Problem Set 1

1. Decipher the following message. You should assume it was enciphered using a monoalphabetic substitution cipher.

EN VCOCGHCP CEQXDCCN DXEPDM-NENC, BUC EWWKCV A OXAZZCNQC DU DXC PCAVCPW UJ

DXC BXEZAVCZBXEA BABCP AZCFANVCP'W YCCSZM DXAD XC OUKZV WUZRC ANM WEGBZC

WKHWDEDKDEUN OEBXCP DXCM WKHGEDDCV. XC BPUOCCVCV DU WUZRC AZZ UJ DXCG,

ENOZKVENQ UNC EN YXEOX WCRCN VEJJCPCND AZBXAHCDW YCPC KWCV.

2. In a paragraph or two, describe the strategies you used to decipher the message above. How did you start figuring out the cipher alphabet? What patterns in the cipher alphabet did you notice that led you to determine the particular substitution cipher used? What other steps did you take as part of your cryptanalysis?

3. Fill in the blanks in the following table. Some of the blanks can be filled in using more than one number, but the rows of your table should be internally consistent.

x	x MOD 5	x MOD 6	x MOD 12
10			
-15			
	1	3	
	0		2
	1	1	1

4. Find five numbers (three positive, two negative) that, when substituted in the following congruence statement for x, make the statement true.

    $x + 12 \equiv 5 \pmod 8$

5. The 30-letter Coptic alphabet is a variant of the Greek alphabet developed when Greece conquered Egypt in the 3rd century BC[1]. It consists of all 24 letters of the Greek alphabet, as well as six addition letters representing sounds not used in Greek. How many unique decimation ciphers are there for the Coptic alphabet? *Justify your answer.*

---

[1] Ager, S. (2010). Coptic alphabet, pronunciation, and language. http://www.omniglot.com/writing/coptic.htm.