**Cryptography**

* What is Cryptography?
  + Cryptography or cryptology from Wikipedia is defined as “the practice and study of techniques for secure communication in the presence of third parties called adversaries”. (summarises the idea well)
  + throughout history cryptography has always been necessary as there is an inherent need for people to communicate in secret. Cryptography before the modern age was almost exclusively referring to encryption, which is a process of converting a plaintext (ordinary text) to ciphertext (unintelligible text). Modern cryptography, on the other hand, is split into multiple areas of study. The main ones include: ciphers (which includes classical ciphers and modern symmetric and asymmetric key algorithms); Cryptanalysis; cryptographic primitives; cryptosystems. Cryptography today is a foundational aspect of our modern lives and without it much of what we take for granted could not exist.
* What are Ciphers? (maybe)
  + Once again Wikipedia offers a nice summary: “In cryptography, a cipher (or cypher) is an algorithm for performing encryption or decryption”
  + Basically, ciphers are different methods of encrypting a message so that unauthorised people cannot read the information.
  + Ciphers and codes are technically an entirely distinct concept within cryptography despite them being relatively similar in definition.
    - A code is a method of converting a group of words or phrases into another words or phrases
      * For example, if I want to write “parasite” I would have a codebook in which it may have “parasite” labelled as “23463” therefore I would send “23463” as the message
      * Codes will usually have a codebook in which lays down the rules of how messages will be converted into the encrypted message
      * Another example would be something like if a word is repeated in a sentence it would modify the meaning of the sentence
    - A cipher is a method of converting a message on a letter by letter (bit by bit) basis
      * For example, “hello” could be turned into “8 10 36 48 75” by converting the letters into their corresponding numbers and then multiplying the numbers by their positional values that is 8 is multiplied by 1, 5 by 2, 12 by 3 and so on.
  + The operation of a cipher will usually rely on an extra piece of information known as a key. A cipher must be made so that without this key the ciphertext is extremely hard to decipher back into plaintext.
  + Ciphers can be separated into 2 eras: classical and modern.
    - Classical ciphers
      * Classical ciphers are ciphers that can be easily (relatively) done using a pen and paper. These are simple ciphers such as substitution ciphers and transposition ciphers. Simple substitution ciphers are monoalphabetic meaning they only use one substitution to create the ciphertext. These were replaced with polyalphabetic substitution ciphers such as the Vigenère cipher.
    - Modern ciphers
      * Modern ciphers can be divided into 2 main categories
        + By type of key used

Symmetric key algorithms (Private-key cryptography)

One key is used for both encryption and decryption

Asymmetric key algorithms (Public-key cryptography)

There are different keys (2 keys) used to encrypt and decrypt

* + - * + By type of input data

Block ciphers (input data is of fixed size)

Stream ciphers (input data is continuous streams of information)

* Origins of Cryptography
  + Earliest uses
  + Special important usages
  + Modern uses (difference between classical cryptography and modern cryptography)