# Safety and Security Engineering

**Similarities:**

The similarities between these fields are due to their problem solving approach and their risk management. Both fields uses the principles of maths and science to solve problems with the objective to create systems that is safe and reliable under different conditions. In terms of risk management, they both aim to prevent safety-related issues like accidents or security-related failures like breaches by both assessing risks and implementing mitigation measures for each.

**Differences:**

Safety Engineering aims to prevent accidents and guarantee the operation of systems prioritizing the anticipation and avoidance of faults to prevent harm to individuals and surroundings. On the hand Security Engineering focuses on safeguarding systems, against attacks ensuring their functionality even in compromised situations. Safety Engineering primarily deals with failures like mechanical issues or human mistakes whereas Security Engineering tackles deliberate threats such, as cyberattacks and hacking.

**Aspects that Refer to Security Engineering:**

Security Engineering focuses on building resilient systems that can continue functioning despite attacks or errors, incorporating redundancies and fail-safes. It involves threat modeling, a systematic process for identifying and prioritizing potential threats, and implementing security policies and mechanisms such as encryption, firewalls, and access controls to enforce these policies. Additionally, security engineering addresses the assurance of how well security mechanisms work together and considers incentives for both defenders and attackers, which can impact a system's overall security.

**Safety Engineering Scenario:**

A good display of safety engineering can be found when enhancing safety in the Sugar Industry of Fiji.

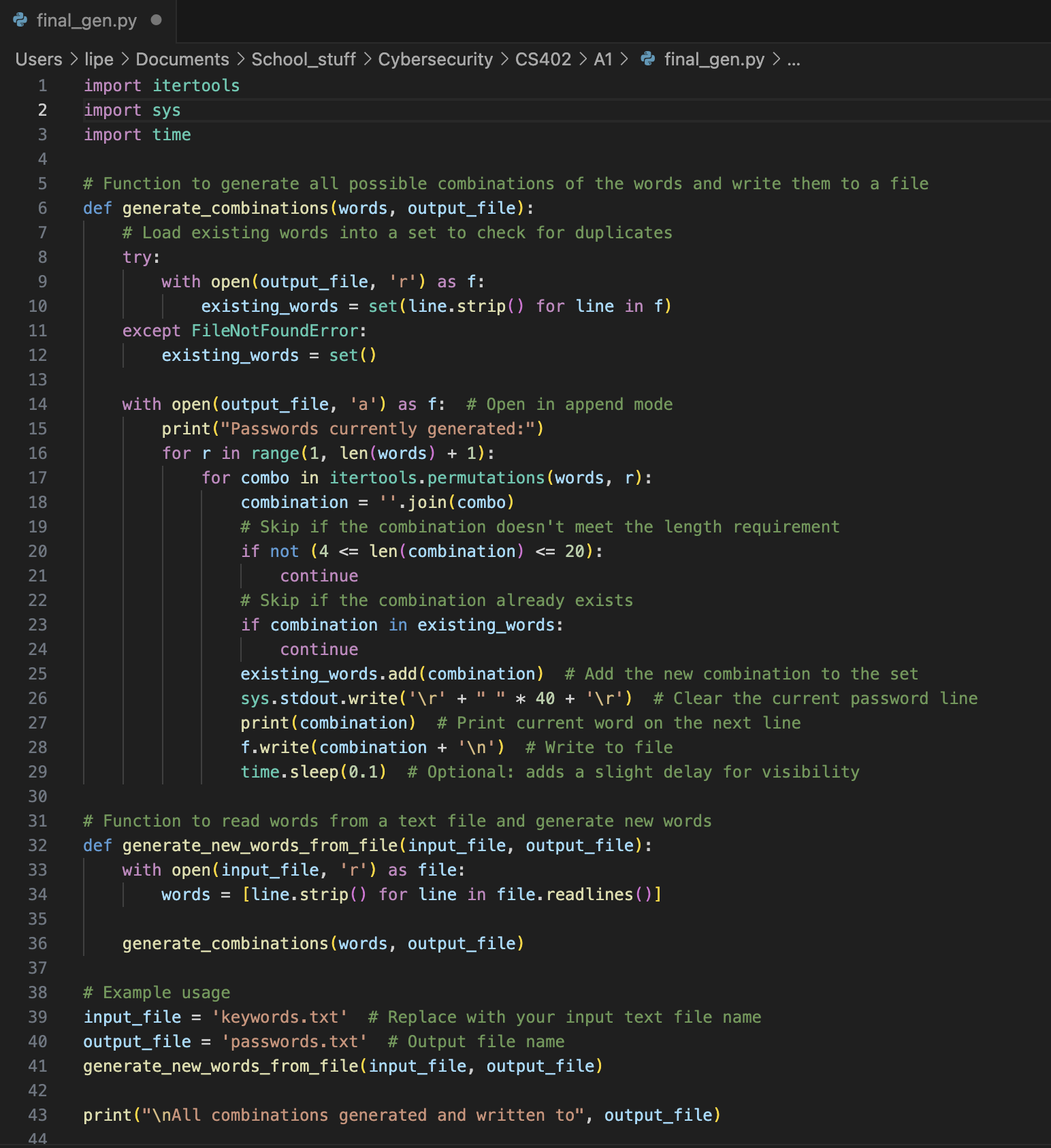
The sugar industry in Fiji plays an important role in providing employment to Fijian citizens. To improve safety measures, engineers have introduced a safety program specifically tailored for sugar mills. This initiative includes inspections, upkeep of machinery and the installation of barriers to prevent accidents. Moreover engineers have devised emergency stop mechanisms for conveyor belts and crushers to safeguard workers from harm in case of entanglement. The primary objective is to minimize the likelihood of equipment malfunctions that could result in injuries or even loss of life thereby prioritizing the well being and security of employees.

**Security Engineering Scenario:**

A good example of the implimentation of security engineering is the Fiji’s banking industries. The Fiji’s banking industry is shifting towards digital platforms such as online banking and mobile banking which makes them a favourable target for cybercriminals. Security experts work on fortifying the safety of these systems by creating secure infrastructure. This includes encrypting data, using intrusion detection tools and conducting vulnerability checks. They also enforce access controls by implementing strict access control mechanisms and predicting possible attack routes, through threat analysis and modelling. The goal is to protect citizens financial information and prevent any breaches that could result in financial harm or economic chaos.

# Social Engineering Practical Attack

Code file for generating the password list. *(4 marks)*



Katherine’s password for the database. *(4 marks)*

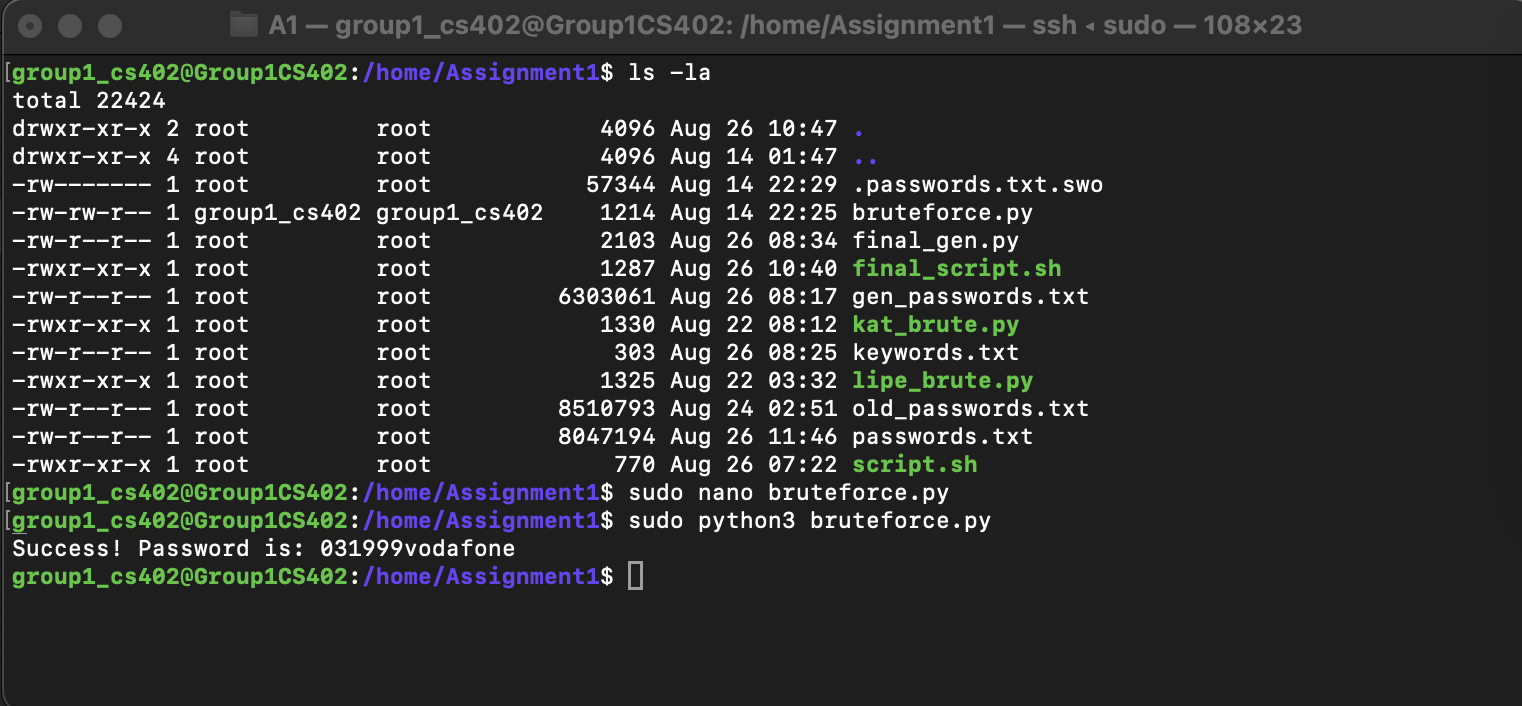
* Foely3103mustang2024

Root users’ password for the database. *(4 marks)*

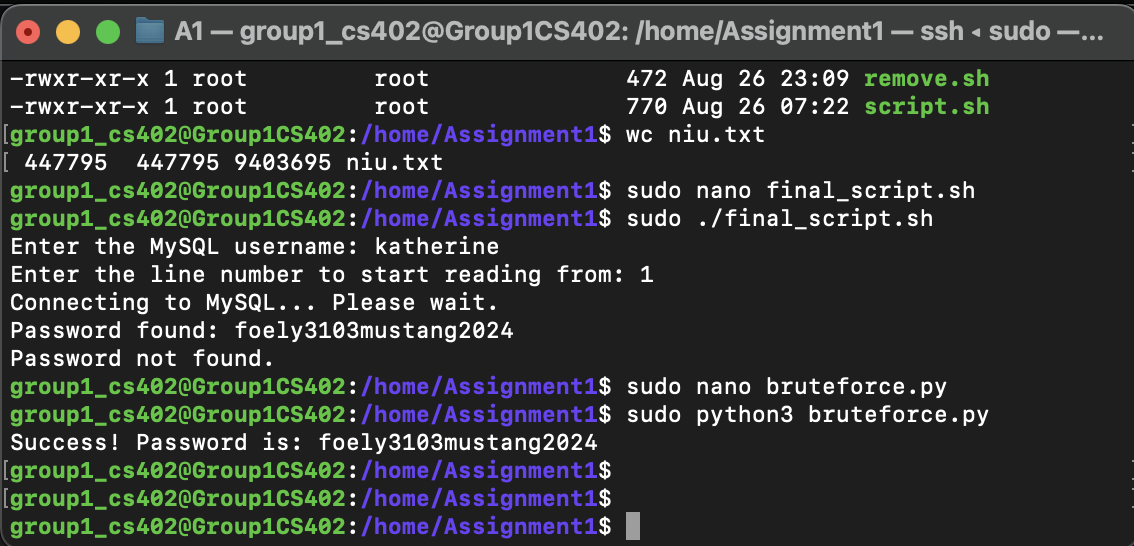
* 031999vodafone

Screenshot of the outputs of the bruteforce.py for *katherine* and *root* users, as evidence that you found the password. *(4 marks)*

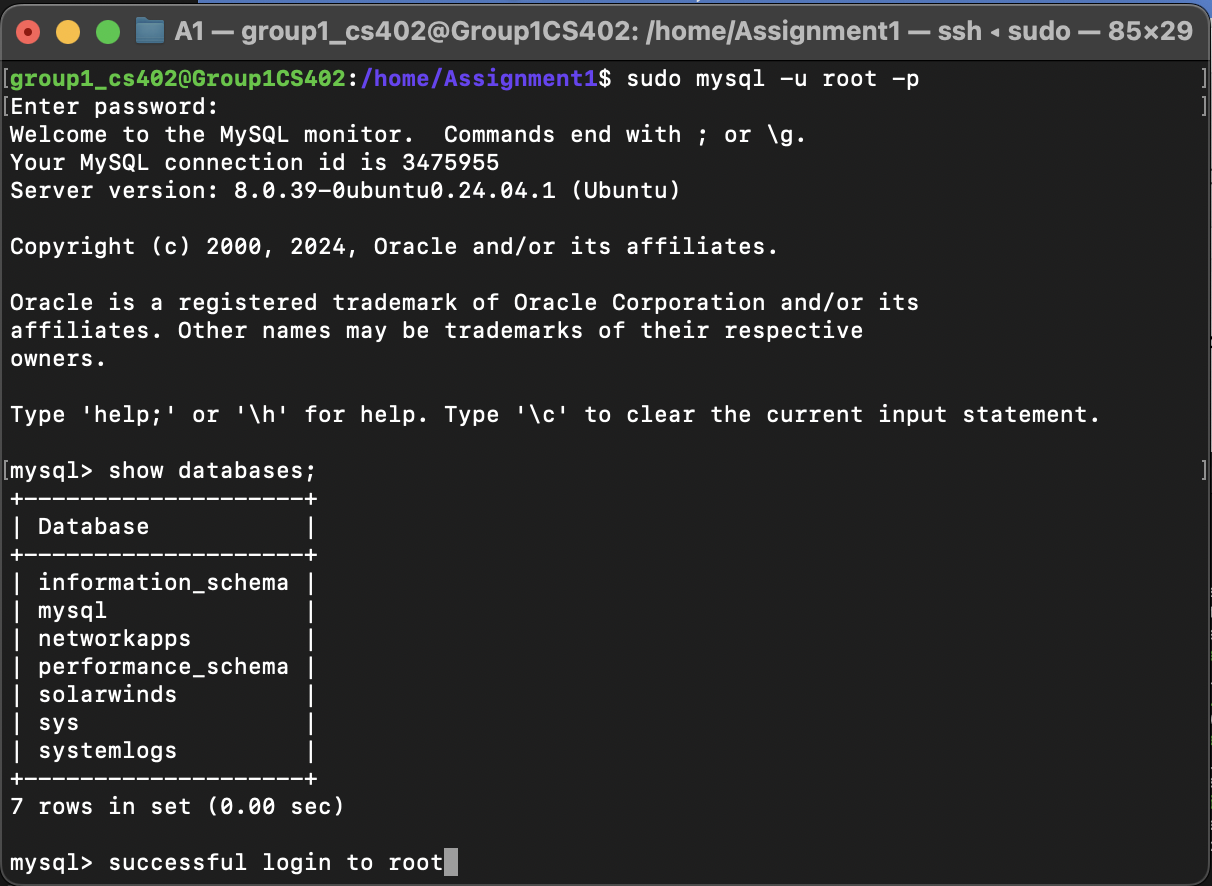
**Root’s Password**



**Katherine’s Password**

****

Login to the database as the root user using the command *mysql -u root -p* and include the output of show databases, command as a screenshot. *(4 marks)*



# Security Goals

**Why does non-repudiation require secure timestamping in many cases? *(2 marks)***

Non-repudiation ensures that an entity cannot deny responsibility for an action. With that in mind, secure timestamping becomes essential in this context as it offers a record of when an action took place. This record helps establish the sequence of events and confirms that a specific entity carried out an action at a certain time. This can prevent arguments over the timing and authenticity of said action which therefore support the principle of repudiation.

In the USP Moodle assignment Dropbox secure timestamping and non-repudiation play a role. Picture a situation where a student hands, in their CS402 assignment, via Moodle Dropbox. Despite the student’s claim that they submitted their assignment on time, the submission record tells a story. To settle any arguments, the USP Moodle Dropbox uses secure timestamping to log the exact date and time of assignment submission. This timestamp serves as a record preventing both the student and teacher from arguing when the assignment was submitted. By acting as a repudiation measure this secure timestamp verifies whether the student kept to the deadline or not thereby maintaining the integrity of the course’s submission guidelines.

**Why is integrity of logfiles important to achieve accountability? *(2 marks)***

Ensuring the accuracy of log files is crucial, for accountability as it ensures that user or system activities are recorded accurately and reliably. If log files are tampered with it becomes difficult to determine who is responsible for actions, which undermines accountability. The ability to trace actions back to their source relies on the integrity of log files. Therefore preserving the integrity of log files is vital, for enforcing non repudiation and creating an audit trail that upholds accountability.

**Why is it very hard to estimate the complete attack surface of a given system? *(2 marks)***

This is challenging due to several factors such as the attack surface comprises of different categories such as network, software and human attack surfaces. Each category with its own set of vulnerabilities and entry points, making comprehensive assessment difficult. The dynamic nature of systems, with regular updates and changes, can create or modify vulnerabilities, complicating the understanding of the attack surface. Unknown or rogue assets, often invisible to security teams, further expand the attack surface. The human factor adds another layer of complexity, as user behaviour can be unpredictable and susceptible to social engineering attacks. The constantly evolving threat landscape, with attackers adapting to new security measures, makes it nearly impossible to predict all potential attack vectors, collectively contributing to the difficulty in accurately estimating the attack surface of a system.

**Someone tells you that you can “just encrypt data” and you can be sure that the following security goals are achieved: confidentiality, integrity, and authenticity. For each goal, explain if the person is right or wrong.**

The person is partially correct, but there are important distinctions to consider regarding the security goals of confidentiality, integrity, and authenticity:

1. Confidentiality: The person is right. Encryption is primarily used to protect data from unauthorized access, ensuring that only authorized parties can read the data. By encrypting data, you achieve confidentiality.

2. Integrity: The person is wrong. While encryption can help protect the data from unauthorized access, it does not inherently ensure that the data has not been altered. Integrity is about preventing unauthorized modification of data, which typically requires additional mechanisms such as hashing. Hashing can verify that the data remains unchanged.

3. Authenticity: The person is wrong. Encryption alone does not guarantee authenticity. Authenticity involves verifying the origin of the data, ensuring that it comes from a legitimate source. This often requires additional measures, such as digital signatures or authentication protocols, to confirm the identity of the sender.

In summary, while encryption is a crucial tool for achieving confidentiality, it does not, by itself, ensure integrity or authenticity. Additional mechanisms are necessary to achieve those security goals.