CRYPTOLOGY

Warm up:

What is cryptology?

DEFINITION

Cryptography => the science (art) of encryption

Cryptanalysis => the science (art) of breaking encryption

Cryptology => cryptography + cryptanalysis

Objectives of Information Security

- Confidentiality (secrecy)

  Only the sender and intended receiver should be able to understand the contents of the transmitted message

- Authentication

  Both the sender and receiver need to confirm the identity of other party involved in the communication

-

Objectives of Information Security

Data integrity

The content of their communication is not altered, either maliciously or by accident, in transmission.

Plain Text   -----------Encryption --------------> Cipher Text

Ciphertext-------------------Decryption------------------>Plain Text

How will the receiver know how to decrypt?

Simple Substitution

substituting every plaintext character for a different ciphertext character.

plain alphabet : abcdefghijklmnopqrstuvwxyz
cipher alphabet: phqgiumeaylnofdxjkrcvstzwb

Ex: Plain Text: Cryptography

Cipher Text: qkwxcdmkpxew

Encrypt this!

plain alphabet : abcdefghijklmnopqrstuvwxyz

cipher alphabet: phqgiumeaylnofdxjkrcvstzwb

giuifg cei iprc tpnn du cei qprcni

Solution!

plaintext : defend the east wall of the castle

Practice

Program Substitution Cipher in Python. Ask the user whether they want to encrypt or decrypt. Take the plain text as input and output the cipher text or Vice versa.

Double encrypt/ Decrypt. Encrypt first time with a key and take the cipher text and use a different key to encrypt it again .