HACK UTK

September 25th, 2018

Cryptography

https://hackutk.slack.com/

Crypto Goals

- Alice and Bob want to talk “in private”
  - They share a key that only they know

- Key + Algorithm + msg = encrypted msg
- Key + Algorithm* + encrypted msg = msg

Algorithm Examples

- Caesar Cipher:
  - Move each letter in msg forward by certain amount to encrypt
  - Move each letter in enc_msg backward by certain amount to decrypt

Caesar Cipher

- Alice sends Bob:

UIJT GMBH JT TP TFDSU

Caesar Cipher

- Alice sends Bob:

THIS FLAG IS SO SECRET

UIJT GMBH JT TP TFDSFU

Caesar Cipher

- Bob decrypts:

THIS FLAG IS SO SECRET

UIJT GMBH JT TP TFDSFU

Key = 1

Caesar Cipher

- Total possible keys?

Caesar Cipher

- Total possible keys?
    - 26 - tiny!
    - Shift by {0, 1, 2, ... 25}

- Demo Code

Substitution Cipher

- Cranking up that key space

- Map every letter in alphabet to another

- Key space is now: 26!

Substitution Cipher

- Can map ‘A’ to any letter in alphabet (26)
- Can map ‘B’ to any letter except the one used for ‘A’ (25)
- Can map ‘C’ to any letter except one used for ‘A’, ‘B’ (24)

.

.

.

.

26!

Substitution Cipher

- Key Mapping:

abcdefghijklmnopqrstuvwxyz

Key - > **wisdomabcxzghjklepqrtuvnyf**

Substitution Cipher

- Plain vs. Cipher Text:

THIS FLAG IS SO SECRET

RBCQ MGWA CQ QK QOSPOR

Substitution Cipher

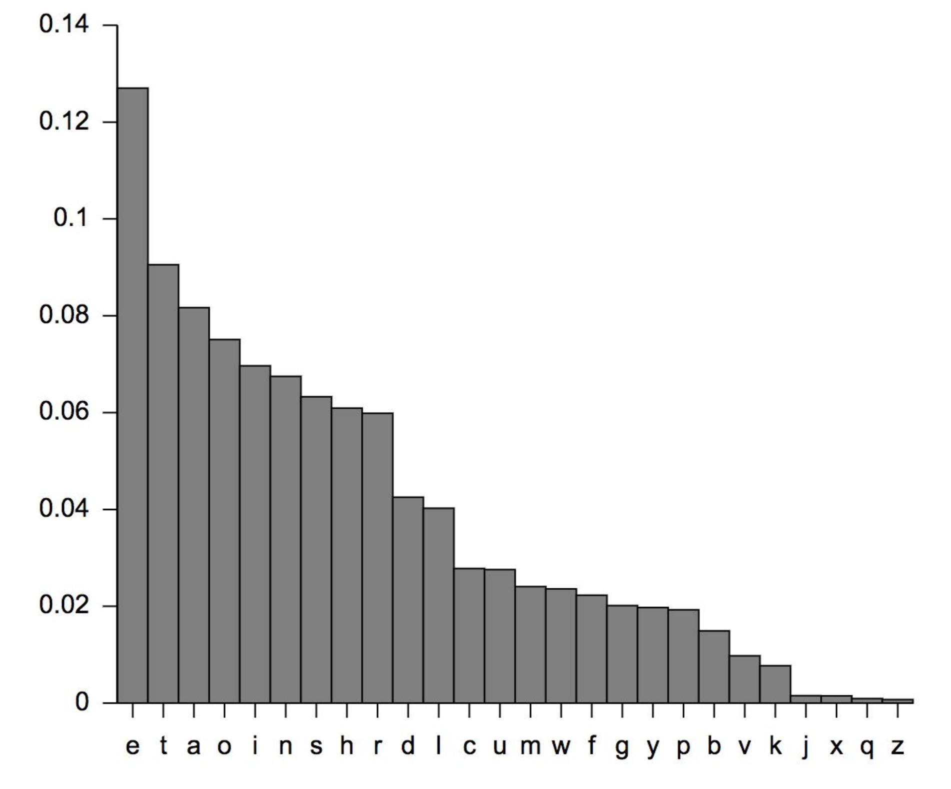
- Observations
  - Can use frequency analysis to figure out character mappings
  - Larger ciphertext gives us bigger sample space to work with

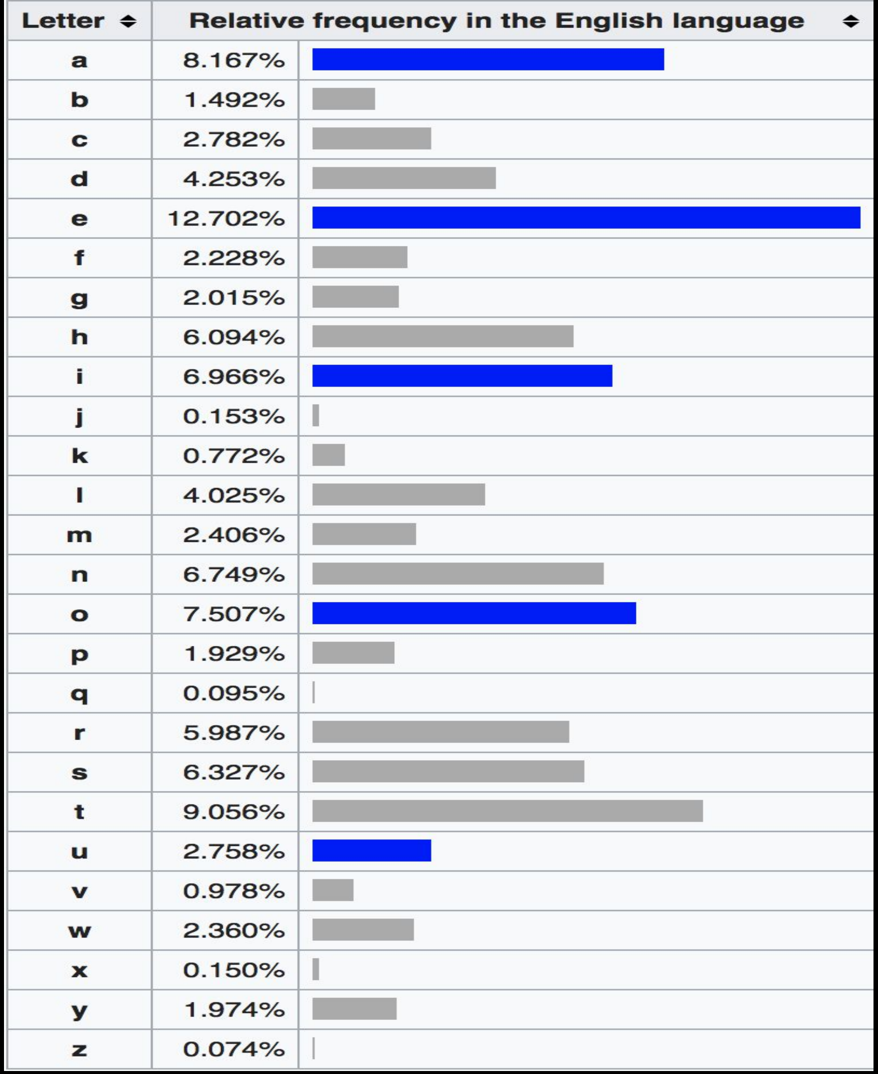
Substitution Cipher

Letters in the ciphertext that share the same frequency as English letters are likely to be the same.

i.e. if “t” appears in roughly 12% of the ciphertext, then it likely maps to “e” in plaintext

Substitution Cipher





Letter ⬍	Relative frequency in the English language ⬍
a	8.167%
b	1.492%
c	2.782%
d	4.253%
e	12.702%
f	2.228%
g	2.015%
h	6.094%
i	6.966%
j	0.153%
k	0.772%
l	4.025%
m	2.406%
n	6.749%
o	7.507%
p	1.929%
q	0.095%
r	5.987%
s	6.327%
t	9.056%
u	2.758%
v	0.978%
w	2.360%
x	0.150%
y	1.974%
z	0.074%

Vigenere Cipher

- Taking it a step further…
  - Key is a block of letters
  - Length of the key is called period
  - Split msg into blocks equal to period
  - The letter in the msg is shifted an amount equal to letter in key

Vigenere Cipher

- Example Key:

H A C C

7,0,2,2

Period = 4

Vigenere Cipher

- Example Key:

```
Blocks: THIS FLAG ISSO SECR ET
Key   : HACC HACC HACC HACC HA
```

Vigenere Cipher

- Example Key:

```
Blocks: THIS FLAG ISSO SECR ET
Key   : HACC HACC HACC HACC HA
Key   : 7022 7022 7022 7022 70
```

Vigenere Cipher

- Example Key:

```
Blocks: THIS FLAG ISSO SECR ET
Key   : 7022 7022 7022 7022 70
Cipher: AHKU MLCI PSUQ ZEET LT
```

Vigenere Cipher

- Use frequency analysis again

- Based on clever observation that
  - On the period, you will see English distribution of letters

Substitution Workshop

www.github.com/hackUTK/Fall2018

Workshop inside “Applied Crypto” Folder