Week 4 - Friday

COMP 1800

Last time

- What did we talk about last time?
- Substitution cipher
- Generating a random key

Questions?

Vigenère Cipher

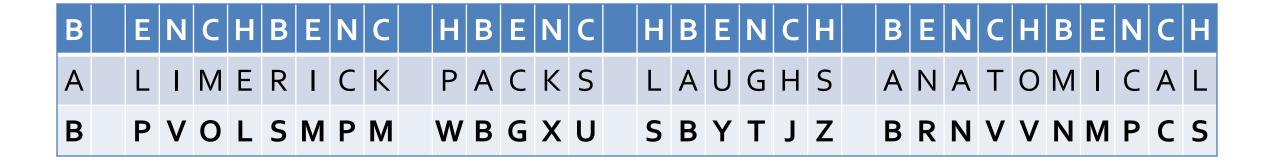
Vigenère cipher

- The Vigenère cipher is a form of polyalphabetic substitution cipher
- In this cipher, we take a key word and "add" its letters to our message
- Assuming letter values are in the range o-25
 - Add them together
 - Mod by 26 to keep them in the range o-25
 - If they're not in that range, convert them to that range and then back
- If the message is longer than the keyword, we start the keyword over again

Vigenère example

Key: BENCH

Plaintext: A LIMERICK PACKS LAUGHS ANATOMICAL



Vigenère encryption in Python

• Algorithm:

- Loop over all characters
 - Convert character to ASCII value
 - Convert ASCII value to a value from o-25 by subtracting the value of 'A'
 - Get appropriate character from key
 - Convert key character to ASCII and subtract 'A'
 - Add letter value and key value together and mod by 26
 - Add the value of 'A' to result and convert back to character
 - Concatenate the final character onto the ciphertext
- Return the ciphertext

```
def vigenereEncrypt(plaintext, key):
```

Vigenère decryption in Python

 Do everything exactly the same as encryption except subtract the key value instead of adding it

```
def vigenereDecrypt(ciphertext, key):
```

Work Time for Assignment 3

Upcoming

Next time...

Collections and lists

Reminders

- Read Chapter 4 of the textbook
- Finish Assignment 3