

|  |  |
| --- | --- |
| Student Number: | 2642159 |
| Programme: | B.Sc Computer Science With International Foundation Programme(Malvern House) |
| Module title: |  |
| Module Code: |  |
| Word Count: |  |

I hereby verify that I have not copied any portion of this task, except for the parts that are directly quoted and properly referenced. I understand that it is against the regulation and rules to plagiarize the work of others without giving proper credit, and I am fully aware that any attempt to do so may result in disciplinary action.

**INTRODUCTION:**

Python is an outstanding programming language that has been used to develop apps and website such as Instagram, drop box, Netflix, Spotify and many more. It has been opined that Python is of more advantage for beginners because of its fewer coding lines and readability. It can be suggested that an advanced knowledge about python makes every other programming language familiar. However, this program was created with the intension of testing students’ knowledge about guessing random numbers.

**AIM/WHAT ARE YOU IMPLEMENTING:**

The "Cows and Bulls" game is a fun code-breaking game. In this game, the computer thinks of a 4-digit secret number, and the player tries to guess it. For each guess, the code-breaker is told how many digits are in the correct position (cows) and how many digits are correct but in the wrong position (bulls).

Cows and Bulls is one of the most popular game often used in computer science education to educate about algorithms and also problem solving techniques. In this game the computer randomly generates a four digit secret number and the player has to guess the secret number. In this game no alphabets are used and no digits are repeated. When we guess a number, the digits of the number guessed also must all be different. If the matching digits are in their right positions, they are "bulls", if in different positions, they are "cows’. And finally when we guess the number we are the winner, else we have to try until our we run out of number of guesses. Later at the end, our score is displayed along with our name.

**ALGORITHM/ PSEUECODE**

Procedure main ():

Step 1: Start

Step 2: Importing random.

Step 3: Display welcome message

Step 4: Ask for player name

Step 5 : Defining the function getDigitis(num)

Step 6 : Defining function ‘noDuplicates(num)’

Step 7 : Defining function ‘generateNum()’

Step 8 : Defining function ‘numOfBullsCows(num, guess)’

Step 9 : Generating the secret code

Step 10: Asking for number of tries

Step 11 : Initialize the score

Step 12: Entering the game loop

Step 13: Displaying the score with the player’s name

**PROCEDURE TO GUESS COWS AND BULLS :**

**Step 1: Determine the Number of Digits**

Step 2: Decide on the length of the secret number (usually 4 digits).

**Step 3: Generate a Secret Number**

Step 4 : The computer thinks of a secret number. The digits must be unique. For example, if the length is 4, a valid secret number might be 1234, and an invalid one might be 1123 (because of the repeated '1').

**Step 5: Make a Guess**: The guesser or the player proposes a number with the same number of unique digits as the secret number.

**Step 6 : Evaluate the Guess**:

* + **Bulls**: A digit in the guess that is in the exact same position as in the secret number.
  + **Cows**: A digit in the guess that is in the secret number but in a different position.

**Step 7: Steps for Each Turn**

1. **Input the Guess**: The guesser provides their guess.
2. **Compare the Guess to the Secret Number**:
   * Count the number of bulls.
   * Count the number of cows.
3. **Provide Feedback**: Tell the guesser how many bulls and cows they have.

**Step 8: Repeat**

1. **New Guess**: Based on the feedback, the guesser makes another guess.
2. **Repeat Steps**: Continue the process of guessing and providing feedback until the guesser correctly identifies the secret number (i.e., all bulls).

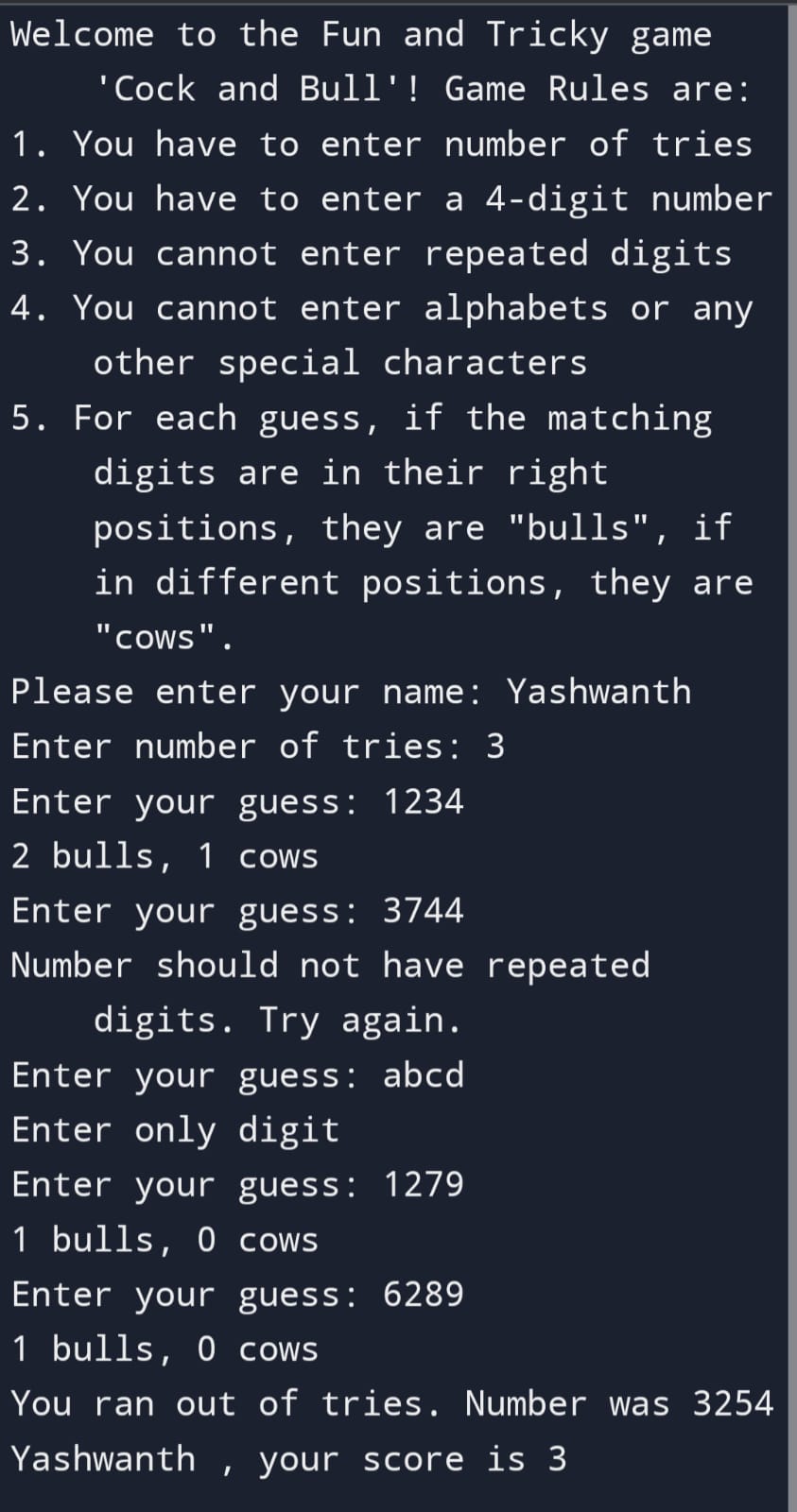
### Step 9: Example

#### **Secret Number: 4271**

1. **Guess 1**: 1234
   * Bulls: 1 (the digit '2')
   * Cows: 2 (the digits '1' and '4')
2. **Guess 2**: 5678
   * Bulls: 0
   * Cows: 0
3. **Guess 3**: 4712

* Bulls: 2 (the digits '4' and '7')
* Cows: 2 (the digits '2' and '1')

**RESULT**



**EXPLANATION:**

The code maker creates a secret code consisting of a sequence of digits or letters (commonly 4 digits long). Each digit or letter should be unique, but variations of the game may allow repetitions.

**Number of Attempts**: Decide on the maximum number of guesses allowed.

**Guessing**: The code breaker makes an initial guess of the secret code. The guess should be the same length and follow the same rules (e.g., unique digits or letters) as the secret code.

### Example

Let's say the secret code is "4271" and the guess is "1234":

* **Bull**: The digit "2" is a bull because it is correct and in the correct position.
* **Cows**: The digits "4" and "1" are cows because they are correct but in the wrong positions.
* **Feedback**: The code maker would say "1 bull and 2 cows."

**FEEDBACK:**

Primarily, after completing my project work, I received feedback from my tutor saying that I can implement more advanced futures such as loops to make my project meets the marking criteria. After completing the project, I asked some of the students to run my project and their response was amazingly great in terms of my project was easy to comprehend and executed as expected.

**What is Malware?**

Malware which is also known as malicious program are software application that are developed with the intension of causing damage to the computer, computer networks, users or gaining unauthorised access to private and confidential information such as bank details, health records, invaluable credential and many more. According to Alenezi et al., (2020), the first malware for PC was created in 1986 by two Pakistan brothers and was called the Brain A virus. This virus was created with the intention of proving that the personal computer was not fully secured. According to Grimes (2001), who opined that this virus affected the floppy disc of the personal computer and was able to replicate itself and attack even newly installed floppy discs. However, making the booting sector of the computer damaged. Since then, the issue about malware attacks have continue up to this 21st century.

**Reasons why cyber criminals uses Malware?**

• Due to the huge financial benefit, they gain from such victims makes such individuals to keep looking for more clients.

• Opportunity to have access into multiple accounts so that they can manipulate individuals and claim false identities.

• Some cybercriminals such as crackers gain access into your information just to destroy them, it might be pay or an unpaid job.

**Distinct types of Malwares?**

* Spyware
* Trojan horses
* Ransomware
* Keyloggers
* Adware
* Viruses
* Worms
* Fileless Malware

**How to protect your computer from Malwares?**

1) Using different Authentication methods: human-chosen passwords can be manipulated but using strong authenticating methods such as biometrics are of great advantage because there are less vulnerable to external attacks. According to Chun-I and Yi-Hui, (2009) It can be opined that using biometrics such as fingerprints and iris scan have no setbacks and can be trusted and dependable for securing data.

2) Protect your personal information’s or credentials private from suspicious online traits using firewall such as Zone Alarm, Windows Firewall, Glass wire, and Comodo Firewall: Malware attackers has created a new method of developing false website that generate your information when you sign into such website using your name, password, and email they use such advantage to bypass your security and gain access into your credentials (Salahdine and Kaabouch, 2019). Meanwhile such gained private, sensitive, and confidential information are used to extract valuable requirement such as money. When you fail to meet up to such demands you are been threaten that such information will be disclosed or destroyed.

3) Always prevent malware by using anti-virus: Globally technology has advanced, and computer cyber securities and programmers are also reenforcing methods of protecting our systems by developing Anti-virus software’s and cryptographic key for verification that detects and remove any malware found or trying to get into the system. Despite how advantageous it is not everyone will be able to buy such anti-virus and keep on subscribing to it, but it is of more advantage if the public will have access to free anti-virus software such as Norton anti-virus, McAfee anti-virus, comodo anti-virus, F-Secure anti-virus etc.

4) Keep all software applications up to date: It is important that application users monitor their software’s and ensure its always up to date. This enables such individual to benefits from the updated security of such software’s. 5) Engage a good browser judgment intelligence: It can be suggested that hackers and crackers that get involve into malevolent activities are people who have studied or practices computer related course such as computer security, computer engineering, data science, information technology, web development. Due to the huge benefits of malevolent activities decides to go into malware. It is of vital value that individuals always apply advance judgement intelligence before opening any website or accepting any invitation links from unknown sender.

**REFERENCES**

1.Alenezi, M.N., Alabdulrazzaq, H., Alshaher, A.A. and Alkharang, M.M., 2020. Evolution of malware threats and techniques: A review. International journal of communication networks and information security, 12(3), pp.326-337.

2. Fan, C.I., and Lin, Y.H., 2009. Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics. IEEE Transactions on Information Forensics and Security, 4(4), pp.933-945.

3.Grimes, R.A., 2001. Malicious mobile code: Virus protection for Windows. " O'Reilly Media, Inc.".

4 .R. Pascanu, J. W. Stokes, H. Sanossian, M. Marinescu and A. Thomas, "Malware classification with recurrent networks," 2015 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), South Brisbane, QLD, Australia, 2015, pp. 1916-1920, Doi: 10.1109/ICASSP.2015.7178304.

5 .Salahdine, F. and Kaabouch, N., 2019. Social engineering attacks: A survey. Future Internet, 11(4), p.89.