**Overview**

**Definitions:**

* Steganography: the science of hiding a message
* Cryptography: the science of encrypting a message
* Code: a system for replacing each word with another word or string of characters, as specified in a codebook.
* Cipher: any general system for hiding the meaning of a message by replacing each letter with another letter
* Plaintext: the original message before encryption
* Ciphertext: the message after encipherment
* Encrypt: to encipher or encode (knowing the key)
* Decrypt: to decipher or decode (knowing the key)
* Cryptanalysis: deducing the plaintext from a ciphertext, without knowing the key
* Transposition cipher: a system of encryption in which each character changes its position within the message
* Substitution cipher: a system of encryption in which each character is replaced with another character

**Code breaking:**

* Brute force: try all possible keys
* Word frequency analysis
* Word dictionary matching
* Guessing parts of the ciphertext
* Regular expressions
* Language model
* Spying

**Caesar Cipher: Assignment 1**

* Original version: given a key between 0 and 25, and a string of letter that follows alphabetic order, and a string of plaintext. The key indicts how many position does the current letter suppose to shift.
  + If the key is 1, ­any A in the plaintext become B in the ciphertext
  + If the shift amount add up more than 25, we use 26 – the shift amount to get the actual shift number.
* Updated version: give a letter key, this key only change the first letter of the plaintext, and the following letter change based on the plaintext letter of the previous.