# CSC 106 - SPRING 2016
# THE PRACTICE OF COMPUTER SCIENCE
# ASSIGNMENT 1
# UNIVERSITY OF VICTORIA

**Due**: Tuesday, January 19th, 2016 at 11:00am.

**Submit your answers on paper to the CSC 106 drop box on the second floor of ECS. Answers must be well formatted and legible or they will not be marked. Answers which include research from the internet or paper sources must cite all sources used (using the work of others without proper citation is considered plagiarism).**

**Question 1**: Security and Privacy [15 marks]
In the past few years, as people increasingly expect a variety of different devices (smartphones, tablets and computers) to have to access to all of their data, there has been a trend towards storing data 'in the cloud', which allows it to be accessed quickly and easily over the internet from any device. Services such as Google Drive, Dropbox and iCloud (among many others) allow arbitary information to be stored online and accessed anywhere. All of these services advertise themselves as 'secure'. Choose a free cloud storage service (which may be one of the ones above) and describe, in a few sentences, how it compares to storing data on your own device (such as your laptop) in terms of the confidentiality, integrity and availability triad discussed in class.

**Question 2**: Counterfeit Money [20 marks]
For a counterfeiting operation to be successful, it is only necessary for the counterfeit money (such as fake $20 bills) to appear convincing to certain members of the public (such as store cashiers), who may not be experts in authenticating money. Historically, one of the main obstacles to producing counterfeit money was the lack of a convenient duplication mechanism. Before the spread of photocopying technology, the only way to mass-produce arbitrary documents was to create new lithographic plates, which was time consuming and error-prone. Early photocopying and digital printing equipment also could not produce sufficient detail to generate convincing forgeries. However, printing technology has advanced to the point where extremely high resolution printers and photocopiers are inexpensive and widely available. Anti-counterfeiting measures have advanced as well. One major change in Canadian money has been the introduction of 'plastic' banknotes instead of paper. However, the older paper Canadian bills are still valid, and American money is still printed on paper.

High-end colour photocopiers and printers may be able to produce accurate duplicates of paper-based bills. However, if you attempt to photocopy recent banknotes of most major currencies (such as the Canadian dollar, the American dollar, the Chinese yuan and the Euro) with a high resolution colour photocopier, the machine will refuse to perform the operation. Image editing programs such as Photoshop will also refuse to edit scanned images of banknotes.

Do some research and answer each of the questions below. Each answer should only require one or two sentences.

(a) How do photocopiers recognize that a document is a banknote? What about cases where the banknote in question did not exist when the photocopier was built? For example, would a photocopier from 2009 be able to recognize and reject a 2011 Canadian $20 bill?
(b) What about 'false positives'? Under what circumstances would a photocopier mistakenly recognize a non-currency document as a banknote and refuse to copy it?
(c) As mentioned above, the American $20 bill is still printed on paper. Suppose a high-resolution photocopy of an American $20 bill was produced. How could the forgery be detected?

**Question 3**: Vigenère Cipher [25 marks]
Recall that a Vigenère cipher takes a plaintext string containing English letters and a key containing English letters, and uses each character of the key to shift the value of the corresponding character of the plaintext. The character '`A`' in the key results in a shift of 0 positions and the character '`Z`' results in a shift of 25 positions. If the key is shorter than the plaintext, it is repeated as necessary.

(a) Encrypt the string '`TECHNOLOGYISAMAZING`' using a Vigenère cipher, using **your last name** as the key (convert every letter to uppercase and remove any spaces or diacritic marks). For the convenience of the marker, please clearly indicate the exact version of your name you are using as the key. Provide the complete ciphertext after encoding.
(b) Was the key you used in part (a) secure? Why or why not?
(c) Suppose the string '`TECHNOLOGYISAMAZING`' is the ciphertext produced by a Vigenère cipher. Provide the plaintext after decrypting the string using the key '`RQQSTVHXOYROGUWOEVO`'.
(d) Find a 9 letter key which encodes the plaintext '`RASPBERRY`' to the ciphertext '`CHOCOLATE`'.