CPSC 418 / MATH 318 — Introduction to Cryptography
ASSIGNMENT 1

Name: Crypto Wizard (replace by your name)
Student ID: 0000000 (replace by your ID number)

Problem 1 — Superencipherment for substitution ciphers, 12 marks

(a) i. *Replace this text by your solution to part (a) i of Problem 1..*
ii. *Replace this text by your solution to part (a) ii of Problem 1 etc.*

(b)

Problem 2 — Key size versus password size, 21 marks]

(a)

(b) i.
ii.

(c)

(d)

(e) i.
ii.

Problem 3 — Equiprobability maximizes entropy for two outcomes, 12 marks

(a)

(b)

(c)

Problem 4 — Conditional entropy, 12 marks

(a)

(b)

(c)

Problem 5 — Perfect secrecy and joint entropy, 43 marks

***** Remove the text for this problem if you don't attempt it. *****

(a) i.
ii.
iii.
iv.

v.

(b) i.

ii.

iii.

iv.

v.

vi.

vii.

Problem 7 — Mixed Vigenère cipher cryptanalysis, 10 marks

***** Remove the text for this problem if you don't attempt it. *****