UNIVERSITY OF WOLLONGONG AUSTRALIA

Assignment

Due: 11:55 pm 28 May 2023
Total Mark: 100 (20% of Final Mark)

Please read the questions carefully.

Q1: (40 points) In this task, you compare GDPR and Australian Privacy Act. Gather relevant information about GDPR and Australian Privacy Act as much as you can and write a case study report including the following contents:

- Summary
- Overview of GDPR and Australian Privacy Act
- Comparison between GDPR and Australian Privacy Act (Differences and similarities should be specified.)
- Your thoughts on the difference between GDPR and Australian Privacy Act
- References

* There are articles comparing the two pieces of legislation, available from the Internet. You can refer to them, but proper citations must be made. (Failure to do so may be regarded as plagiarism.)

To get full marks for this question, you need satisfy the following requirements.

Requirements:

- The length of your report should be 1500 – 1800 words *excluding references*.
- Your report should be single-spaced with font size 12 and be typed using MS Word.
- Name your report as `Q1.doc` or `Q1.docx`.

Your report will be marked based on presentation, clarity, structure and succinctness of the report contents.

Q2: (60 points) In this task, you write a Python program that implements the requirements described in the following scenario.

- **Scenario**
  Suppose that Alice sends a zip file that compresses her message to Bob. The zip file is protected as it is locked with the password that Alice has chosen. Of course, Alice does not want the password to be revealed to anyone. So, Alice decides to encrypt the password (for the zip file) using a symmetric encryption scheme that takes four-digit PIN as input to create a secret symmetric key and encrypts the password (That is, the password for the zip file is considered as a message for the symmetric encryption scheme.); and to send the resulting ciphertext along with the protected zip file to Bob. Let us call the resulting ciphertext "PWDCiphertext". Since Alice told Bob what the four-digit passcode was over the phone, Bob could decrypt the received

PWDCiphertext and get the password for unlocking the protected zip file to recover Alice's message. However, Charlie, the hacker, was able to capture PWDCiphertext and crack the password to unlock the protected zip file! Now, Alice's message to Bob is at Charlie's hand too.

- Your task

Your task is to write a Python program for Charlie to crack the password for the protected zip file from PWDCiphertext. Once you have found the password the protected zip file, unzip it and recover Alice's message.

To complete the above task, three files are given in the assignment folder on Moodle:

- `protected_file.zip`: This is the protected zip file that compresses Alice's message (to Bob) using the password Alice chose.
- `PWDCiphertext.text`: This is the ciphertext that encrypts the password. (In other words, PWDCiphertext is created by encrypting the password for the protected file.)
- `EncryptPWD.py`: This is the Python code for encrypting the password for the protected file. Note that a 4-digit PIN is used as a symmetric key to encrypt the password (for the protected file) in this encryption program.

To get full marks for this question, you need satisfy the following requirements.

Requirements:

- You need to modify the given code Q2_start.py to write your program. After completing code, you rename it to `Q2_answer.py`.
- Your code should be able to output the found PIN (4 digit) and the password for the protected file *on screen*.
- Write a one-page report (in MS Word format), which must include Alice's message (i.e., unzipped protected file) and why it was possible to crack the password from PWDCiphertext even if we use the strong symmetric encryption from Python cryptography module (i.e., Fernet encrypt).
- Your program must be compliable using Python3. Compilation failure will result in at least 50% of deduction of the marks.
- Name your report `Q2_readme.doc` (or `Q2_readme.docx`).

How to submit

Put all your files (`Q1.doc`, `Q2_answer.py` and `Q2_readme.doc`) to one folder named as your surname followed by your student ID number (e.g. John12345). And compress this folder to make one **zip** file. Submit your (zip) file through Moodle. (Not compressing your files with zip may result in the reduction of at least 10% of your total mark. If you do not use zip to compress, you will lose the mark. – Do not use **rar** or any other compression algorithms.)