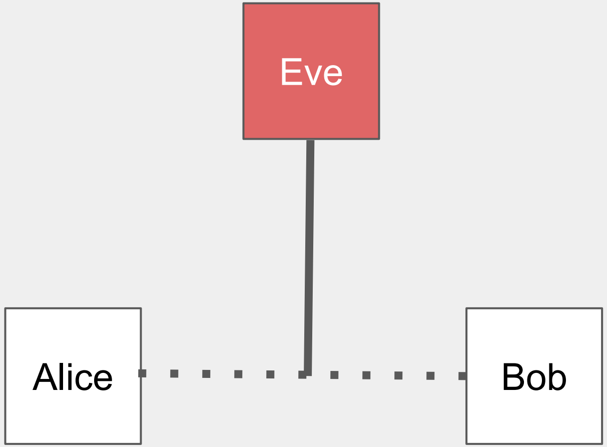
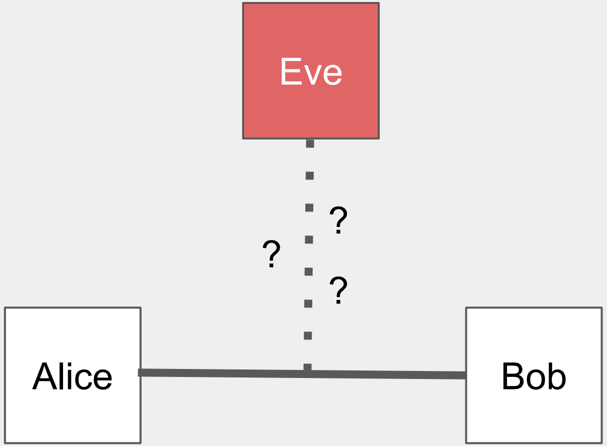
Intro to Crypto

Cameron Lonsdale clonsdale @myoutpost

Two Party Communication



Without Cryptography



With Cryptography

Quick Definitions

To keep a message secret we **encrypt** it

- The message is called the **plaintext**
- Encrypted, it is the **ciphertext**

Cryptanalysis - the art or process of deciphering coded messages without being told the key.

Cryptography - the art of writing or solving codes

Cryptology = Cryptanalysis + Cryptography

Cryptographic Goals

Confidentiality - Message is secret to everyone except the recipient

Integrity - Message has not been altered

Authentication - Identify the sender

Non-repudiation - Sender cannot deny sending the message

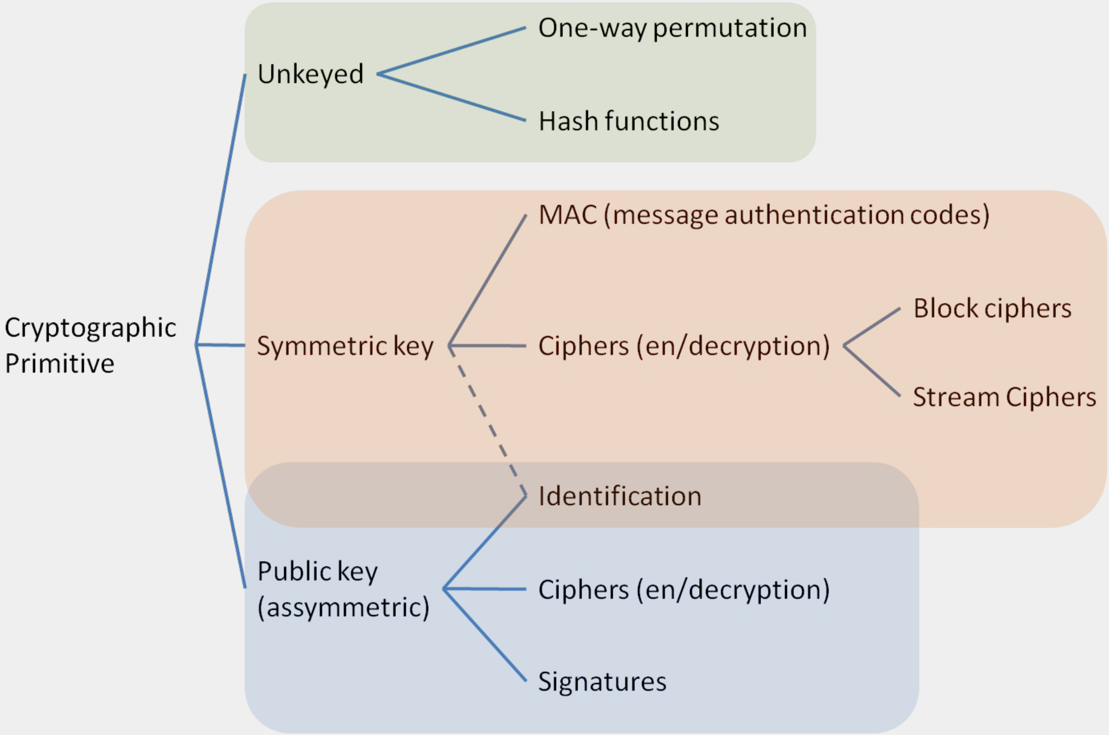
Cryptographic Primitives

Building blocks of a cryptographic system

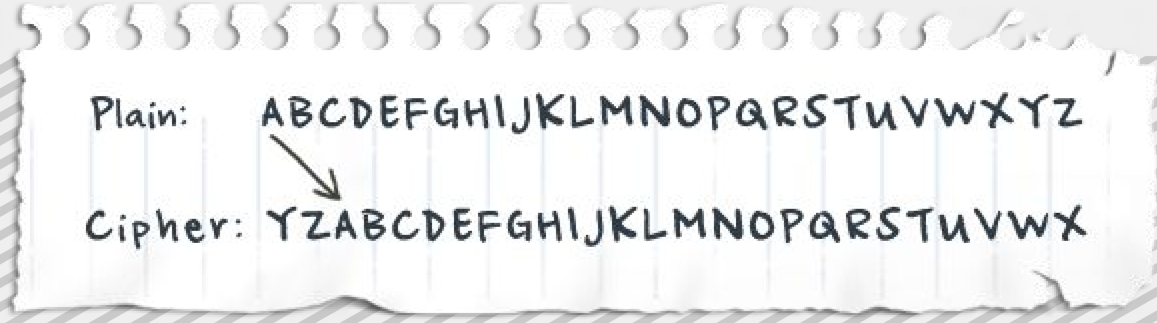
Unkeyed = 0 keys

Symmetric = 1 Key

Asymmetric = 2 Keys



Caesar Cipher



Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cipher: YZABCDEFGHIJKLMNOPQRSTUVWX

Encryption

Cyclically Shift each letter k places forward

$k = 3$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

For $k = 3$, the plaintext HELLO is encrypted as KHOOR

WARNING

Maths Ahead

Some Extra information

$$E_k(i) = i + k \ (mod \ 26)$$

$$D_k(j) = j - k \ (mod \ 26)$$

$$|K| \ = \ 26$$

Or 25 if you don't count k = 0

Decryption

Brute force is best force

Only 25 possible keys to check, let's just check them all!

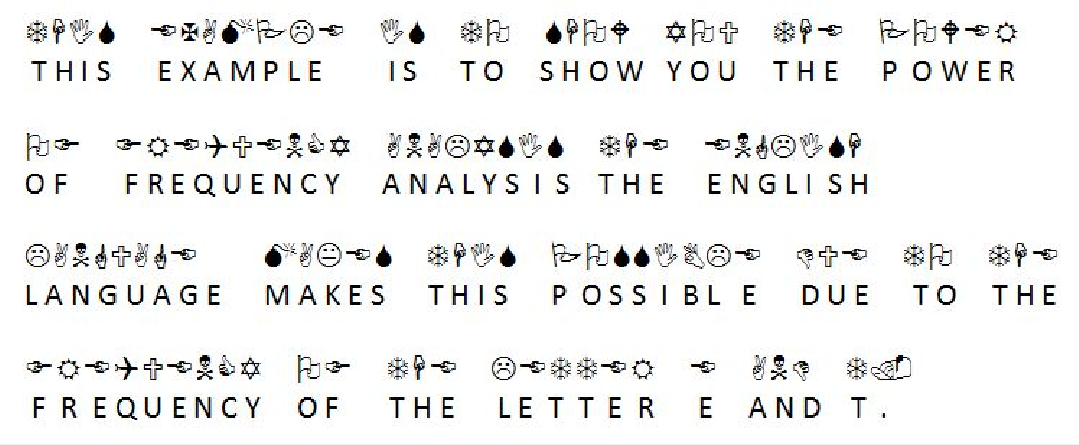
JGNNQ
IFMMP
HELLO
GDKKN
FCJJM
EBIIL
DAHHK
CZGGJ
BYFFI
AXEEH
ZWDDG
YVCCF
XUBBE
WTAAD
VSZZC
URYYB
TQXXA
SPWWZ
ROVVY
QNUUX
PMTTW
OLSSV
NKRRU
MJQQT
LIPPS

Activity

unswsecurity.com/crypto

A. Decrypt by hand or use an online tool to help you
B. H4CK3RZ Edition: Write a script to brute force through all decryptions

SImple Substitution Cipher



THIS EXAMPLE IS TO SHOW YOU THE POWER

OF FREQUENCY ANALYSIS THE ENGLISH

LANGUAGE MAKES THIS POSSIBLE DUE TO THE

FREQUENCY OF THE LETTER E AND T.

Encryption

Permute the alphabet for a key, then map letters to encrypt.

Mapped alphabet to a scrambled version

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
P	Q	S	T	U	V	W	X	Y	Z	C	O	D	E	B	R	A	K	I	N	G	F	H	J	L	M

The plaintext HELLO is encrypted as XUOOB

WARNING

Maths Ahead

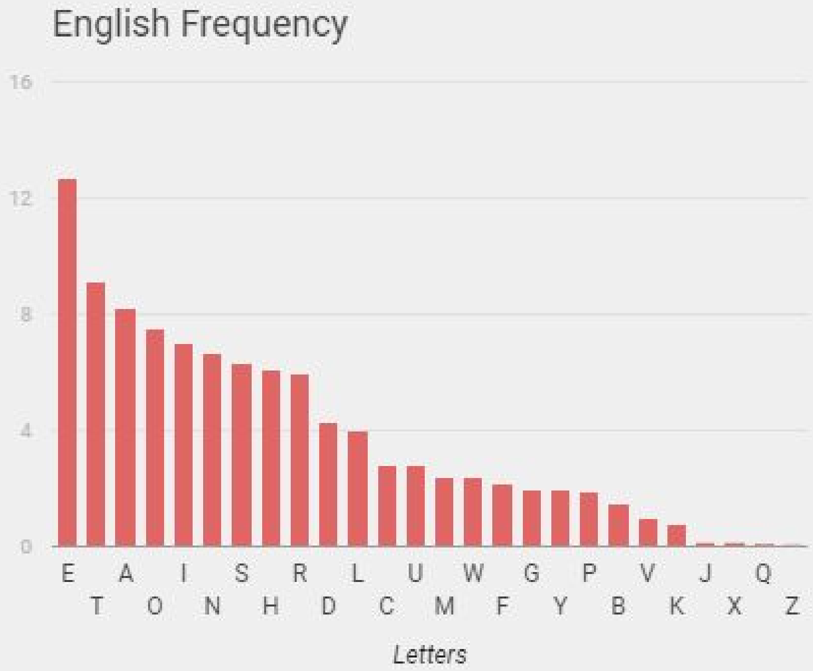
Some Extra information

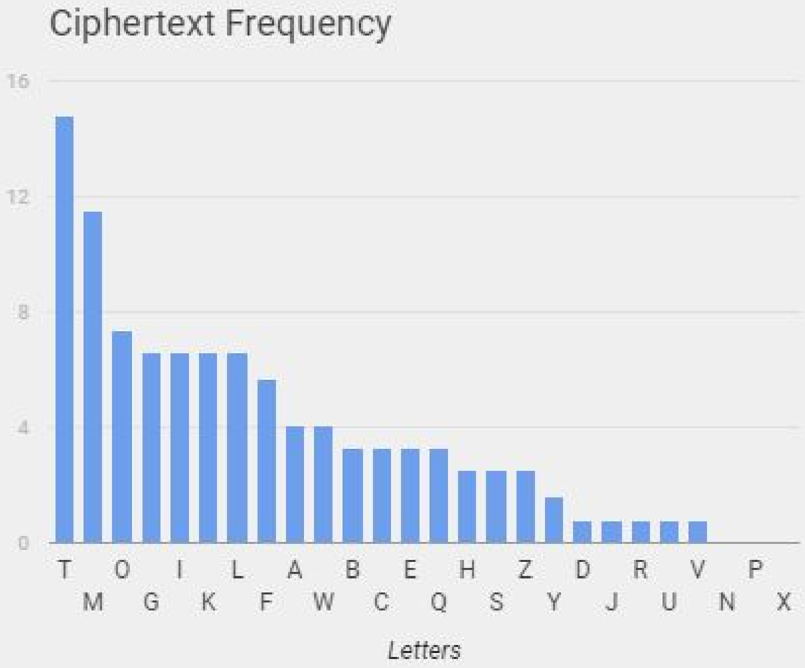
$$E_\pi(i) = \pi(i)$$

$$D_\pi(j) = \pi^{-1}(j)$$

$$|K| = 26! \approx 4 \times 10^{26}$$

Decryption - The magic of frequency





Decryption - More letters the better

N-grams, like letters but more of them!

Bigrams - TH is common, QU normally appear together...

Trigrams - THE, AND, ING are common

Example time:

```
ZKTAQOFU MIT LWZLMOMWMOGF EOHITK CGKQL ZTLM CITF MITKT OL A SGM GY EOHITKMTVM MG CGKQ
COMI. BGW EAF WLT YKTJWTFEB AFASBLOL MG ITSH RTMTKDOFT MIT QTB
```

Decryption - Like, totally

But Cameron! - don’t we like, need like, lots of like, letters for frequency to be effective?

Yes.

Unicity Distance: the length of an original ciphertext needed to break the cipher using brute-force.

Substitution Cipher = 28 characters.

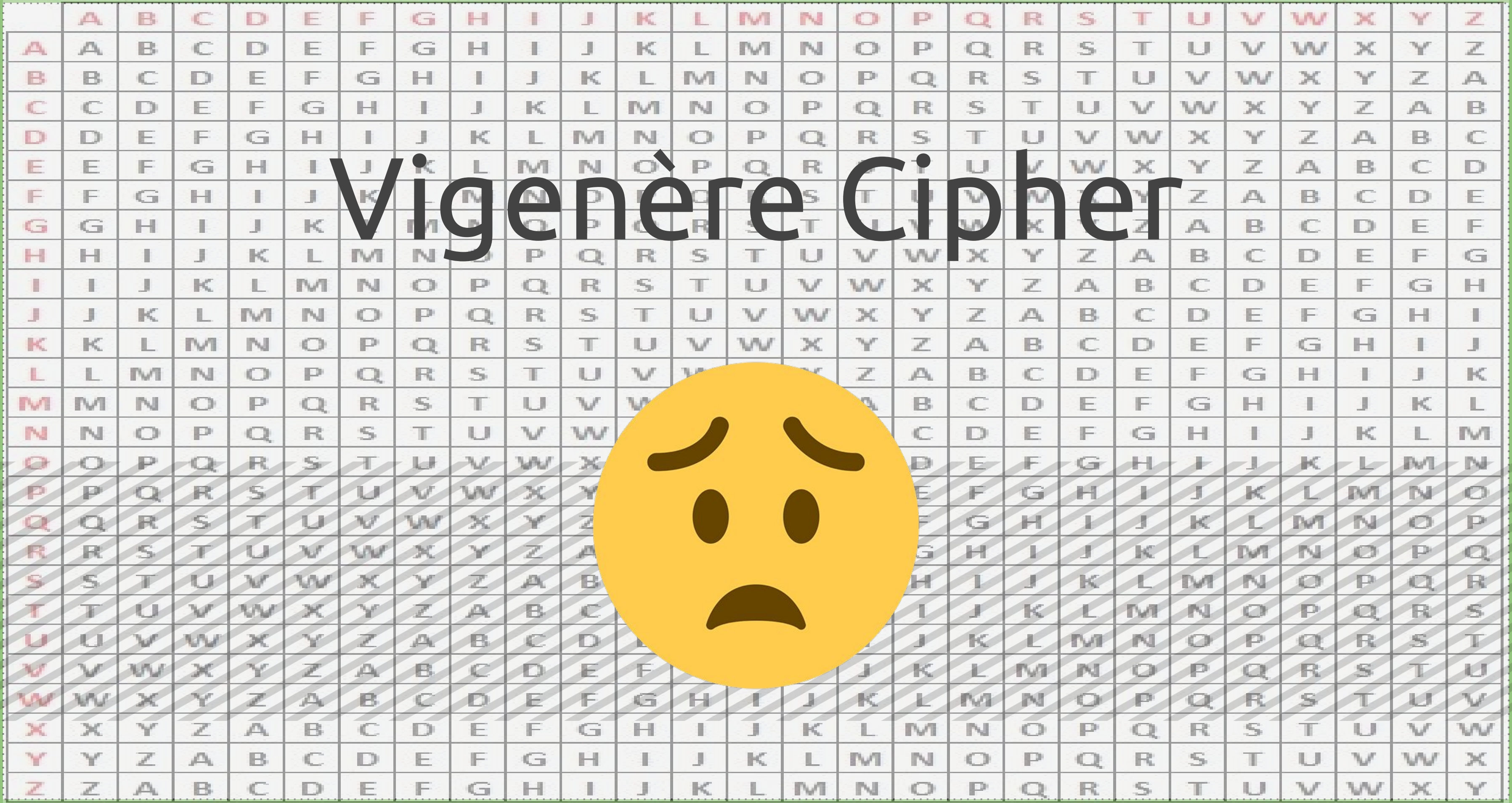
Need even more characters in order to decipher with frequency analysis.

Activity

unswsecurity.com/crypto

A. Decrypt by hand / use an online tool to help you
B. H4CK3RZ Edition: Write some code to calculate frequency and produce a possible key

Vigenère Cipher



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	[illegible]	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	[illegible]	[illegible]	[illegible]	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	[illegible]	[illegible]	[illegible]	[illegible]	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	[illegible]	[illegible]	[illegible]	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Encryption

r different Caesar Ciphers applied **periodically**

Key	C	O	D	E	C	O	D	C	O	D	E	C	O	D	E
Plaintext	T	H	I	S	I	S	A	N	E	X	A	M	P	L	E
Ciphertext	V	V	L	W	K	G	D	R	G	L	D	Q	R	Z	H

A = 0, B = 1, C = 2

T + 2 = V

WARNING

Maths Ahead

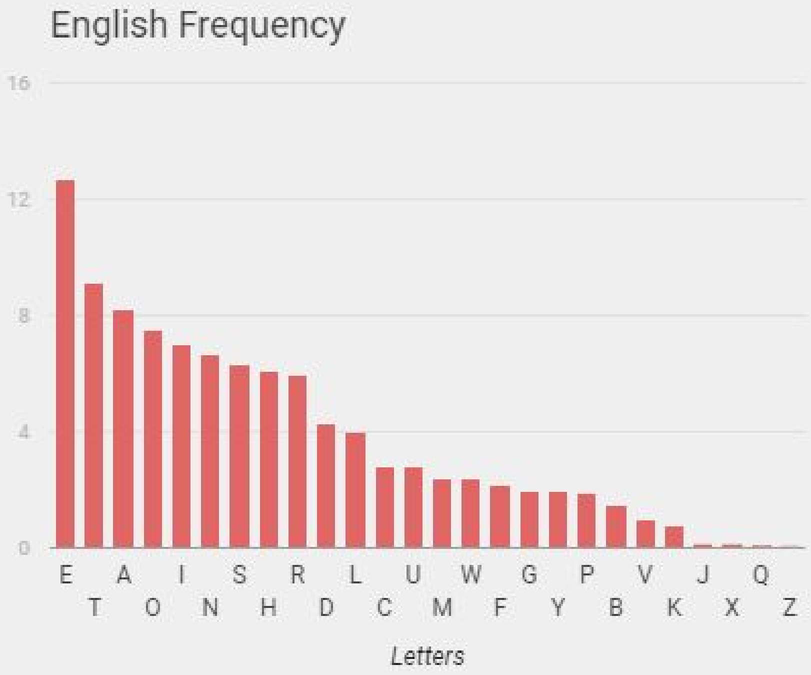
Some Extra information

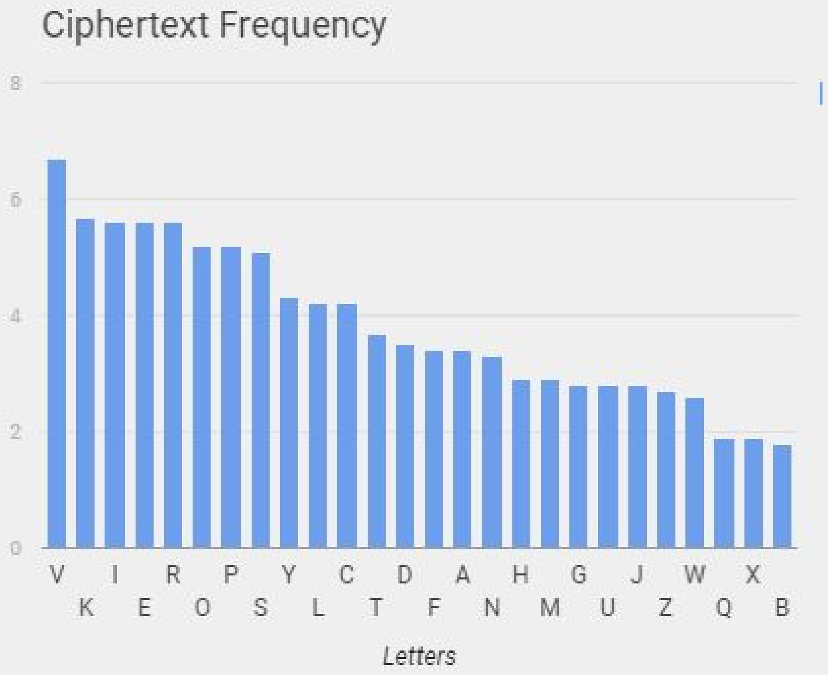
$$E_k(M_i) = (M_i + K_i)\ mod\ 26$$

$$D_k(C_i) = (C_i - K_i)\ mod\ 26$$

$$|K| \ = \ 26^r$$

Decryption - That don’t look right





Decryption - Frequency can still save us

Remember back to the frequency when encrypting with Substitution / Caesar, it did not change!

If the key length was 4..

```
HNQD
LVYO
POKF
ACCE
KYAT
....
```

Frequency of each column should look like the frequency of english.

Decryption - What a coincidence!

So I’m meant to ~feel~ whether or not the frequency is similar to English?

I didn't come here to feel.

Index of Coincidence - A summary of frequency

The probability of two letters randomly selected being the same.

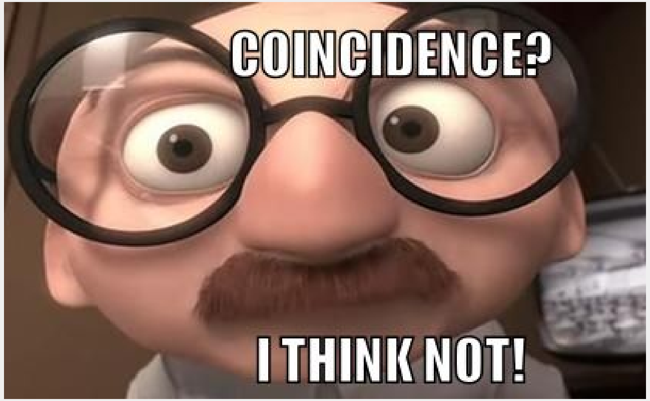
$$I.C. = \frac{\sum_{i=A}^{i=Z} f_i(f_i - 1)}{N(N-1)}$$

f_i is the count of the letter i.

N is total number of letters in the ciphertext

Decryption - I.C of English

Text	I.C
English	0.066
Substitution Cipher	0.066
Vigenère Cipher	0.042



Activity

unswsecurity.com/crypto

A. Just decrypt it, this is a tough one.

Bonus Round

Non-periodic polyalphabetic substitution ciphers

Cracking vigenere relied on a key which repeats! What about ciphers that use keys that don't repeat?

- Feeding (plaintext / ciphertext) back into key
- Rotation Ciphers (very long period)
- Key from an external source (like using an entire book text)

Is there any cipher that can’t be broken?

Yes!

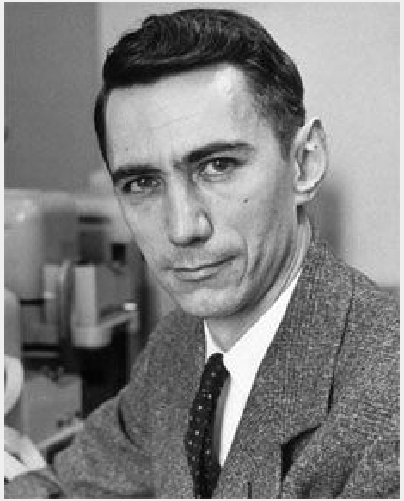
Common Patterns

We could learn something about the key, and the plaintext from the ciphertext for the previous ciphers.

What if we tried a key that never repeats and we only use once?

One Time Pad

A key the size of the message we want to send that is generated randomly and we never ever use again. Theoretically cannot be cracked!



WARNING

Serious Maths Ahead

This is just to freak you out

Some Extra information

$$H(X) = -\sum_{i=1}^{n} P(x_i) log_b P(x_i)$$

Let

- M be the set of possible plaintext messages
- C be the set of possible ciphertexts

$$H(M) = H(M|C)$$

$$I(M,C) = H(M) - H(M|C) = 0$$

Where can I learn more?

- http://practicalcryptography.com/
- http://overthewire.org/wargames/krypton/
- https://www.crypto101.io/
- https://cryptopals.com/

Best Caesar / Substitution Cipher Solver (for now)
http://quipqiup.com/

- Handbook of applied cryptography - Menezes, Oorschot, Vanstone
- Cryptography Engineering - Bruce Schneier

Thank You!