Cryptography and Security

How to keep secrets secret
when other people don’t want them to be

Brief History

- Entirely just encryption for a long time
  - Turning a message into something unintelligible
  - We don't get into secure communication until the modern age
- Around for probably as long as writing has been
  - Julius Caesar was a fan over 2k years ago
- Ciphers
  - The methods for encrypting and decrypting information
  - Used all over the world for 1000s of years
  - Many early version crack-able, but worked on the layman
- Computers made cipher cracking suddenly much more possible
  - Ciphers become more complex too though
- Generally a movement from linguistic theory -> math and complexity

Transposition Ciphers

- Take the letters already there and jumble them up

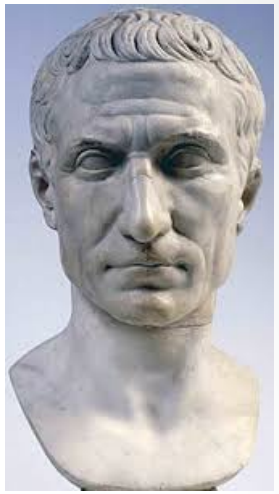
- E.g. Rail Transposition
- "Secret message" gets put on N "rails"

S				E				S				E
	E		R		T		E		S		G	
		C				M				A		

- Our encrypted message becomes

  "seseertesgcma"

Substitution Ciphers



- Replace every letter with a consistent alternative
- E.g. Caesar Cipher
  - Replace each letter with the letter 3 spaces ahead of it in the alphabet
  - “Attack at dawn” becomes “dwwdfn dw gdzq”
- These types are **monoalphabetic** and easy to crack
- Better substitution methods are…

Polyalphabetic Cipher

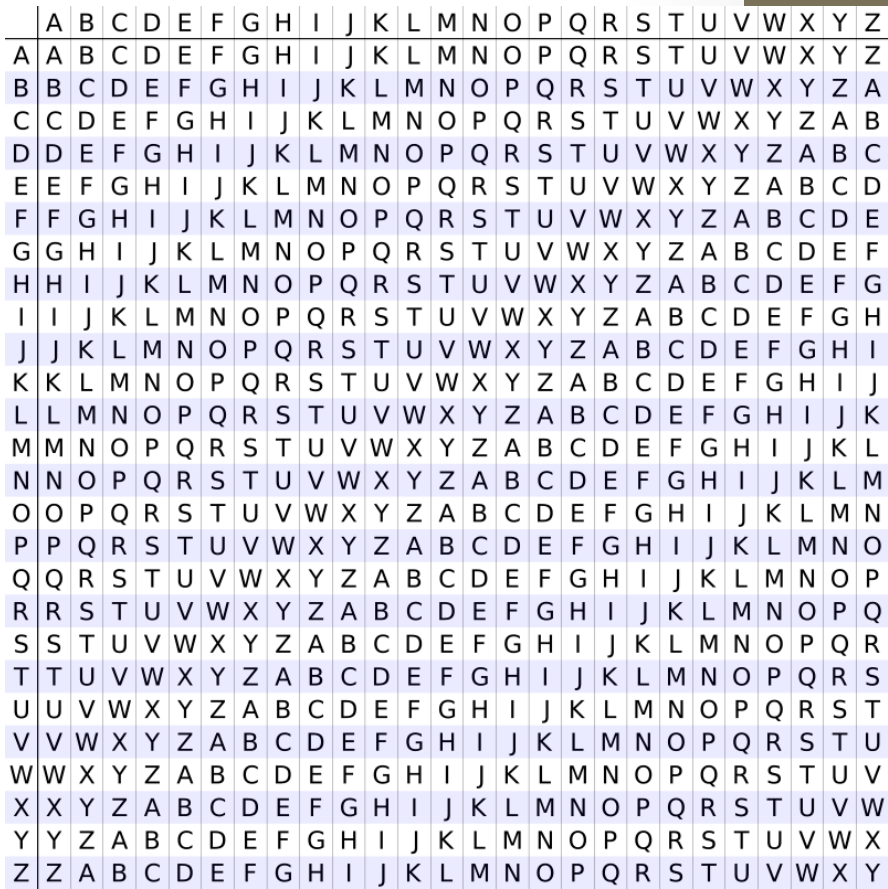
- Like the Caesar cipher, but change the distance between letters on each new letter

Vigenère square

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

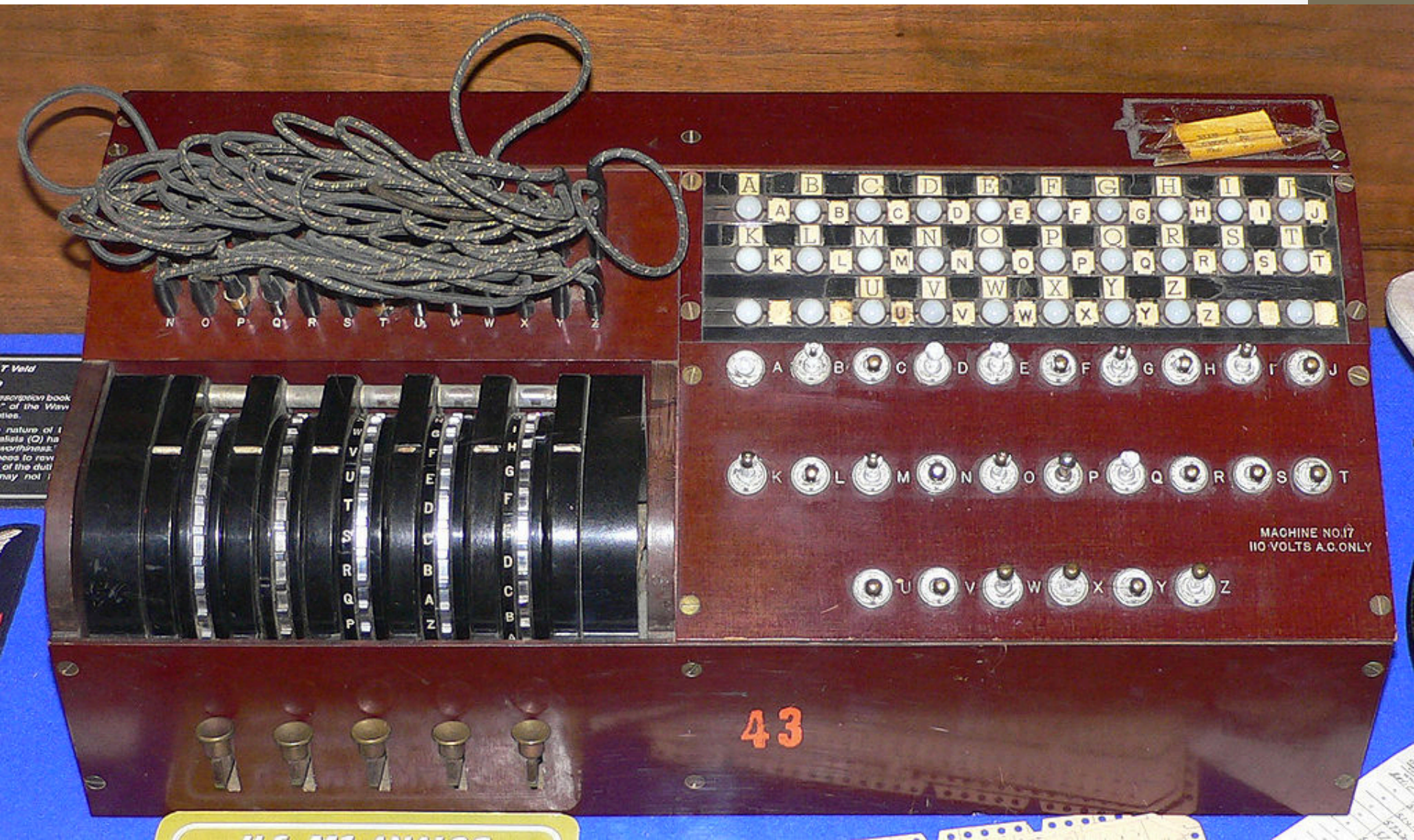
Vigenère Cipher

- Pick a code word, e.g. “locked”
- Repeat the code word over the message to match the length
  - “secret message” + “lockedlockedl”
- The letter from the repeated code word decides what Ceasar cipher we use on that letter
- Our message becomes “dsebiwxsucejp”



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

The Enigma Machine



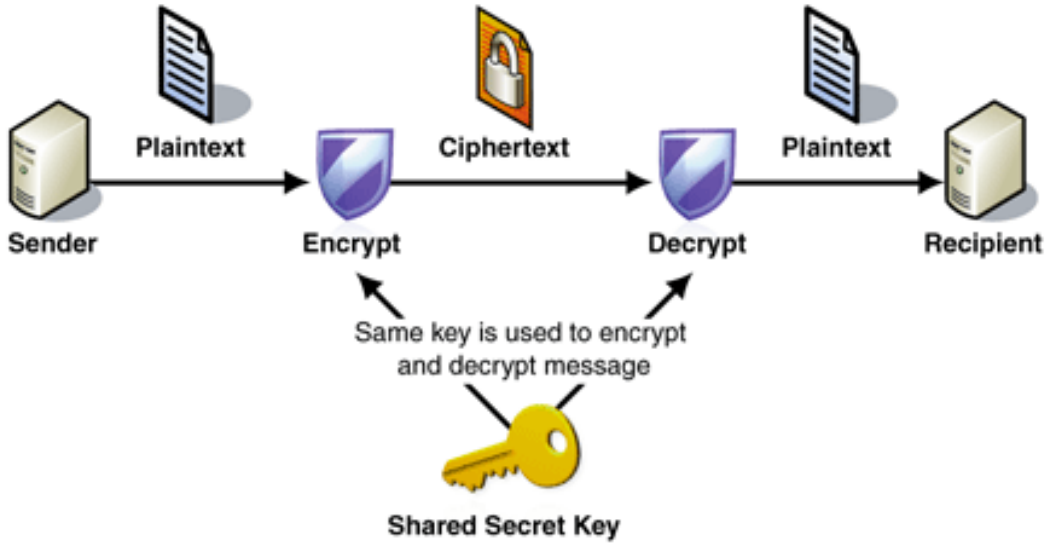
Steganography

- Keep people from knowing there's any information at all

- E.g.
  - Invisible ink
  - Messages in clothes or tattoos
  - Hide it in other writing
    - In the margins
    - Change the font
    - The first letter of each line of writing
  - Morse code
    - Jeremiah Denton

Modern Methods – Symmetric Key Cryptography

- "My friend and I have the same key for one lock"
- Similar to the ciphers we saw, but based in numbers instead of letters
- The only (publicly) known encryption method until 1976
- Both parties have to have the same key
  - This sucks! Why?



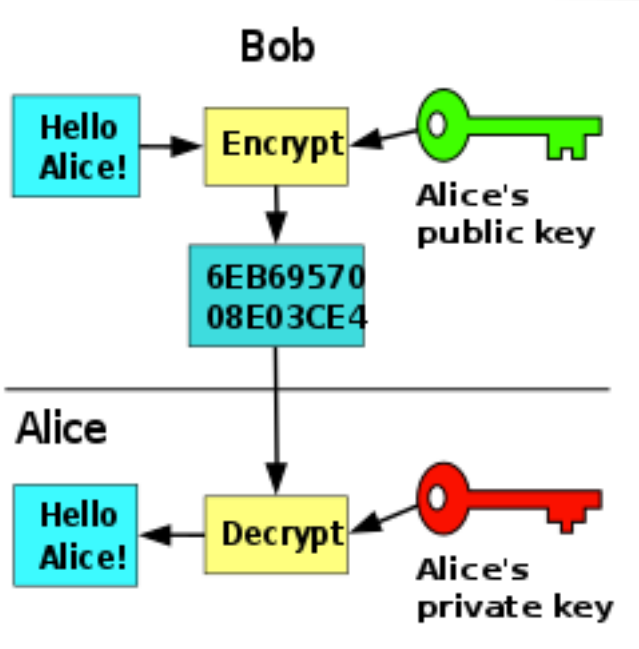
Public Key Cryptography

- What modern software typically uses
- Introduced (publicly) by Diffie and Hellman in 1976
  - Potentially known in secret since at least 1970
- The biggest advancement in crypto since polyalphabetic ciphers

- Basic idea: separate the encryption and decryption ciphers
- Share the encryption cipher with whoever (public key)
- Keep the decryption cipher for yourself (private key)
- Anyone can send a message to you and only you will be able to decrypt it
  - Why is this a big deal?

RSA (Rivest-Shamir-Adleman)

- First detailed public key system
- Still widely used
  - SSH, SSL, OpenPGP



Start with two prime numbers:

p = 13
q = 17

Calculate their product n = p * q = 13 * 17 = 221
And their totient t = (p – 1)*(q – 1) = 12 * 16 = 192

RSA

Pick a 3rd prime that isn't a divisor of t

e = 23 t/e = 192/23 = 8.347…. we're good

Now we need a number d where (d * e) % t = 1
This is the long step, but the lowest example is 167

RSA

We’ve got everything now, to recap

p = 13
q = 17
n = 221
t = 192
e = 23
d = 167

Encrypting the Message

The public key uses n and e

Call our plaintext message M, which has been converted to one big number
Call our encrypted message E

$E = M^e \% n$

E.g. if our message is 16, then the encrypted one is

$15^{23} \% 221 = 59$

Decrypting the Message

The private key uses n and d

M (the original message) = E^d % n

E.g. 15 = 59^{167} % 221

Our message is decrypted and we didn't have to share the private key with anyone

Why is this safe?

- In a real scenario, p, q, and thus n are very, very large numbers
  - 2048 bits each, about 10^{617}
  - d is the important #, but can't be figured out without p and q
- We can safely share n because it would take a really long time to find p and q
  - Brute force
  - Best attempt so far was hundreds of connected computers factoring a 768-bit number over two years, with over 2000 years of total computing time
  - Complexity increases exponentially as the bits go up

Now for the other side…

- Can a cipher be completely unbreakable?
  - One-time pad
- Can a whole system be secure?

Social Engineering

- Most security breaches are from human error
  - Easiest way into most systems
- The most secure system in the world is useless if it employs even one idiot

- Phishing
- Keylogging
- Eavesdropping
- Ignoring/breaking the air gap

Breaking Ciphers - Cryptanalysis

- What do we know and what can be found out?
  - What would be useful to know?

- Rail Transposition
  - If we know the # of rails we can solve it, and it's easy to guess

Frequency Analysis

If we know they used a substitution cipher, how do we break it?

Frequency Analysis

If we know they used a substitution cipher, how do we break it?

English (or any natural language) has predictable patterns

Some letters appear far more often than others

Crack a Message

- Encrypted message:

XLIVIMWRSAECCSYEVIGVEGOMRKXLMWQIWWEKI

- What are the most common letters?

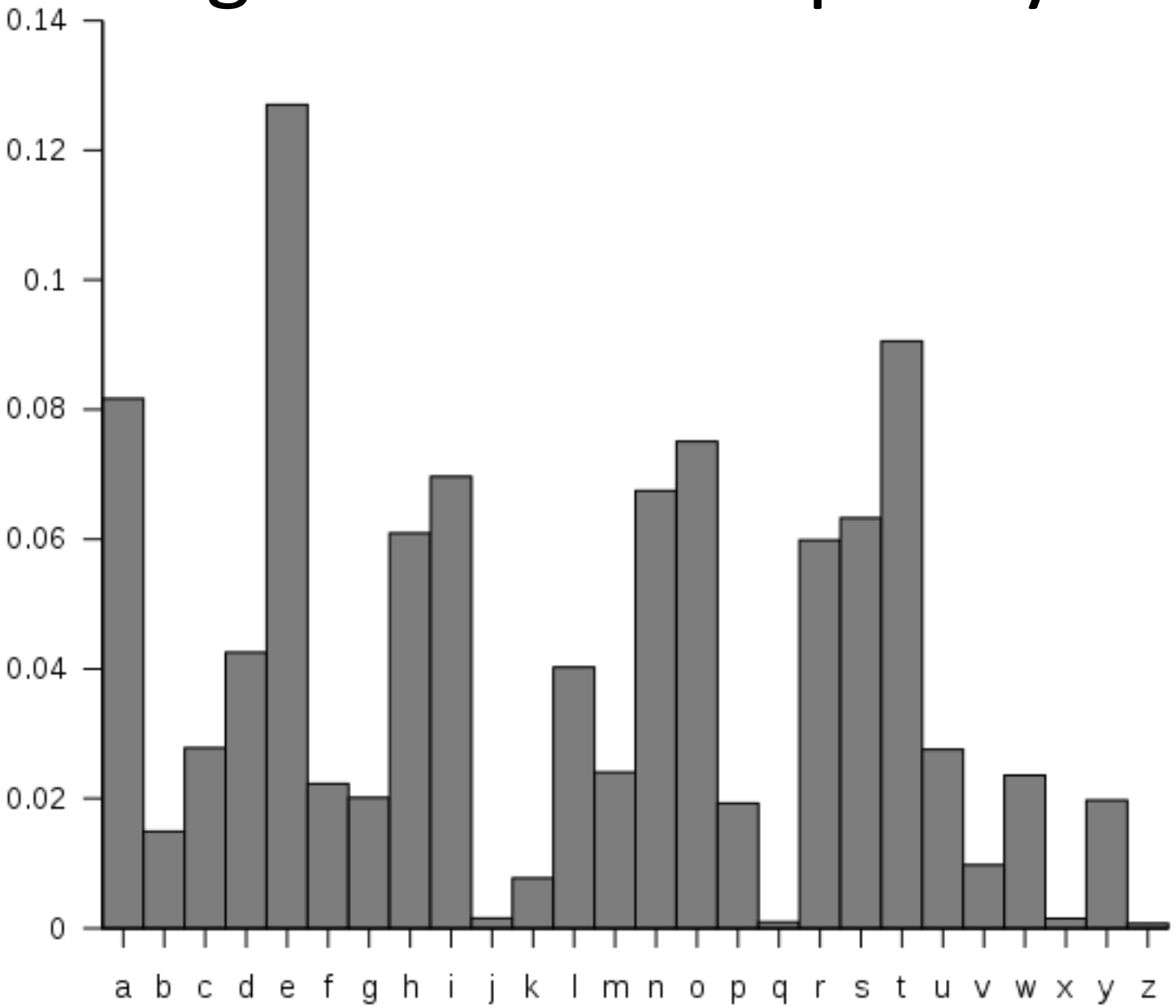
Crack a Message

- Encrypted message:

XLIVIMWRSAECCSYEVIGVEGOMRKXLMWQIWWEKI

- What are the most common letters?
  - I,V,W,E are each > 10% of the total, M at 8%
  - I has the most at 5x

English Letter Frequency



Now We Guess

- Naïve guess
  - I -> E
  - If the cipher is monoalphabetic, that's all we need
    - Why?

Does It Work?

XLIVIMWRSAECCSYEVIGVEGOMRKXLMWQIWWEKI

	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

It Works!

THEREISNOWAYYOUARECRACKINGTHISMESSAGE

Unicity Distance

- How much ciphertext do we need to know we can crack it?
- For simple ciphers the answer is usually very little
  - About 50 characters for polyalphabetic
  - Keep in mind this ignores computation cost
- The longer the message, the more vulnerable it is

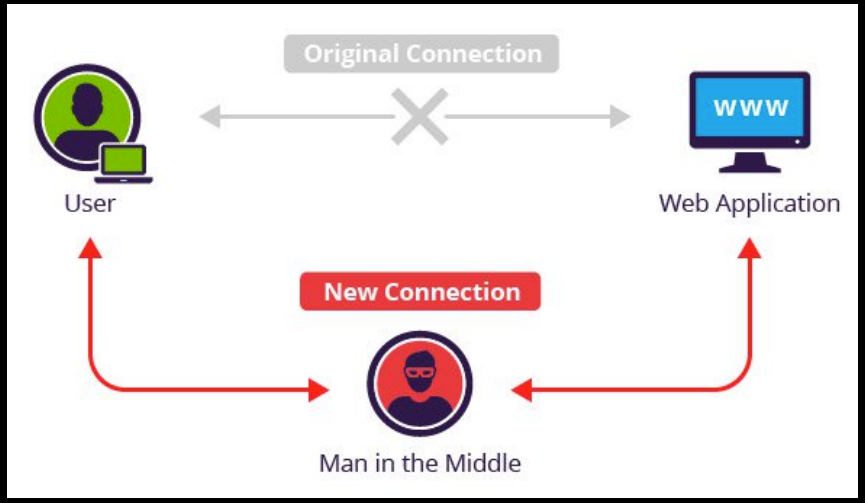
What about RSA?

- If the users are smart, and the keys are well-chosen, what do we have left?

What about RSA?

- If the users are smart, and the keys are well-chosen, what do we have left?
  - Still plenty of options

Man in the Middle



- Alice asks for Bob's public key, but Eve intercepts the message and sends her public key instead
- Eve does the same to Bob with Alice's response
- Now she fully controls all communication between them

Side-Channel Attacks

- Computers are physical, imperfect machines
- Huge number of things we can do to gather more information
  - Examine the cache
    - Meltdown & Spectre
  - Look at processing time for various inputs
  - Look at power usage for various inputs
  - Examine improperly wiped data
- Works outside of computers too
  - Detecting sound with lasers pointed at vibrating windows
  - Reading body movement by analyzing changes in room's electrical circuit

Let's Play a Game…

Decrypt your login access, keys are the passwords with the numbers stripped out

Username: pc11 Password: mGKq6hu9
Encrypted PC Name: YGQWPY

Username: pc12 Password: Vxwc36jU
Encrypted PC Name: YLVGA

Username: pc13 Password: 8cmopGP7
Encrypted PC Name: UMHX

Username: pc14 Password: xBb6Zx3u
Encrypted PC Name: BJHGQ

Username: pc15 Password: qRgcCc58
Encrypted PC Name: DZTG

Pick one and figure out which PC it logs into

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