Cryptography Assignment 1

After completing `Cryptography` *you have been hired by a government agency in Canberra, which believes that members of American Literature Departments at Australian Universities are using enciphered messages to hide terrorist activities. Fortunately, due to educational cutbacks, they were only able to hire a student who completed the first weeks of* `Cryptography`*, and who is unaware of the weaknesses of classical ciphers. Your supervisor presents you with the following problems before promoting you to more challenging tasks within the agency.*

1. (2.5 marks) [Vigenère cipher] You suspect that the first ciphertext uses a Vigenère cipher. Find the deciphering key and plaintext.

2. (2.5 marks) [Substitution cipher] The second ciphertext has a standard coincidence index for English, and you suspect a simple substitution cipher. Find the deciphering key and plaintext.

3. (2.5 marks) [Information theory] Your supervisor presents you with a model cryptosystem, giving the probabilities of each the plaintexts and a specification of the enciphering algorithm. Find the entropy of the plaintext space, key space, and ciphertext space, and the conditional entropy of the cryptosystem.

4. (2.5 marks) [Product cipher] After recognizing the weaknesses of previous ciphers, the cryptosystem suddenly changes, and your supervisor believes that the University Junta is now using product cipher, composing substitution and transposition ciphers. Find the substitution key, the transposition key, and the plaintext message.

Individual data for this assignment can be accessed from the course home page. Answers to the assignment should be submitted by Friday 2 February 2007, following the directions on the course home page.