Guided Exploration 02: Abstractions, Encoding, Internet and Cybersecurity

**Points:** 30

**Due Date:**  Mar 7.

Work will be accepted up to 24 hours after the due date with a 10% penalty. Meaning if you turn it in at 12:01 am of the next day you will be deducted 10% of the total points from your score. If the assignment is more than 24 hours late, it will be a 0.

**Purpose:** This guided exploration allows students to explore fundamental computing concepts, including data encoding, the Internet’s structure, and cybersecurity principles. Through hands-on activities, analysis, and reflection, students will deepen their understanding of how data is processed, transmitted, and secured in computing systems.

Objectives

1. **Understand how data is encoded and transmitted** using different encoding schemes and network protocols.
2. **Analyze the structure and function of the Internet**, including IP addressing, DNS, and packet routing.
3. **Explore cybersecurity principles** such as encryption, authentication, and secure communication.
4. **Apply knowledge through interactive activities**, including encryption exercises and cybersecurity games.
5. **Reflect on the impact of cybersecurity threats** and develop strategies for data protection.

Effort: Collaborative and Individual following [CS Academic Integrity and AI Policy - Harding](https://docs.google.com/document/d/1SY4-RMJ2B9GkEbTzmpRVSfKKsgQnYWYF/edit)

* You are encouraged to collaborate to discuss concepts but individually write your own code and answer the questions in your own words . When you ask questions and explain to others you get a deeper understanding. You can use AI tools but remember
  + Acceptable: Using ChatGPT to explain HTML
  + Unacceptable: Asking ChatGPT to generate your explanation

**Deliverables:**

* Upload this document as a pdf or word document with your answers

[Part 1 Explore and Analyze](#_heading=h.1fob9te)

[1.1 Data Encoding Schemes](#_heading=h.xjt07tpdomw0)

[1.2 Internet Fundamentals](#_heading=h.86eznhfwnzuu)

[1.3 Cybersecurity](#_heading=h.ccr3azg3zs62)

[1.4 Encryption](#_heading=h.s576fqvn9hww)

[2 Apply Concepts](#_heading=h.lppebdwg94h)

[🔍 Choose One of the following 5 games to explore and learn](#_heading=h.7rdrqjczeqin)

[3 Reflection](#_heading=h.5ssd56a4uuo)

| **Criterion** | **Exemplary A+** | **Proficient A-B** | **Developing C-D** | **Insufficient F** |
| --- | --- | --- | --- | --- |
| **Explore and Explain Concepts**  **10pts** | Clearly explains key ideas with detailed examples, using accurate words from lectures, books, or provided resources. Demonstrates the ability to connect different ideas. | Explains most key ideas with examples and evidence, but some details or examples may be missing. | Explains some ideas but is not clear or complete. Provides limited examples. | Fails to explain key ideas, or explanations are incomplete and lack examples. |
| **Analyze and Apply**  **10pts** | Uses computing concepts to solve problems correctly, showing a strong connection between ideas and practice. | Uses computing concepts correctly, with small mistakes or missing minor details. Solutions show an understanding of ideas and practice. | Tries to use computing concepts, but there are major mistakes or missing steps. | Does not use computing concepts correctly, or the work is not complete. |
| **Reflection**  **5pts** | Response demonstrates in-depth personal reflection on the experience and learnings that includes plans for future action. | Response demonstrates a general reflection on the experience and learnings that includes plans for future action | Response shows little evidence of personal reflection and future action. | Limited evidence, incomplete or missing. |

# 

# Part 1 Explore and Analyze

## 1.1 Data Encoding Schemes

Watch [Why do computers use 1s and 0s?](https://www.youtube.com/watch?v=Xpk67YzOn5w&t=10s)

| 1.1.1 Explain the difference between base 10 and binary values.  Base 10 is 0-9. Used to translate code down to Binary.  Binary is 0-1. Used for on/off situations and is the most crude and basic form of programming. |
| --- |
| 1.1.2 Explain bits and bytes.  A BIT is the smallest line of code possible, a single binary digit, a BYTE is 8 BITs together. |
| 1.1.3 Explain ASCII and include an example of how the character ‘Z’ is represented.  ASCII is the standard code translator, it is used to translate human input into base ten and down to binary so that computers can comprehend input.  Z = 5A in ASCII |
| 1.1.4 What decimal number is represented by 01011? Use the table below to show how to get your answer.   | 0 | 1 | 0 | 1 | 1 | | --- | --- | --- | --- | --- | | 24 | 23 | 22 | 21 | 20 | | 0 | 8 | 0 | 2 | 1 |   Explain your answer.  0+8+0+2+1=11 |
| 1.1.5 How would you write the number 20 in binary? Use the table below to show how to get your answer.   | 16 | 8 | 4 | 2 | 1 | | --- | --- | --- | --- | --- | | 24 | 23 | 22 | 21 | 20 | | 1 | 0 | 1 | 0 | 0 |   Explain our answer.  16+0+4+0+0=20 |
| 1.1.10 What is the largest number you can represent using 8 bits? Explain your answer.  255  128+64+32+16+8+4+2+1=255 |
| 1.1.11 Explain how colors can be represented on a webpage using RGB and hexadecimal. Include examples.  Three 8 bit inputs that determine the brightness of one of three colors, which then combines the three colors together to show the combined color  0 = Darkest, 255 = Brightest  Red: 0-255  Blue: 0-255  Green: 0-255 |

## 1.2 Internet Fundamentals

Answer the following. Diagrams can be drawn on paper or you can use a drawing tool or powerpoint. Here are some tools. If you draw it on paper you can take a picture and then put the picture in the document. Let me know if you need help with this.

1. Excalidraw (<https://excalidraw.com/>)

* Simple, freehand-style sketching tool.
* Great for quick network sketches and flowcharts.
* No sign-up required and supports real-time collaboration.

2. Diagrams.net (formerly Draw.io) (<https://app.diagrams.net/> )

* Free drag-and-drop tool for creating flowcharts and network diagrams.
* Integrates with Github, Google Drive, OneDrive, and Dropbox for saving work.

3. Sketch.io (Sketchpad) (<https://sketch.io/sketchpad/> )

* A simple browser-based drawing tool with basic shapes and freehand sketching.
* Works well for visualizing network paths and redundancy concepts.

| 1.2.1 **Internet’s Structure**  On paper, draw a simple diagram of how your device connects to a website on the Internet to send information to another computer. Label the following: **Internet, router, packets, protocol, transmission.** |
| --- |
| 1.2.2 **Network Paths and Routing**  Draw a simple map showing multiple routes a packet could take to reach a website. Label routers, network paths, and alternative routes. |
| 1.2.3 **DNS and IP Addressing**  Create a diagram showing how **DNS** works like a phone book for the Internet. Include: **domain name, IP address, DNS lookup, resolution, and hierarchical structure**. |

## 1.3 Cybersecurity

| 1.3.1 Define encryption and decryption  Encryption is the process of securing a message or image via scrambling the data information within a special pattern. With Decryption being the inverse of this process and is instead the reforming of the scrambled data into an image or text. |
| --- |
| 1.3.2 Explain the difference between **symmetric and asymmetric encryption**.    Symmetric encryption uses a single key between trusted addresses.  Asymmetric encryption uses a public key meant for a wide public to access. |
| 1.3.3 Why is encryption important for online security?  To ensure that vital systems, websites, computers and devices that can access the internet aren’t easily accessed and maliciously tampered with. |
| 1.3.4 How do public and private keys work together in encryption?  Public and Private keys work together to ensure who has and who hasn’t got access to certain digital spaces or items. |

## 

# 2 Apply Concepts

**🔐 Cybersecurity Game Challenge: Pick Your Path & Learn Key Concepts! 🚀**

You're about to dive into cybersecurity through hands-on challenges! Choose a game that fits your interests and experience level. After playing, share your thoughts, results, and new vocabulary you learned!

## 🔍 Choose One of the following 5 games to explore and learn

| **Intro Game 🕵️‍♂️** [**KC7 Cyber Detective**](https://kc7cyber.com/) **→ Solve cybercrime cases using log analysis & investigation.**   * Concepts & Vocabulary You'll Learn: 🔹 Threat detection – Identifying suspicious activity in logs 🔹 Social engineering – How attackers manipulate people to gain access 🔹 Incident response – Steps taken after a security breach |
| --- |
| 2.1.1 **Complete 1 full case**  What was the biggest challenge?  Loading the game.  What was your favorite part of the game?  Not much, text games about complex subjects don’t catch my attention, but do teach me. |
| 2.1.2 List and summarize the cybersecurity concepts or vocabulary you learned.  Threat detection: Identifying activity that’s either suspicious or unusual to find a potential security breach.  Social engineering: Manipulation and trickery performed by hackers/attackers in order to gain access to a system.  Incident response: How to control the damage and the fire caused by a security breach. |
| 2.1.3 How can companies or individuals protect against the threats you encountered? Understand the signs of an attempted security breach and an undergoing security breach and knowing how to do damage control to ensure more information isn’t stolen. |

| **Intro Game 💻** [**TryHackMe: Introduction to Cybersecurity**](https://tryhackme.com/) **→ Hands-on cybersecurity fundamentals.**   * Concepts & Vocabulary You'll Learn: 🔹 Phishing – Tricking users into revealing credentials 🔹 Encryption – Protecting data using ciphers 🔹 Hashing – Verifying data integrity without storing passwords 🔹 Firewalls – Security barriers to block unauthorized access |
| --- |
| **2.1.1 Complete the first 3 rooms**  What was the biggest challenge?  Figuring out what to do first  What was your favorite part of the game?  Nothing. |
| 2.1.2 List and summarize the cybersecurity concepts or vocabulary you learned.  Phishing: Praying on the gullibility of people to steal personal information via fake messages, emails and websites.  Encryption: Scrambling received data before sending it to ensure it isn’t easily accessed by any intercepting third parties.  Hashing: Verifying incoming information.  Firewalls: A defensive measure made to filter out incoming/outcoming information to ensure no malicious code is allowed to enter. |
| 2.1.3 How can companies or individuals protect against the threats you encountered? |

| **Advanced Game 🔐** [**TryHackMe: Advanced Rooms**](https://tryhackme.com/) **→ Penetration testing, ethical hacking, and OSINT.**   * Concepts & Vocabulary You'll Learn: 🔹 Penetration testing – Simulating real cyberattacks to find weaknesses 🔹 SQL injection – Exploiting databases through malicious queries 🔹 Cross-site scripting (XSS) – Injecting malicious scripts into websites 🔹 Privilege escalation – Gaining higher access than authorized |
| --- |
| **2.1.1 Finish 1 pentesting challenge**  What was the biggest challenge?  Injecting code  What was your favorite part of the game?  Nothing. |
| 2.1.2 List and summarize the cybersecurity concepts or vocabulary you learned.  Penetration testing: Simulating a cyberattack to identify weaknesses.  SQL Injection: Sending in malicious scripts and code to alter and manipulate a database, Server, device or website.  Cross-site scripting: Manipulating several websites via the transfer of malicious code or scripts. |
| 2.1.3 How can companies or individuals protect against the threats you encountered? Ensuring that malicious information can’t be sent into vital software of databases or websites and that it can’t be sent to friendly users. Firewalls can filter this information decently well. |

| **Advanced Game 💀** [**OverTheWire: Bandit**](https://overthewire.org/wargames/bandit/) **→ Command-line hacking and privilege escalation.**   * Concepts & Vocabulary You'll Learn: 🔹 Command-line navigation – Using Linux/Unix for cybersecurity 🔹 Privilege escalation – Gaining unauthorized admin access 🔹 Brute force attacks – Guessing passwords systematically 🔹 SSH (Secure Shell) – Securely accessing remote systems |
| --- |
| **2.1.1 Reach Level 5**  What was the biggest challenge?  Figuring out the first lines of code.  What was your favorite part of the game?  Feeling like I was committing cyber crimes. |
| 2.1.2 List and summarize the cybersecurity concepts or vocabulary you learned.  Brute Force Attacks: Lucky guesses or using systems or code to figure out passwords to systems or devices. Very common.  Privilege Escalation: Upgrading the level of access a hacker has via changing clients and accessing high importance/control clients and devices.  Command-line navigation: Using the command lines of an operating system for a variety of uses, from altering the OS, gaining admin access to systems or running more thorough scans of a system or device. |
| 2.1.3 How can companies or individuals protect against the threats you encountered? Ensuring that remote systems can’t be accessed by out of network devices or clients. |

# 3 Reflection

## Part 3: Reflection

Write a brief reflection on this guided exploration.

| **3.1.1** What concepts were new to you?  Defensive hacking. |
| --- |
| 3.1.2 How does this knowledge apply to real-world cybersecurity?  Understanding the basics of cybersecurity and getting an idea of how much damage hacking can both cause and repair. |
| 3.1.3 If you had more time, what would you explore further? Offensive/Defensive Hacking |

Read what the deliverables are to be uploaded and due date for this assignment