SIT111 Computer Systems

**Computer Systems Overview and Gate Logic (Week 1):**

* This topic provides a general introduction to computer systems, including hardware and software components. Understanding the interaction between hardware and software is essential for grasping the overall functioning of a computer system. In the context of cybersecurity, this knowledge is valuable for identifying potential attack surfaces, securing hardware components (e.g., BIOS), and developing secure software applications that mitigate common vulnerabilities and exploits.

**Logic Gate Implementation (Week 2):**

* Logic gates, such as AND, OR, and NOT gates, are the fundamental building blocks of digital circuits. By understanding logic gates, you can analyze and design digital circuits, which are essential components of computer systems. In cybersecurity, knowledge of logic gate implementation helps in understanding the behavior of digital systems, identifying potential vulnerabilities, and designing secure logic circuits for tasks like encryption and access control.

**Boolean Arithmetic, Adders & ALU (Week 3):**

* Boolean arithmetic involves performing logical operations (AND, OR, NOT) on binary values (0s and 1s). Adders and ALU (Arithmetic Logic Unit) are components that perform arithmetic and logic operations in a computer. In the context of cybersecurity, these concepts are relevant for cryptographic algorithms, which rely on bitwise operations and logical functions to ensure data confidentiality and integrity.

**Memory (Week 4):**

* Computer memory refers to the storage and retrieval of data during program execution. Different types of memory, such as RAM (Random Access Memory) and cache memory, play important roles in computer systems. In cybersecurity, understanding memory management is crucial for preventing attacks like buffer overflows, where an attacker tries to write data beyond the bounds of a memory buffer to exploit vulnerabilities in software.

**Memory & Machine Language (Week 5):**

* Machine language is a low-level programming language that directly corresponds to the instructions executed by a computer's hardware. Understanding machine language is important for tasks like reverse engineering, where analysts examine the binary code of software to understand its functionality and identify potential vulnerabilities. In cybersecurity, knowledge of machine language helps in analyzing malware, identifying malicious instructions, and developing countermeasures to protect against cyber threats.

**Hack Computer (Week 6):**

* The topic of Hack Computer likely focuses on a specific computer architecture or system known as the "Hack Computer." Understanding the architecture of a particular computer system is valuable in cybersecurity for various reasons. It helps in analyzing the system's strengths and weaknesses, identifying potential vulnerabilities, and designing secure systems. Knowledge of specific computer architectures can also aid in reverse engineering, analyzing malware targeting that architecture, and developing appropriate security measures.