300128 - Information Security

Tutorial and Lab Practice - Week Two (follows lecture 1 & 2)
This work will be marked in Week Four during lab. session **(4%)**

Read text book and review the terminology introduced

Reading chapters:

For general reading:

- Chap1.1 Computer security concept
- Chap1.2 The OS security architecture
- Chap1.3 Security attacks
- Chap1.4 Security services
- Chap1.5 Security mechanisms
- Chap1.6 Fundamental security design principles
- Chap1.8 A model for network security
- Chap1.9 Standards

For the tutorial work:

- Chap3.1 Symmetric cipher model
- Chap3.2 Substitution techniques
- Chap3.3 Transposition techniques
- Chap3.5 Steganography

Tutorial

1. Find the secret message hidden in the following paragraph.
   Susan eats truffles. Under pressure, that helps everything before owning Major Bullwinkle. **(1%)**

2. Encrypt the plaintext "SECURITY" by using the following methods. Use letter"Z" as a padding letter if necessary.

   [i] Caesar Cipher with the key=3.

[ii] a keyed monoalphabetic cipher (refer to noteP16, lecture 2) with the key = ATTACK. **(1%)**

[iii] The substitution table is constructed by listing the alphabet row by row, reading off column by column from a six column rectangle. **(1%)**

Lab Practice

1. Write a program to implement the Caesar Cipher for both encryption and decryption. Your program should be able to encrypt or decrypt a sentence and handle different keys by deciding the key at run time. **(1%)**