CRYPTOGRAPHY

Artemis 2017

HELLO!

Dara, Mira, and Pia

We are going to be talking about Cryptography today!

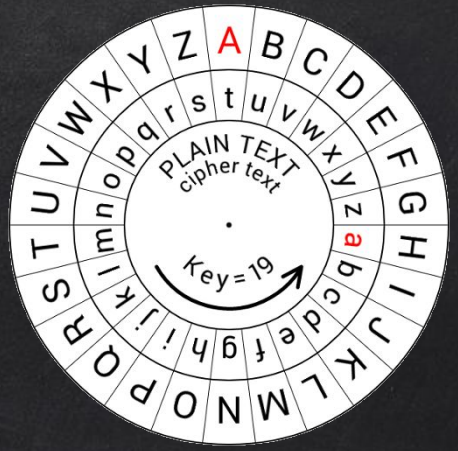
What is cryptography?

Cryptography is the science of writing in secret code.

The History of Cryptography

Cryptography is an ancient art form. It was first documented in 1900 BC in ancient Egypt.

Cryptography was developed with the advancement of technology with computers encoding and decoding secret messages.



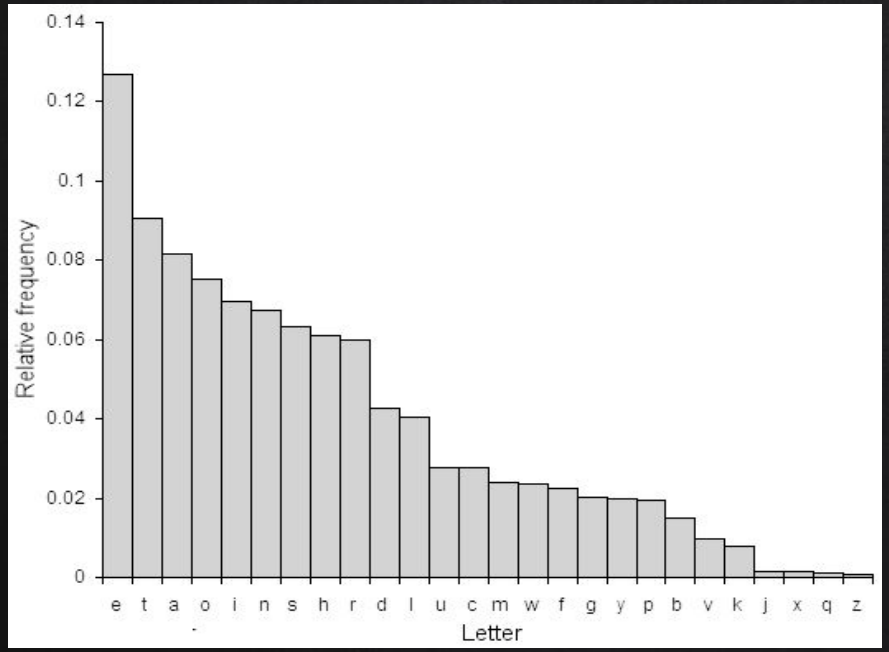
What is the Caesar Cipher Shift?

The Caesar Cipher shift is an encryption method where all letters in a message are shifted over a certain amount of times

Artemis BU is great → Duwhplv EX lv juhdw

Shift of 3

Frequency of letters



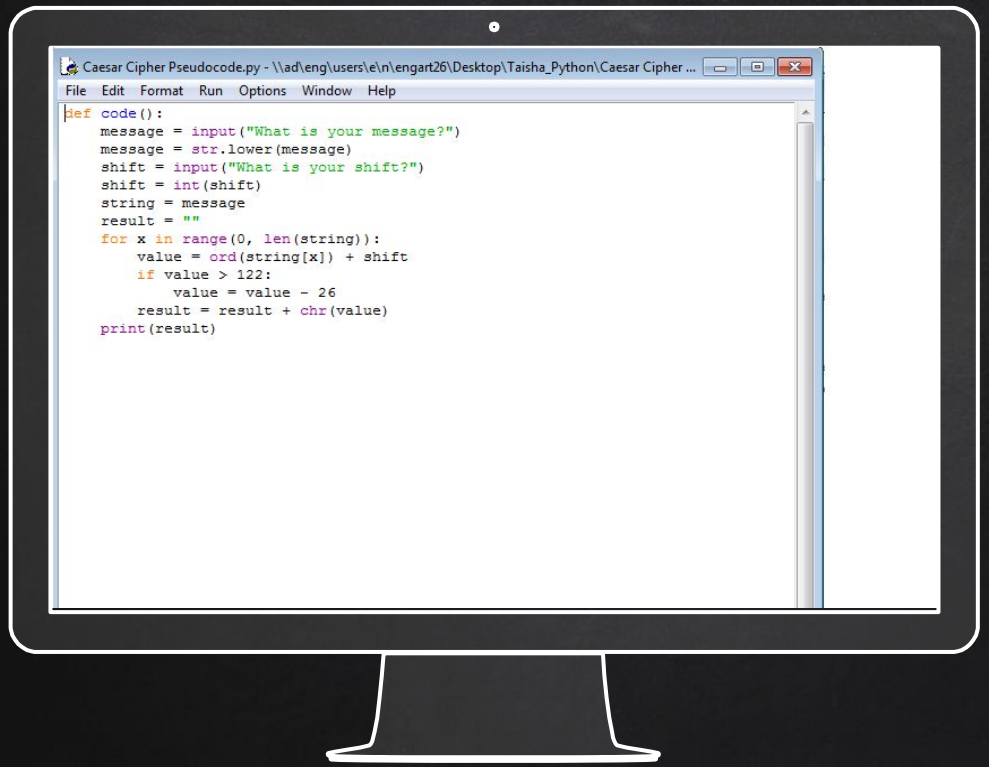
A longer message is easier to decrypt.

Encoder/Decoder

Encoder: transfers your message into code

Decoder: transfer your coded message into the original

Python Encoder and Decoder

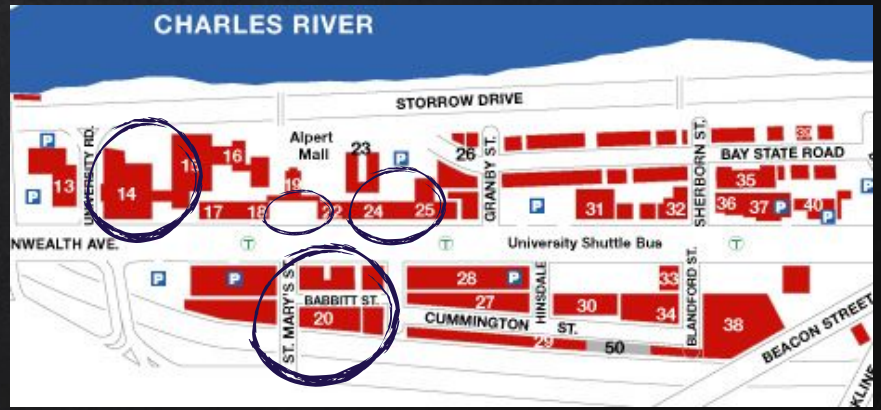


This is the encoder. It will ask you what your code is and then how many letters you want to shift it.

We had to transfer the number values of letters into strings for this code to work

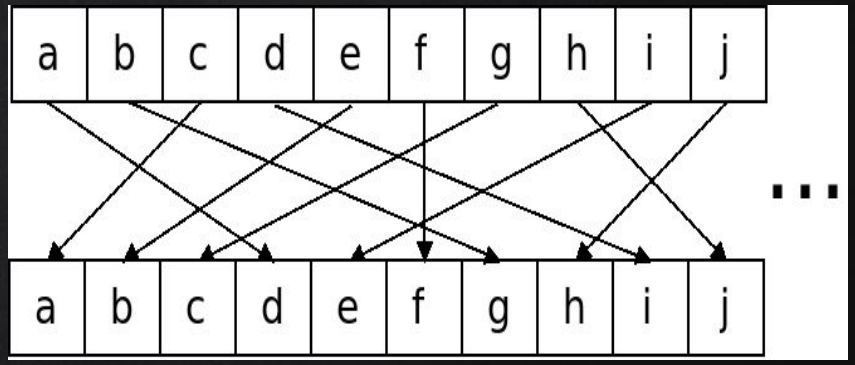
Cryptography Scavenger Hunt

- ✘ We were split up into 4 teams and given a coded message with an assigned shift
- ✘ The coded messages lead us to different areas around the BU Campus
  - This included the CAD lab, the GSU, the meeting area, Marsh Plaza and to finish the lecture hall



Substitution Cipher

- ✘ Each letter in the alphabet is randomly assigned another letter
- ✘ Hard to decode
- ✘ Uses frequency analysis



Using this code the word high would change to jecj

Private Key

Both people participating have the same key.

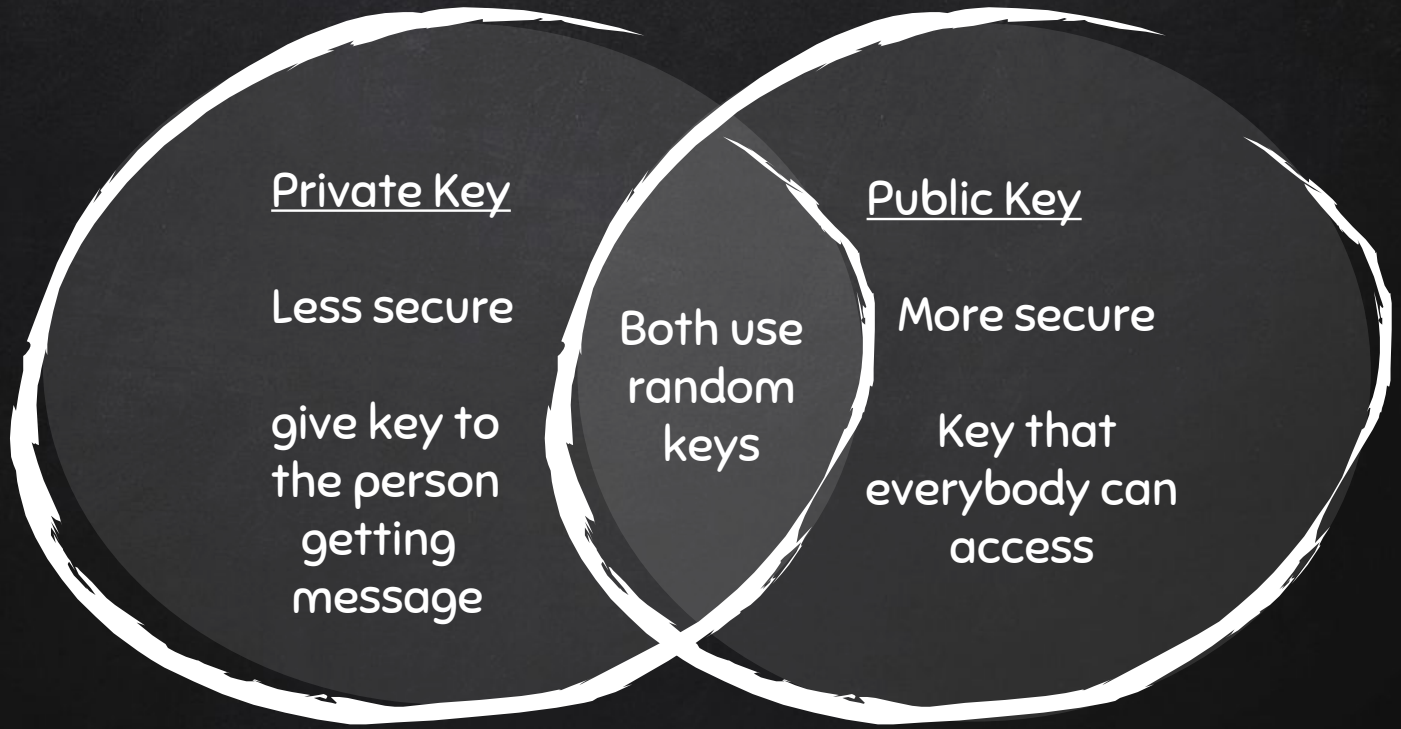
1. The sender encodes the message using the key
2. The receiver uses the key to decode the encoded message
3. The receiver ends up with the intended original message

Public Key

Each person who participates in the exchange has their own key.

1. Both people encrypt the message using the public key and his/her own key then sends the encrypted message to the receiver
2. Each person receives the message and applies their own private key
3. Now both people have the same message that was encrypted using both private keys and the public key

Public Vs. Private Key



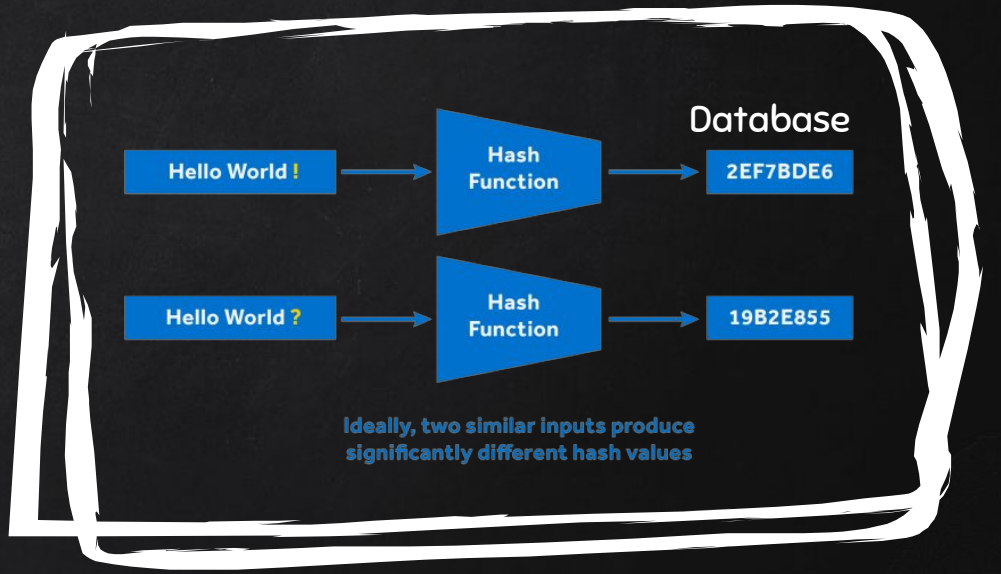
Hash function

Hash function is a cipher that is impossible to decrypt.

A hash is an encrypted message. It is randomly generated.

Hash function is used for saving passwords. Every time you type in your password, the computer sees the hash, rather than your actual password.

The computer looks in the database to find if the hash matches another hash.



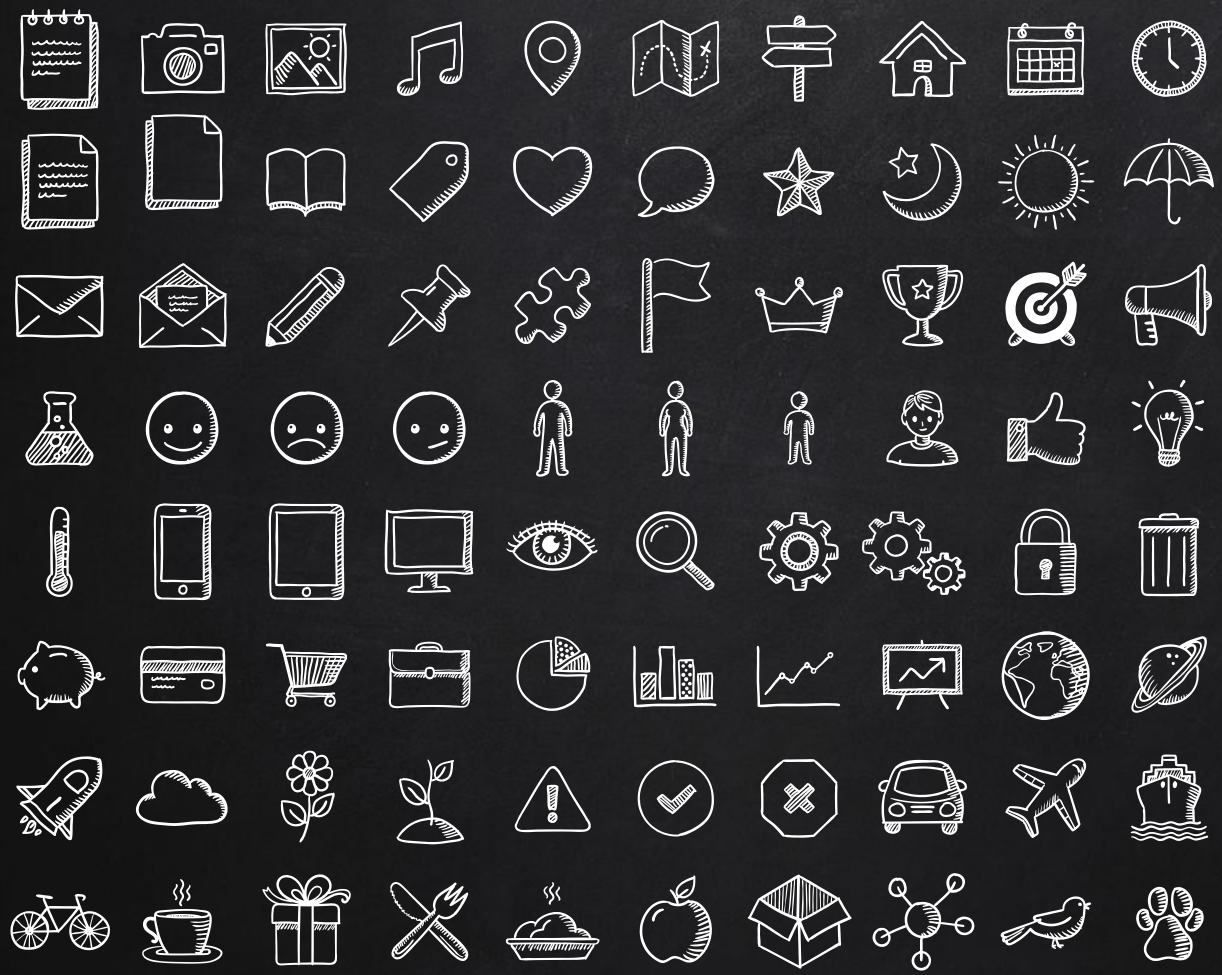
THANKS!

Any questions?

Credits

Special thanks to all the people who made and released these awesome resources for free:

- ✘ Presentation template by SlidesCarnival
- ✘ Map of BU: BU Campus Map
- ✘ Hash Function: GRA Quantum
- ✘ BU Campus: Dennis Lab
- ✘ Caesar Cipher: Reddit



SlidesCarnival icons are editable shapes.

This means that you can:

- Resize them without losing quality.
- Change fill color and opacity.

Isn't that nice? :)

Examples: