## NWEN243 Assignment One

- 1. Steganography: The hiding of a secret message within an ordinary message, and the extraction of it at its destination.
  - Cryptography: The method of storing and transmitting data in a form that only people who are allowed to read it can read it.
  - The difference is that steganography takes cryptography futher by hiding an encrypted message so that no one knows the message exists.
- 2. Original Caesar cipher uses just one letter/offset and applies that to every letter in the message.
  - Using the keyword Caesar cipher applies a word to the beginning of the alphabet and the rest of the remaining letters are applied to the end of the keyword.
  - the method to crack both cipher schemes is the same, using letter frequency in the message and comparing to frequency analysis of the language.
- 3. Monoalphabetic used only one cypher alphabet, whereas polyalphabetic ciphers use two or more cypher alphabets so that the substitution depended on both the letter and its position.
- 4. AVYUL HWLEE UCZLL LTYVI YOFJI ZSLNI ICUJH ZOCVC LGNWV KOSLL HOUSE ATATA XINCR EASEI SNEED EDNOW
  - The Chairman of the federal reserve board said yesterday that a tax increase is needed now.
- 5. Split the cypher text into separate monoalphabetic cypher texts and apply frequency analysis to each part separately.
  - recombine and apply grammatical and word structure knowledge.
  - keep trying by spltting the message into more and more separate parts, depending on how many alphabets are used. (practical limit to how many keywords would have been used).