MAS433 Cryptography: Assignment 1
Deadline: 10:30am 08.10.2010

Instructions.

1. This assignment consists of two questions.
2. 50 marks for each question.
3. Submit your answers to the instructor before 10:30 am, 08 October 2010 (Friday). You can submit the paper version, or email your answeres to the instructor (wuhj@ntu.edu.sg) with the email subject "MAS433 Assignment 1 Answers".

Q1. Attack Vigenere cipher
1.1. Describe the methods to attack Vigenere cipher using ciphertext-only attack, i.e., how to determine the key length using two different methods, and how to determine the key value. (25 Marks)
1.2. Develop a new method to determine the key length using entropy instead of using the index of coincidence. (Hint: consider the entropy of single letters.) (25 Marks)

Q2. CBC mode
Let the letters A, B, C, D, E ... Z be represented as 0, 1, 2, 3, ... 25.
2.1. We define the encryption of Vigenere cipher in CBC mode as $c_i = (k_{i \bmod m} + p_i + c_{i-1}) \bmod 26$ for $i \geq 0$, with c_{-1} being the IV (a random letter). Briefly describe the ciphertext-only attack against this encryption scheme. (25 marks)
2.2. We define the encryption of substitution cipher in CBC mode as $c_i = S((p_i + c_{i-1}) \bmod 26)$ for $i \geq 0$, with c_{-1} being the IV (a random letter). How to attack this encryption scheme (ciphertext-only attack)? (25 marks)