security event* refers to an occurrence during which company data or its network may have been exposed. And an event that results in a data or network breach is called a *security incident.* Listed are the top 10 types of information security threats.

➔ **Source:** https://www.techtarget.com/searchsecurity/feature/Top-10-types-of-information-security-threats-for-IT-teams

What is Cybersecurity?

➔ **Source:** https://www.cisco.com/c/en_au/products/security/what-is-cybersecurity.html

Cyberspace, network security and data transfer

Networks make computers more powerful, but also more vulnerable to attack. In the era of the internet and cloud computing, what are the threats to data security?

➔ **Source:** https://www.bbc.co.uk/bitesize/guides/zycm97h/revision/1

Activities

Cyberspace, network security and data transfer test questions

➔ **Source:** https://www.bbc.co.uk/bitesize/guides/zycm97h/test

The Open University: Introduction to Cyber Security *Free course*

→ **Source:** https://www.futurelearn.com/courses/introduction-to-cyber-security

Privacy Challenge game – Dodge the data dangers!

How data smart are you? Personal information is valuable. It's important to understand how to protect personal information from a data breach. Do you have what it takes to keep your data safe? Take this Privacy Challenge and put your data protection skills to the test!

→ **Source:** https://education.oaic.gov.au/privacy-challenge/

Australian Privacy Principles Quiz

→ **Source:** https://quizgecko.com/learn/australian-privacy-principles-n9aj4g

Undertaking a Privacy Impact Assessment

→ **Source:** https://education.oaic.gov.au/elearning/pia/test.html

Concept Four Focus: Data Flow Diagrams

☑ Objectives

Topic One
Symbolise

- Representations of a digital solution
- Data flow through a system using data flow diagrams

Topic Two
Analyse and explain

- A system's data process by developing data flow diagrams that link external entities, data sources, processes and data storage

🛠 Resources

What is a Data Flow Diagram?

➔ **Source:** http://www.youtube.com/watch?v=6VGTvgaJlIM

DFD Symbols and Diagrams

➔ **Source:** http://www.youtube.com/watch?v=i3lgsdefgkU

Data flow diagram tool

➔ **Source:** https://www.lucidchart.com/pages/examples/data-flow-diagram-software

Why do we need DFD's?

➔ **Source:** http://www.youtube.com/watch?v=kBeUY8noj6A

Student DFD Example

➔ **Source:** https://www.youtube.com/watch?v=Ik85hZkyYPA

Activities

The following four DFD examples can be edited to follow the QCAA DFD guidelines.

Data Flow Diagram – Accessing / Using an Email Server

➜ **Source:** http://www.youtube.com/watch?v=ZFIynt3K3U0

Context & Data Flow Diagram Sample 1: YouTube

➜ **Source:** http://www.youtube.com/watch?v=hiMeEswjWuk&t

Context & Data Flow Diagram Sample 2: Uber

➜ **Source:** http://www.youtube.com/watch?v=X-O6s5sah4o

Context & Data Flow Diagram Sample 3: Netflix

➜ **Source:** http://www.youtube.com/watch?v=dFb21Bldf0A

Planning a Data Flow Diagram Activity

➜ **Source:** http://www.youtube.com/watch?v=VeLkVD0Q_6M

Concept Five Focus: Algorithms using pseudocode

☑ Objectives

Topic One

Recognise and describe

- How simple algorithms consist of input, process and output at various stages

Topic Two

Explain
- The purpose of code and / or algorithm statements using code comments and annotations

⚒ Resources

What is an algorithm?

- → **Source:** https://www.bbc.co.uk/bitesize/topics/z3tbwmn/articles/z3whpv4
- → **Source:** https://youtu.be/6hfOvs8pY1k

Fundamentals of algorithms

- → **Source:** https://www.bbc.co.uk/bitesize/guides/zjddqhv/revision/1

Standard algorithms – three basic programming constructs

- → **Source:** https://www.bbc.co.uk/bitesize/guides/z7kkw6f/revision/6

INPUT and OUTPUT validation

- → **Source:** https://www.bbc.co.uk/bitesize/guides/zfnny4j/revision/1

Designing an algorithm

- → **Source:** https://www.bbc.co.uk/bitesize/subjects/zvc9q6f

Searching algorithms

→ **Source:** https://www.bbc.co.uk/bitesize/guides/zgr2mp3/revision/1

Sorting algorithms

→ **Source:** https://www.bbc.co.uk/bitesize/guides/z2m3b9q/revision/1

Sequencing algorithms

→ **Source:** https://www.bbc.co.uk/bitesize/guides/zsf8d2p/revision/1

Selection algorithms

→ **Source:** https://www.bbc.co.uk/bitesize/guides/zy3q7ty/revision/1

Iteration algorithms

→ **Source:** https://www.bbc.co.uk/bitesize/guides/zg46tfr/revision/1

Logical reasoning

→ **Source:** https://www.bbc.co.uk/bitesize/guides/z8jfyrd/revision/1

How to write Pseudocode

→ **Source:** https://www.geeksforgeeks.org/how-to-write-a-pseudo-code/

Common Pseudocode Action Keywords

→ **Source:** http://users.csc.calpoly.edu/~jdalbey/SWE/pdl_std.html

Fibonacci served three ways

Students compare algorithms used to find the Fibonacci numbers, examine the processes they use and compare their speeds. Students will determine their favoured algorithm and give reasons for their choice. They will learn to apply this knowledge to new problems.

→ **Source:** https://www.digitaltechnologieshub.edu.au/teach-and-assess/classroom-resources/lesson-ideas/fibonacci-served-three-ways/

Activities

Activity Process

Activity 1: Test on Designing Algorithms / Pseudocode

➜ **Source:** https://www.bbc.co.uk/bitesize/guides/zpp49j6/test

Activity 2: Test on Algorithms / Pseudocode

➜ **Source:** https://www.bbc.co.uk/bitesize/guides/z3bq7ty/test

Activity 3: Algorithm Activities

➜ **Source:** https://classic.csunplugged.org/searching-algorithms/

Activity 4: Challenge

Write an algorithm for the following problem.

Write pseudocode for a program that asks the user for a number and outputs all the numbers added together (and including) the number they provided.
e.g. User enters 3 - program returns 6 (0+ 1 + 2 + 3 = 6)

Step 1: Write an algorithm
Step 2: Copy the algorithms to VSC and code a program to replicate the algorithm

Solution:

Activity 4: Solution

```
START
        NUM userInput
        NUM counter =
        0 NUM storage
        = 0


        INPUT userInput
        WHILE counter <= userInput
            storage = storage +
            counter ADD 1 to count
        ENDWHILE

        OUTPUT storage
END
```

Activity 5: Challenge

In a simple number game, the program generates a secret number between 1 and 100. In no more than 10 guesses you try to guess the number. After each guess the program tells you if your guess was too high, too low or correct. The program also keeps track of how many guesses you have had and tells you the game is over when you use all ten of your guesses or when you guess the number correctly.

Write an algorithm (pseudocode) to describe the processes run by the program to play the game. In your solution include:

- A condition which checks for illegal guesses (those less than 1 or greater than 100).
- Function (method) to generate a secret number
- Function to *check the guess* and provide appropriate feedback

This solution will require use of the following control structures **sequence, iteration, selection** and **functions**.

Which of the following iteration methods would you choose? Why?

- **A.** Counted loop (FOR loop)
- **B.** Pre-tested loop (WHILE loop)
- **C.** Post-tested loop (REPEAT_____ UNTIL loop)

Review some **control structures** on the following sites to help you with the solution:

BBC Bitesize "Programming" https://www.bbc.co.uk/bitesize/guides/z433rwx/revision/1

W3schools JavaScript resources https://www.w3schools.com/js/default.asp

WRITE THE ALGORITHM - adhere to the pseudocode rules.

Activity 5: Solution

An algorithm to describe a game in which the user tries to guess a number between 1 and 100, using no more than ten guesses.

BEGIN Program

SET NumOfGuess to 0 (or number of guesses is set to

0) SET GotIt to FALSE

GENERATE a secret number using random number function/method

REPEAT

GET a guess from the user

IF the guess is in range

THEN INCREMENT the number of

guesses Check the guess

ELSE

WRITE the guess is out of range

ENDIF

UNTIL guess is correct (GotIT is TRUE) OR number of guesses is

10 IF the guess is incorrect (GotIt is FALSE) THEN

WRITE you have run out of guesses

(=10) SHOW the secret number

ENDIF

END Program

BEGIN FUNCTION check the

guess IF guess > secret

number THEN

WRITE the guess is too big (or tell the user their guess is too big)

ELSE

IF guess < secret number THEN

WRITE the guess is too

small

ELSE

WRITE Congratulations, you got it

SHOW the number of guesses it took to get the secret number

SET GotIt to TRUE

ENDIF

ENDIF

END FUNCTION check the guess

Concept Six Focus: SQL Querying

📋 Objectives

Topic Three

Use SQL statements including

- CREATE, DROP and ALTER
- INSERT and UPDATE
- SELECT, WHERE, GROUP BY, HAVING, ORDER BY, sub-selection and inner-join clauses

🛠 Resources

SQL - Structured Query Language - is a standarised programming language used to manage and manipulate relational databases. It enables users to perform a variety of tasks such as querying data, creating and modifying database structures and managing access permissions. (**Source:** https://www.geeksforgeeks.org/what-is-sql/)

Learn SQL with Socratica

This resource is for a beginner, learning all the SQL essentials.

➔ **Source:** https://www.youtube.com/watch?v=nWyyDHhTxYU

SQL Interactive Lessons

The SQLBolt platform is a series of interactive lessons and exercises designed to help you quickly learn SQL right in your browser.

➔ **Source:** https://sqlbolt.com/lesson/introduction

What is Inner Join in SQL?
The INNER JOIN selects all rows from both participating tables as long as there is a match between the columns. An SQL INNER JOIN is same as JOIN clause, combining rows from two or more tables. The INNER JOIN in SQL joins two tables according to the matching of a certain criteria using a comparison operator.

➔ **Source:** https://www.sqltutorial.org/sql-inner-join/

The most important and frequently used of the joins is the **INNER JOIN**. They are also referred to as an **EQUIJOIN**.

➔ **Source:** https://www.tutorialspoint.com/sql/sql-inner-joins.htm

The INNER JOIN keyword selects records that have matching values in both tables.

➔ **Source:** https://www.w3schools.com/sql/sql_join_inner.asp

Activities

Activity 1: SQL Teaching

Existing tables are queried covering the majority of SQL statements.

➔ **Source:** https://www.sqlteaching.com/#!select

Activity 2: SQL Tutorial

Learn SQL step by step.

➔ **Source:** https://sqlzoo.net/wiki/SQL_Tutorial

Activity 2: SQL Online Quiz

➔ **Source:** https://www.w3schools.com/sql/sql_quiz.asp

Concept Seven Focus: Emerging Technologies

☑ Objectives

Topic One

Recognise and describe

- How particular algorithms process data differently e.g. machine learning, deep learning, natural language processing and reinforcement learning algorithms

Topic Two
Analyse problems and information to determine

- The potential role of emerging technologies in data exchange solutions, e.g. machine learning

Topic Three
Evaluate

- The personal, social and economic impacts of emerging technologies, e.g. artificial intelligence

🛠 Resources

AI vs Machine Learning vs Deep Learning vs Neural Networks: What's the difference?

While artificial intelligence (AI), machine learning (ML), deep learning and neural networks are related technologies, the terms are often used interchangeably, which frequently leads to confusion about their differences.

➔ **Source:** https://www.ibm.com/think/topics/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks

Examples of Emerging Technologies and Impacts

The multifaceted influence of emerging technologies on diverse aspects of human experience, encompassing personal, societal, organizational and national impacts. Seven different emerging technologies examples are explained and what opportunities and challenges bring about.

➔ **Source:** https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2024/volume-17/emerging-technology-key-challenges-and-opportunities

What is natural language processing and how does it work?

Natural language processing (NLP) is a field of AI that enables computers to understand language like humans do.

➜ **Source:** https://www.techtarget.com/searchenterpriseai/video/What-is-natural-language-processing-NLP

10 Machine Learning Algorithms

➜ **Source:** https://www.simplilearn.com/10-algorithms-machine-learning-engineers-need-to-know-article

Machine Learning Cheat Sheet

This is a guide around the top machine learning algorithms, their advantages and disadvantages, and use-cases.

➜ **Source:** https://www.datacamp.com/cheat-sheet/machine-learning-cheat-sheet

Reinforcement Learning: What It Is, Algorithms, Types and Examples

➜ **Source:** https://www.turing.com/kb/reinforcement-learning-algorithms-types-examples

What is deep learning and how does it work?

Deep learning is a type of machine learning (ML) and artificial intelligence (AI) that trains computers to learn from extensive data sets in a way that simulates human cognitive processes. Deep learning features neural networks constructed from multiple layers of software nodes that work together. Deep learning models are trained using a large set of labeled data and neural network architecture.

➜ **Source:** https://www.techtarget.com/searchenterpriseai/definition/deep-learning-deep-neural-network

Guide to Understanding Reinforcement Learning

Reinforcement learning is a type of machine learning technique where a computer agent learns to perform a task through repeated trial and error interactions with a dynamic environment. This content covers the different types of training algorithms and the pros and cons of each type of algorithm.

➜ Source: https://shorturl.at/7MBf6

Five Future Trends in API

This article provides a glimpse on how Artificial Intelligence (AI) is making significant strides in API development, acting as a catalyst for innovation. AI-driven tools are automating various aspects of API development, including testing, documentation and deployment.

➔ **Source:** https://itsrorymurphy.medium.com/5-future-trends-in-api-development-a-glimpse-into-2024-85d2922a55d0

The Turing Test: What is it, What can pass it, and limitations

➔ **Source:** https://www.geeksforgeeks.org/turing-test-artificial-intelligence/

Human-Computer Interaction & Usability 2024

➔ **Source:** https://books.google.com.au/books?hl=en&lr=&id=cwoSEQAAQBAJ&oi=fnd&pg=PA2006&dq=Human-Computer+interaction+%26+usability+2024&ots=ZwU2TmbhGA&sig=ScWyJlZoPyvEyH8afSO7JcFcgZU#v=onepage&q=Human-Computer%20interaction%20%26%20usability%202024&f=false

Activities

Machine Learning: Take the Quiz

➜ **Source:** https://shorturl.at/9uSxy

AI Detector

➜ **Source:** https://quillbot.com/ai-content-detector

Emerging Technologies Quiz

This topic is designed as an interactive quiz.

➜ **Source:** https://quizizz.com/admin/quiz/5d87736fecf7cd001ab9c161/emerging-technologies

Emerging Technologies – Questions and Answers

A question bank in the form of true / false, fill in the blanks and MC questions on the topic of Emerging Technologies.

➜ **Source:** https://simplycoding.in/emerging-technologies-questions/#google_vignette

Quiz: AI or real?

Can you tell the difference between a real video or picture, or one that has been generated by artificial intelligence (AI)?

➜ **Source:** https://www.bbc.co.uk/bitesize/articles/zqnwxg8

AI quiz: Can you tell which person is real?

How much do you know about artificial intelligence? As the technology rapidly advances, test your know of how AI affects life now and its possible impacts in the near future.

➜ **Source:** https://www.bbc.com/news/uk-66110953

Concept Eight Focus: Desk Checking

☑ Objectives

Topic Three
Evaluate

- Algorithmic steps using desk checks to predict the output for a given input, identify and fix errors (debug) and validate algorithms

🛠 Resources

Desk Checking definition

A method used by a human to check the logic of a computer program's algorithm to reduce the likelihood of errors occurring. This may be done on paper, using a diagram, or mentally trying a sample of typical inputs to see what the outputs would be. For example, to desk check a branching statement {IF age >65 THEN 'retire' ELSE 'keep working'}, the values for age of 64, 65 and 66 could be tried to show that 64 and 65 would result in 'keep working' and 66 in 'retire' so that it could be decided if the statement worked as intended.

➔ **Source:**https://k10outline.scsa.wa.edu.au/home/p-10-curriculum/curriculum-browser/syllabus/technologies-overview/glossary/desk-checking

Desk Check Example

➔ **Source:** https://www.youtube.com/watch?v=cV8CHJFUYNM

What is desk checking and trace table example?

Desk checking is a technique for verifying the logic of an algorithm. It does not involve use of a computer, rather a person is responsible for carrying out the desk check. The desk checker observes and analyses the logic behind the algorithm.

➔ **Source:** https://www.professionalqa.com/desk-checking

Desk checking algorithms using trace tables

➔ **Source:** https://youtu.be/i2qLAVBUERs

Activities

Algorithms and desk checking workbook – scroll down on web page to download

→ **Source:** https://education.nsw.gov.au/teaching-and-learning/curriculum/tas/tas-curriculum-resources-7-12/tas-11-12-curriculum-resources/hsc-algorithms-and-desk-checking

Desk Checking Algorithm Activities

→ **Source:** http://passyworldofict.com/programming/programming11/

Activity:

The following pseudocode calculates the area of a floor so that a carpet can be fitted that is the correct size. Perform a desk-check on this algorithm using a table to show the values in each variable after the execution of each line. You should assume an input value of 50 for length and 50 for width.

- Data width as whole number
- Data length as whole number
- Data area as whole number
- Output "Welcome to the carpet area calculator"
- Output "What is the width of your floor"
- Input width

→ Output "What is the length of your floor"
→ Input length
→ Area = length * width
→ Output "For your floor you will need a carpet that is:"
→ Output area
→ Output "Thank you for using this program."

Concept Nine Focus: Networks

☑ Objectives

Topic One

Explain

- Network performance metrics of latency, jitter and the guarantee and timeliness of delivery
- Network transmission principles, including protocol standards e.g. TCP / IP, HTTP, FTP and VNP, packet switching, error detection and correction, routing and forwarding, flow and congestion control, quality of service (QoS), security e.g. confidentiality, integrity and availability of data
- Methods for data exchange used to transfer data across networked systems, including REST, JSON and XML, with the assistance of APIs that facilitate data exchange between different systems and applications

Symbolise and explain:

→ How application sub-systems e.g. front end, back end, work together to constitute a solution

🛠 Resources

Networks

→ **Source:** https://www.bbc.co.uk/bitesize/guides/zj88jty/revision/1

What are network metrics?

→ **Source:** https://www.cbtnuggets.com/blog/technology/networking/what-are-network-metrics

Jitter, Packet Loss and Latency in Network Performance

→ **Source:** https://www.dnsstuff.com/jitter-packet-loss-and-latency-in-network-performance

Delivery, Accuracy, Timeliness, Jitter within data communications

→ **Source:** https://www.scribd.com/document/489515677/Chapter-1

Communication Technologies – Data Transfer Principles

→ **Source:** https://www.computersciencecafe.com/23-data-transmission-principles.html

Essential Network Protocols

➔ **Source:** https://www.youtube.com/watch?v=jQ6_XhsMwws

Packet Switching

Packet Switching in computer networks is a method of transferring data to a network in the form of packets. In order to transfer the file fast and efficiently over the network and minimize the transmission latency, the data is broken into small pieces of variable length, called **Packet**. At the destination, all these small parts (packets) have to be reassembled, belonging to the same file.

➔ **Source:** https://www.geeksforgeeks.org/packet-switching-and-delays-in-computer-network/

CIA Triad

The three letters in CIA triad stand for Confidentiality, Integrity and Availability. The CIA Triad is a common model that forms the basis for the development of security systems.

➔ **Source:** https://www.itgovernance.co.uk/blog/what-is-the-cia-triad-and-why-is-it-important

What is Quality of Service (QoS) in Networking?

Quality of Service is a network feature that sorts and prioritizes data, ensuring that essential activity like video calls get the necessary bandwidth and speed. This process helps maintain efficient and reliable network performance for high-priority tasks.

➔ **Source:** https://www.cbtnuggets.com/blog/technology/networking/what-is-qos-in-networking

The Internet Crash Course

Covering network types, IP & how data travels over the network.

➔ **Source:** https://youtu.be/AEaKrq3SpW8

World Wide Web

➔ **Source:** https://youtu.be/guvsH5OFizE

Khan Academy "How the Internet Works"

➔ **Source:** https://www.khanacademy.org/computing/computer-science/computers-and-internet- code-org/computers-and-internet-code-org/internet-works-intro/v/the-internet-wires- cables-and-wifi

Khan Academy "The Internet"

Covers wide range of concepts about file transfer protocols and security, readings, and quizzes.

➔ **Source:** https://www.khanacademy.org/computing/ap-computer-science-principles/the-internet

FTP explained

➔ **Source:** https://www.youtube.com/watch?v=tOj8MSEIbfA

What is a VPN?

➔ **Source:** https://www.youtube.com/watch?v=q4P4BjjXghQ

REST API essentials

➔ **Source:** https://restfulapi.net/security-essentials/

Remote APIs

➔ **Source:** https://www.youtube.com/watch?v=GZvSYJDk-us&t=775s

How the web works

➔ **Source:** https://www.youtube.com/watch?v=GZvSYJDk-us&t=1024s

RESTful API Constraint Scavenger Hunt

➔ **Source:** https://www.youtube.com/watch?v=GZvSYJDk-us&t=1320s

Web API security

➔ **Source:** https://www.imperva.com/learn/application-security/web-api-security/

How SMTP mail server works

➔ **Source:** https://www.hostinger.com/tutorials/how-to-use-free-google-smtp-server

JSON and XML differences and syntax

➔ **Source:** https://www.guru99.com/json-vs-xml-difference.html

Stepped through introduction to JSON

➔ **Source:** https://restfulapi.net/introduction-to-json/

Activities

Activity 1: HTTP and Abstraction on the Internet

→ **Source:** https://curriculum.code.org/csp-19/unit1/13/

Activity 2: Network Security Activities

→ **Source:** Log-in to Grok Learning - https://groklearning.com/course/cyber-910-py-networking/ (Courses: Monitoring and securing networks; Network Security)

Activity 3: Coding with JSON and JavaScript basics

→ **Source:** https://developer.mozilla.org/en-US/docs/Learn/JavaScript/Objects/JSON

Glossary

NB: These terms are not included in the Unit 4 in the Digital Solutions syllabus glossary.

TERM	DEFINITION
A	
Advanced Encryption Standard	The more popular and widely adopted symmetric encryption algorithm is the Advanced Encryption Standard (AES). It is found at least six times faster than triple DES. AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. Source: https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm
Application sub-systems	a smaller, simpler part of a larger system Source: http://www.cs.fsu.edu/~myers/cop3331/notes/sysdesign.html
ASCII	ASCII stands for the "American Standard Code for Information Interchange". ASCII is a 7-bit character set containing 128 characters. It contains the numbers from 0-9, the uppercase and lowercase English letters from A to Z, and some special characters. The character-sets used in modern computers, HTML, and Internet are all based on ASCII. Source: https://www.w3schools.com/charsets/ref_html_ascii.asp
Authentication	Verifying the integrity of a transmitted message and / or verifying the identity of a user logging into a network or computer. Passwords, digital certificates, smart cards and biometrics can be used to prove user identity. Digital certificates can also be used to identify the network to the client. Source: https://www.pcmag.com/encyclopedia/term/authentication
B	
Bandwidth	Bandwidth measures how much data can flow through a specific connection at one time. Bandwidth is typically expressed in *bits per second*, like 60 Mbps or 60 Mb/s, to explain a data transfer rate of 60 million bits (megabits) every second. Source: https://techterms.com/definition/bandwidth
Biometrics	The biological identification of a person e.g. face, iris and retinal patterns and voice recognition. Source: https://www.pcmag.com/encyclopedia/term/biometrics
Bitrate	Bitrate describes the rate at which bits are transferred from one location to another. In other words, it measures how much data is transmitted in a given amount of time. Bitrate is commonly measured in bits per second (bps), kilobits per second (Kbps), or megabits per second (Mbps). Source: https://techterms.com/definition/bitrate
Blowfish Encryption	Blowfish is a symmetric encryption algorithm, meaning that it uses the same secret key to both encrypt and decrypt messages. Blowfish is also a block cipher, meaning that it divides a message up into fixed length blocks during encryption and decryption. The block length for Blowfish is 64 bits; messages that aren't a multiple of eight bytes in size must be padded. Source: https://www.embedded.com/encrypting-data-with-the-blowfish-algorithm/
C	
Checksum	A checksum is a value (sequence of numbers or letters) used to verify the integrity of a file or a data transfer. In other words, it is a sum that checks the validity of data. Checksums are typically used to compare two sets of data to make sure they are the same. Source: https://techterms.com/definition/checksum

Client-Server architecture	The "client-server" architecture is common in both local and wide area networks. For example, if an office has a server that stores the company's database on it, the other computers in the office that can access the database are "clients" of the server. Source: https://techterms.com/definition/client
Cybersecurity	is the set of practices and tools that individuals, IT staff, and governments use to keep information and devices safe from attackers. Ultimately, the goal of cybersecurity is to ensure the integrity, confidentiality, and availability of digital information. Files must be accessible to authorised users on demand, but must remain inaccessible to anyone else. Source: https://www.techradar.com/au/news/cybersecurity-what-is-it
D	
Data Confidentiality	In the context of computer systems, allows authorized users to access sensitive and protected data. Specific mechanisms ensure confidentiality and safeguard data from harmful intruders. Source: https://www.techopedia.com/definition/10254/confidentiality
Data encryption standard (DES)	DES is a block cipher and encrypts data in blocks of size of 64 bit each, means 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits. Source: https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/
Data Exchange Systems	A data exchange system is a structured system that facilitates the transfer of data between different entities, such as organizations, information systems, and individuals. This system relies on a set of standards, protocols, and technologies to ensure that data is transmitted accurately, securely, and efficiently. Source: https://www.teradata.com/insights/data-platform/what-is-data-exchange
Data Input	Any information or data sent to a computer for processing is considered input. Input or user input is sent to a computer using an input device. Source: https://www.computerhope.com/jargon/i/input.htm
Data Integrity	Is the assurance that digital information is uncorrupted and can only be accessed or modified by those authorised to do so. Data integrity describes data that's kept complete, accurate, consistent and safe throughout its entire lifecycle. Source: https://www.techtarget.com/searchdatacenter/definition/integrity
Data Output	Any information that is processed by and sent out from a computer or other electronic device is considered output. An example of output is anything viewed on your computer monitor screen. Source: https://www.computerhope.com/jargon/o/output.htm
Data Privacy	is the right to control how personal information is collected, with whom it is shared, and how it is used, retained or deleted. Source: https://www.imperva.com/learn/data-security/data-privacy/
Data Protection	Data protection is the process of safeguarding data and restoring important information in the event that the data is corrupted, compromised or lost due to cyberattacks, shutdowns, intentional harm or human error. Source: https://www.techtarget.com/searchdatabackup/definition/data-protection
Data Security	Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption. Source: https://www.techopedia.com/definition/26464/data-security
Data Structure	The physical layout of data. Data fields, memo fields, fixed length fields, variable length fields, records, word processing documents, spreadsheets, data files, database tables and indexes are all examples of data structures. Source: https://www.pcmag.com/encyclopedia/term/data-structure

Data Transmission	Data transmission is the process of sending digital or analogue data over a communication medium to one or more computing, network, communication or electronic devices. Source: https://www.techopedia.com/definition/9756/data-transmission
Deep Learning	Deep learning is a type of machine learning (ML) and artificial intelligence (AI) that trains computers to learn from extensive data sets in a way that simulates human cognitive processes. Source: https://www.techtarget.com/searchenterpriseai/definition/deep-learning-deep-neural-network
Desk Check	Desk checking is a technique for verifying the logic of an algorithm. It does not involve use of a computer, rather a person is responsible for carrying out the desk check. Source: https://www.professionalqa.com/desk-checking
Digital Environment	A context, or a "place", that is enabled by technology and digital devices, often transmitted over the Internet, or other digital means, e.g., mobile phone network. Records and evidence of an individual's interaction with a digital environment constitute their digital footprint. Source: https://www.igi-global.com/dictionary/models-of-competences-for-the-real-and-digital-world/7610
Distributed Denial of Service (DDoS)	A denial of service (DoS) attack is an attempt to overload a website or network, with the aim of degrading its performance or even making it completely inaccessible. A distributed denial of service attack is a form of DoS attack that originates from more than one source. Source: https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection
Domain Name System (DNS)	The domain name system (DNS) is a naming database in which internet domain names are located and translated into Internet Protocol (IP) addresses. The domain name system maps the name people use to locate a website to the IP address that a computer uses to locate that website. Source: https://www.techtarget.com/searchnetworking/definition/domain-name-system
DNS Spoofing	DNS spoofing is a type of attack that exploits vulnerabilities in the domain name system to divert internet traffic away from legitimate servers and towards fake ones. Source: https://www.howtogeek.com/161808/htg-explains-what-is-dns- cache-poisoning/
F	
Fibre Optic Cable	Fibre optic cable is used to transmit a serial bit stream using pulses of light. Source: https://erg.abdn.ac.uk/users/gorry/course/phy-pages/fibre.html
Firewall	A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. Source: https://www.cisco.com/c/en_au/products/security/firewalls/what-is-a- firewall.html
G	
Gronsfeld Cipher	The Gronsfeld cipher is a polyalphabetic cipher, a series of Caesar ciphers, where the shift is determined by numbers (between 0 and 9). It is similar to the Vigenère cipher, but the key uses digits instead of letters. Source: https://www.boxentriq.com/code-breaking/gronsfeld-cipher
H	
Hashing	Hashing is the practice of taking a string or input key, a variable created for storing narrative data, and representing it with a hash value, which is typically determined by an algorithm and constitutes a much shorter string than the original. Source: https://www.techopedia.com/definition/14316/hashing- cybersecurity

I	
Internet Protocol Address (IP address)	A unique address is the unique identifying number organised in a particular way to identify each device on the network. *e.g. 192.168 1.1* and assigned to every device connected to the Internet. Source: https://www.fortinet.com/resources/cyberglossary/what-is-ip-address
Internet Protocols	Internet Protocols are a set of rules that governs the communication and exchange of data over the internet. Source: https://www.geeksforgeeks.org/types-of-internet-protocols/
Internet Service Provider (ISP)	An Internet service provider (ISP), also known as Internet access provider is a company that provides customers with Internet access. Source: https://www.techopedia.com/definition/2510/internet-service- provider-isp
J	
Jitter	Jitter is the variation in the latency on a packet flow between two systems when some packets take longer to travel from one system to the other. Jitter results from network congestion, timing drift and route changes. Source: https://www.techtarget.com/searchunifiedcommunications/definition/jitter
M	
Machine Learning	Machine learning (ML) is a branch of artificial intelligence (AI) and computer science that focuses on the using data and algorithms to enable AI to imitate the way that humans learn, gradually improving its accuracy. Source: https://www.ibm.com/topics/machine-learning
N	
Naming Convention	(Universal Naming Convention) A standard for identifying servers, printers and other resources in a network, which originated in the Unix community. A UNC path uses double slashes or backslashes to precede the name of the computer. The path (disk and directories) within the computer are separated with a single slash or backslash, as in the following examples. Note that in the DOS/Windows example, drive letters (c:, d:, etc.) are not used in UNC names. Source: https://www.pcmag.com/encyclopedia/term/unc
Network Redundancy	Network redundancy is a process through which additional or alternate instances of network devices, equipment and communication mediums are installed within network infrastructure. It is a method for ensuring network availability in case of a network device or path failure and unavailability. As such, it provides a means of network failover. Source: https://www.techopedia.com/definition/29305/network- redundancy
Network Types	A wireless network allows devices to stay connected to the network, but roam untethered to any wires. Access points amplify Wi-Fi signals, so a device can be far from a router but still be connected to the network. A wired network uses cables to connect devices, such as laptop or desktop computers, to the Internet or another network. Source: https://www.cisco.com/c/en_au/solutions/small-business/resource-center/networking/wireless-network.html A local area network (LAN) is a collection of devices connected together in one physical location, such as a building, office, or home. A wide area network (WAN) or metropolitan area network (MAN) covers larger geographic areas. Source: https://www.cisco.com/c/en/us/products/switches/what-is-a- lan-local-area-network.html A cellular mobile network consists of three components: mobile devices, a radio access network and a core network. The mobile device might be a smart phone,

	tablet, or a computer with a USB dongle, but could also be a low-cost sensor with a simple transmitter. The radio access network consists mainly of base stations (mobile phone towers) and is connected to the core network. The base station uses radio waves to relay communications between the mobile device and the core network. The area covered by a base station is called a cell. Source: https://theconversation.com/what-is-a-mobile-network-anyway-_this-is-5g-boiled-down-102199
Neural Network	A neural network is a machine learning program, or model, that makes decisions in a manner similar to the human brain. Source: https://www.ibm.com/topics/neural-networks
O	
Object-oriented programming language (OOP)	Object-oriented programming (OOP) is a computer programming model that organizes software design around data, or objects, rather than functions and logic. An object can be defined as a data field that has unique attributes and behaviour. Source: https://searchapparchitecture.techtarget.com/definition/object-oriented-programming-OOP
One-time pad encryption algorithm	One-time pad cipher is an unbreakable cipher; the key is exactly same as the length of message which is encrypted; the key is made up of random symbols; as the name suggests, key is used one time only and never used again for any other message to be encrypted. Due to this, encrypted message will be vulnerable to attack for a cryptanalyst. The key used for a one-time pad cipher is called pad, as it is printed on pads of paper. Source: https://www.tutorialspoint.com/cryptography_with_python/cryptography_with_python_one_time_pad_cipher.htm
R	
Reinforcement Learning	Reinforcement learning is a type of machine learning technique where a computer agent learns to perform a task through repeated trial and error interactions with a dynamic environment. Source: https://shorturl.at/7MBf6
Router	A router connects multiple networks and routes network traffic between them. The router sits in between your Internet connection and your local network. Source: https://www.howtogeek.com/234233/whats-the-difference-_between-a-modem-and-a-router/
RSA Algorithm	Under RSA encryption, messages are encrypted with a code called a public key, which can be shared openly. Due to some distinct mathematical properties of the RSA algorithm, once a message has been encrypted with the public key, it can only be decrypted by another key, known as the private key. Each RSA user has a key pair consisting of their public and private keys. Source: https://www.comparitech.com/blog/information-security/rsa-_encryption/
S	
SSL Certificate	SSL stands for Secure Sockets Layer, it's the standard technology for keeping an internet connection secure and safeguarding any sensitive data that is being sent between two systems, preventing criminals from reading and modifying any information transferred, including potential personal details. TLS (Transport Layer Security) is just an updated, more secure, version of SSL. Source: https://www.websecurity.digicert.com/en/au/security-_topics/what-is-ssl-tls-https

T	
Timeliness	Timeliness refers to the time expectation for accessibility and availability of information. Timeliness can be measured as the time between when information is expected and when it is readily available for use. Source: https://www.sciencedirect.com/topics/computer- science/timeliness
Transmission Control Protocol (TCP)	The Transmission Control Protocol (TCP) is a transport protocol that is used on top of IP to ensure reliable transmission of packets. Source: https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:the- internet/xcae6f4a7ff015e7d:transporting-packets/a/transmission- control-protocol--tcp
Twofish	is a symmetric block cipher; a single key is used for encryption and decryption. Twofish has a block size of 128 bits and accepts a key of any length up to 256 bits. (NIST required the algorithm to accept 128-, 192-, and 256-bit keys.) Source: https://www.schneier.com/academic/archives/1998/12/the_twofish_encrypti.html
U	
Universal Naming Convention (UNC)	UNC is a filename format that is used to specify the location of files, folders, and resources on a local-area network (LAN). The UNC address of a file may look something like this: \\server-name\directory\filename UNC can also be used to identify peripheral devices shared on the network, including scanners and printers. Source: https://techterms.com/definition/unc
Uniform Resource Locator (URL)	URL is defined as the global address of documents and other resources on the World Wide Web. The first part of the URL is called a *protocol identifier* and it indicates what protocol to use, and the second part is called a *resource name* and it specifies the IP address or the domain name where the resource is located. The protocol identifier and the resource name are separated by a colon and two forward slashes. Source: https://www.webopedia.com/TERM/U/URL.html
V	
Vigenère Cipher	Vigenere cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using the *Vigenère square or Vigenère table*. Source: https://www.geeksforgeeks.org/vigenere-cipher/