CSCI 15: AN INTRODUCTION TO THE MODERN INTERNET

Lecture 6: Cryptography

ADMIN

- Project ideas on website
- Topic due next Wednesday

- Computer science today!
- Activity I really want to do at the end of class
  - Might end early
  - Might extend until Monday

WHAT DOES IT MEAN TO ENCRYPT A MESSAGE?

- Want to be able to send a message to someone else
- If someone else sees the encrypted text, they cannot understand the message
- But the receiver can!

WHY IS CRYPTOGRAPHY IMPORTANT?

Without cryptography, everything is public on the internet

- All sites we see, all emails we send
- All texts, etc
- All passwords we send to websites

PRIVATE KEY CRYPTOGRAPHY

ALICE AND BOB WANT TO EXCHANGE MESSAGES

- How do they do this?

ALICE AND BOB WANT TO EXCHANGE MESSAGES

- Step 1: Meet secretly to exchange a key

ALICE AND BOB WANT TO EXCHANGE MESSAGES

- Step 2: Use that key to encode messages
- An eavesdropper (Eve) cannot understand them

ALICE AND BOB WANT TO EXCHANGE MESSAGES

WHAT HAPPENED?

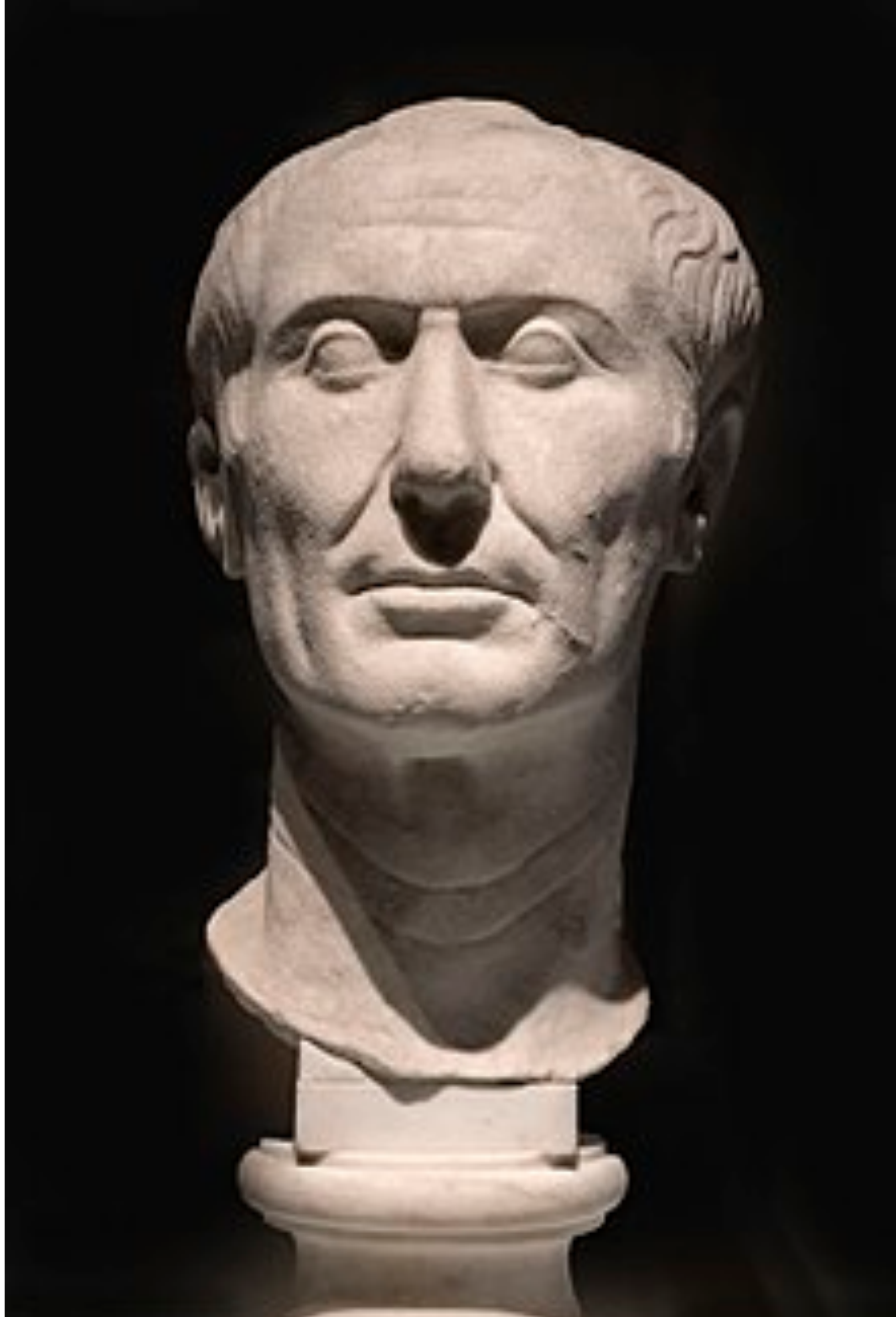
- Alice, Bob, and Eve have the encrypted text
- Only Alice and Bob have the key (they met secretly to exchange it)
- Hopefully, only Eve cannot decrypt the text without the key

HOW DOES IT WORK?

- Need a key to get from an message (plaintext) to a difficult-to-decode cyphertext
- And back!

CAESAR CIPHER

- Key: number between 1 and 26
- Move each character forward that number of letters
- (Punctuation, spaces stay same)



LET'S TRY IT!

- Split into groups of size 2-4
- Can you decode this secret message:

```
Fubswrjudskb lv ixq!
```

WHY IS CAESAR CIPHER BAD?

- Only 26 keys
- Lots of information about length of words, etc.

- Who can think of a way to do better?

SUBSTITUTION CIPHER

Key

Plaintext:	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
Ciphertext:	C R Y P T O G R A M 5 6 7 8 9 B D E F H I J K L N Q

Additional ciphertext symbols:

- C, 1, U
- T, 2, V, Z
- A, 3, W
- 9, 4, X
- I, S

Message

Plaintext:	THIS IS A SECRET MESSAGE
Ciphertext:	HRAF AF C FTYE2H 7VFF1GZ

SUBSTITUTION CIPHER

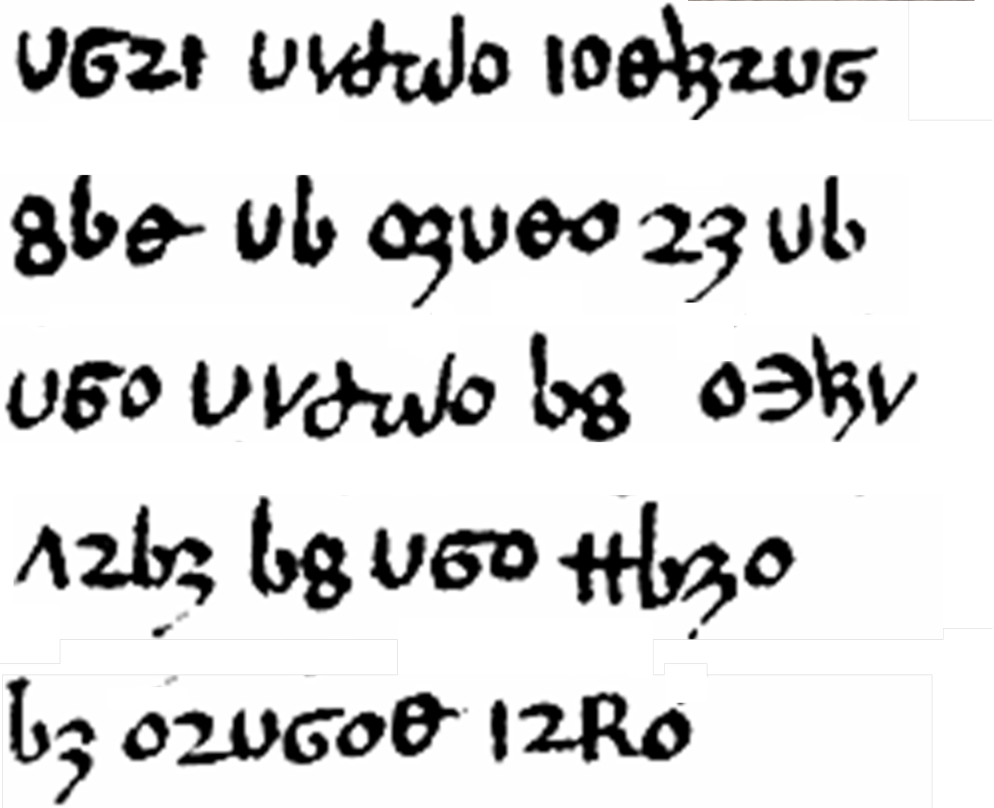
Seems pretty secure!

Too many keys for brute force, even for a computer (about 10^26 keys)

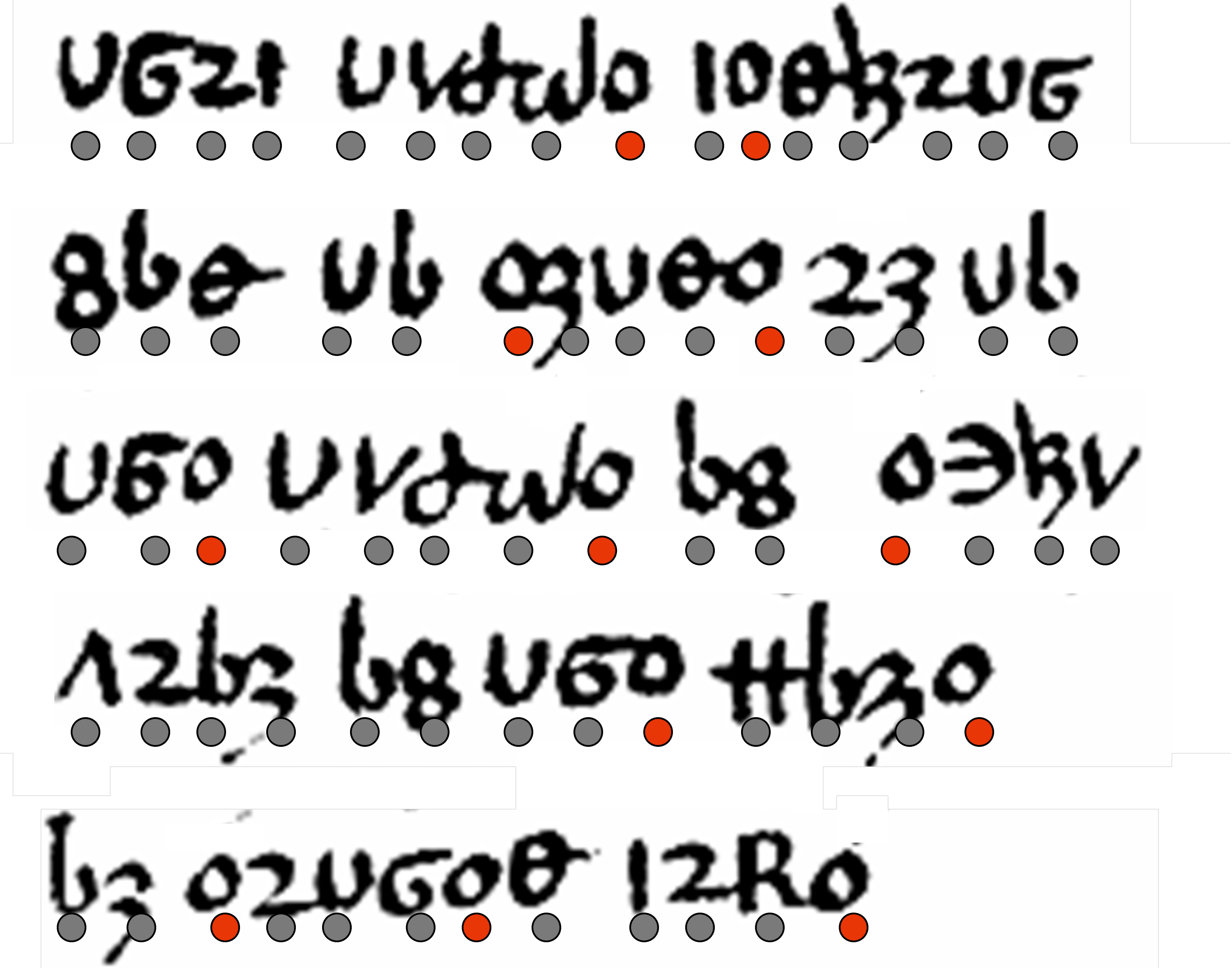
Why don't we use this?

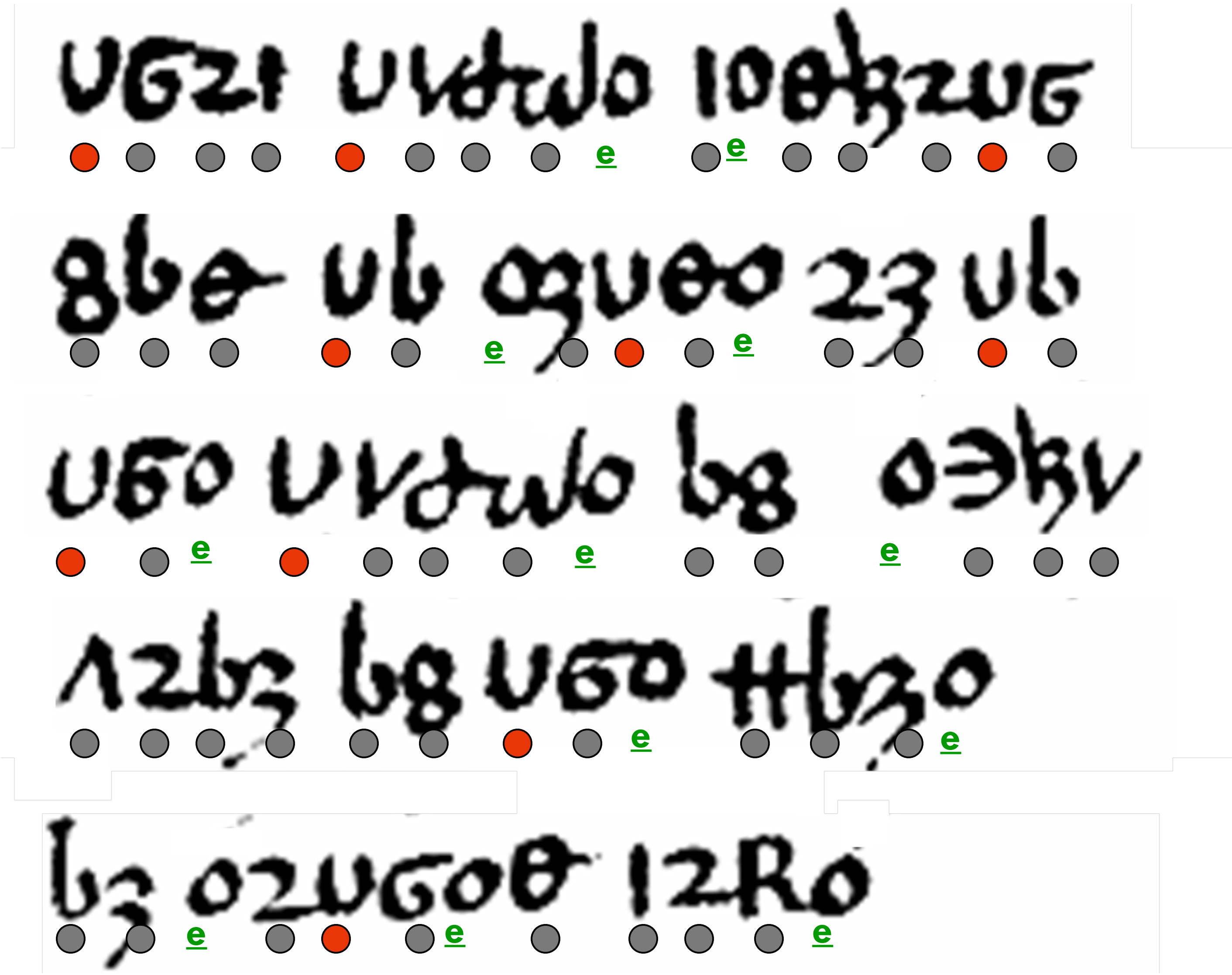

A TREATISE ON THE ASTROLABE PROLOGUS

LOWIS MY SONE, I HAVE PERCEIVED wel by certeyne evidences thyn abilite to lerne sciences touchinge noumbres and proporciouns; & as wel considere I thy bisy preyere in special to lerne the Tretis of the Astrolabie. Than, for as mechel as a philosofre seith, he wrappeth him in his frend, that condescendeth to the rightful preyers of his frend, therfor have I geven thee a suffisaunt Astrolabie as for oure orizonte, compowned after the latitude of Oxenford; upon which, by mediacion of this litel tretis, I purpose to teche thee a certein nombre of conclusions apertening to the same instrument. I seye a certein of conclusiouns, for three causes. The furste cause is this: truste wel that alle the conclusiouns that han ben founde, or elles possibly mighten be founde in so noble an instrument as an Astrolabie, ben unknowe perfitly to any mortal man in this regioun, as I suppose. Another cause is this; that sothly, in any tretis of the Astrolabie that I have seyn, there ben some conclusions that wole nat in alle thinges performen hir bihestes; & some of hem ben to harde to thy tendre age of ten yeer to conseyve. This tretis, divided in fyve parties, wole I shewe thee under ful lighte rewles & naked wordes in English; for Latin ne canstow yit but smal, my lyte sone. But natheles, suffise to thee thise trewe conclusiouns in English, as wel as suffyseth to thise noble clerkes Grekes thise same conclusiouns in Greek, & to Arabiens in Arabik, and to Jewes in Ebrew, & to the Latin folk in Latin; whiche Latin folk han hem furst out of othre diverse

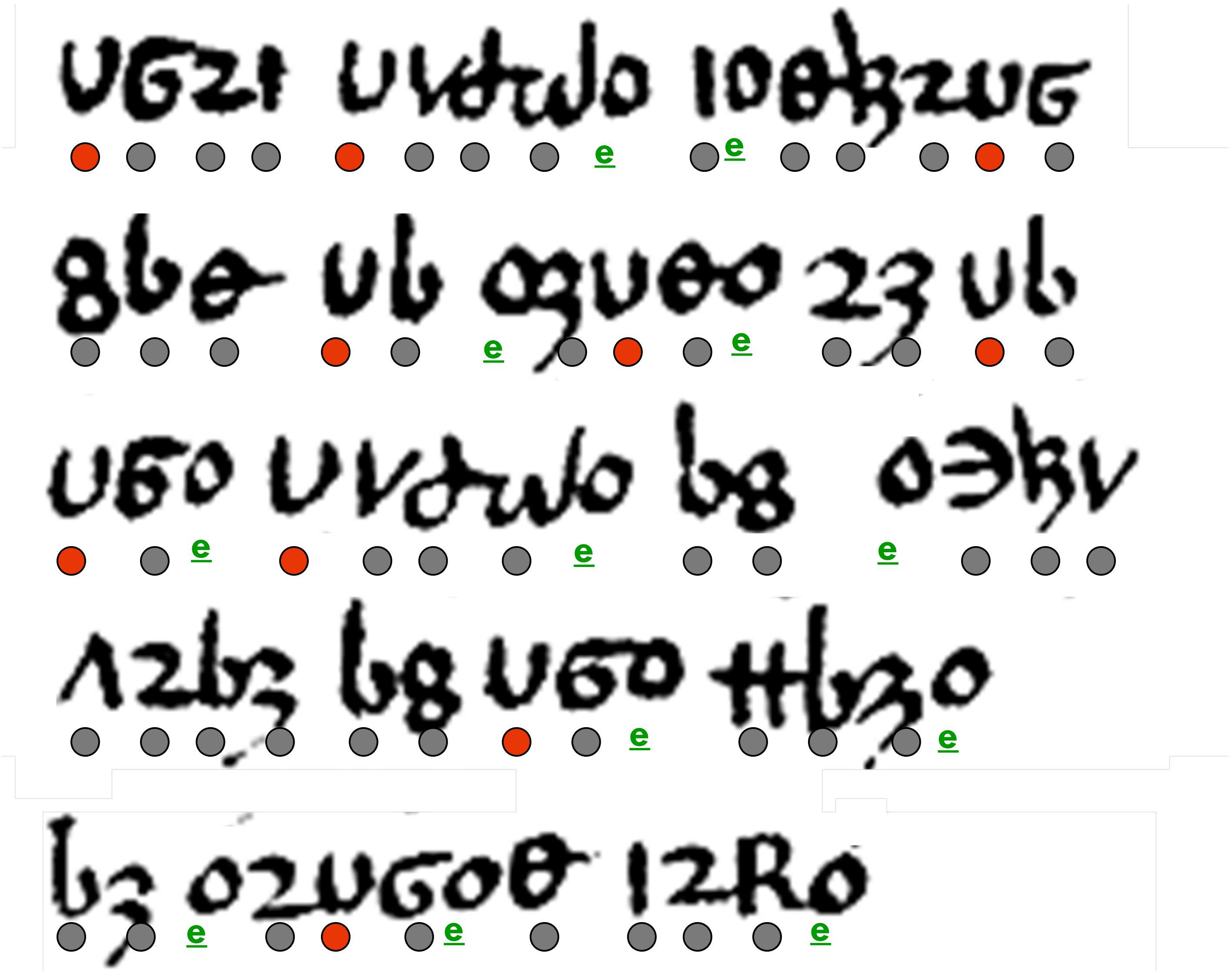


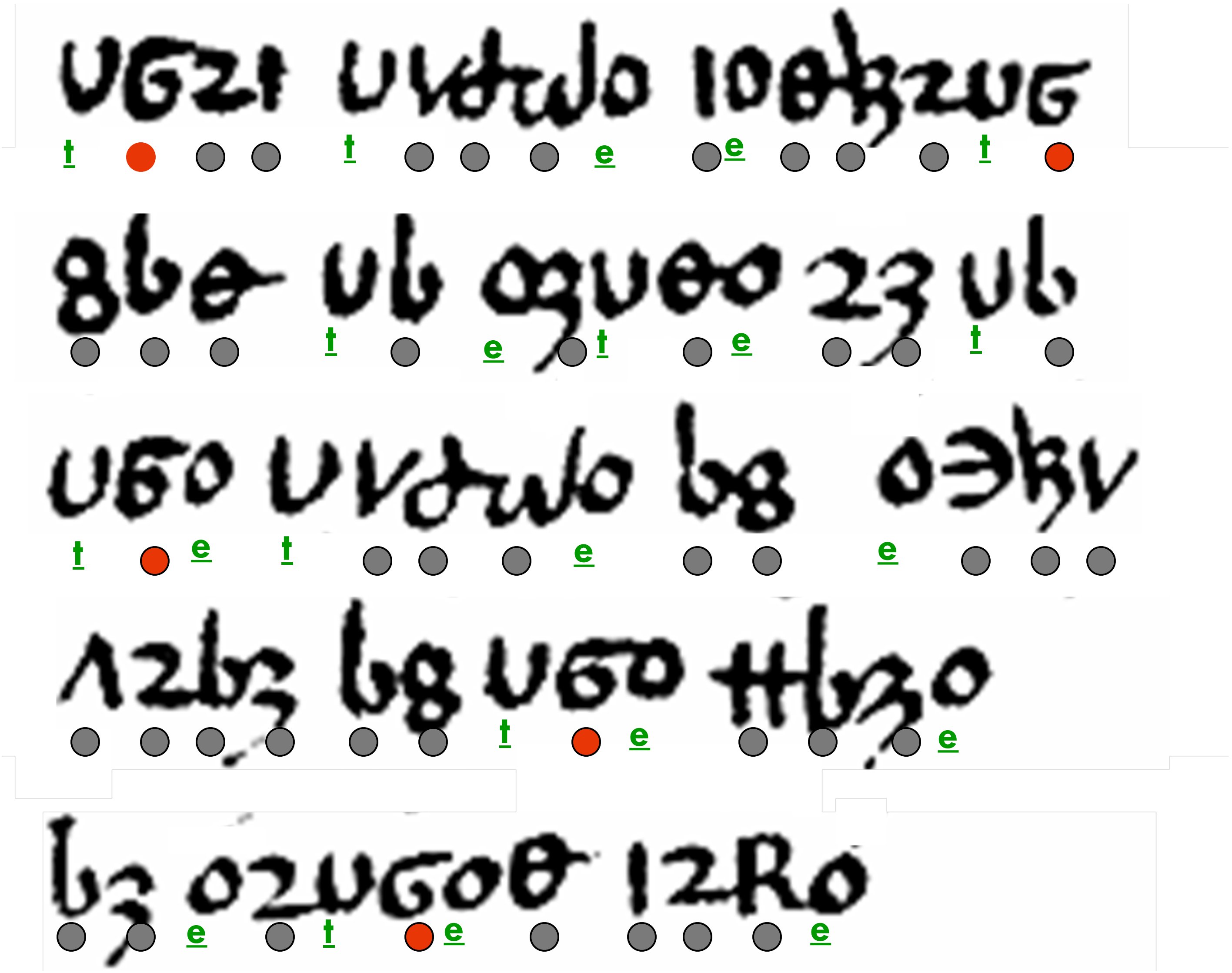
Geoffrey Chaucer, *Treatise on the Astrolabe*, 1391

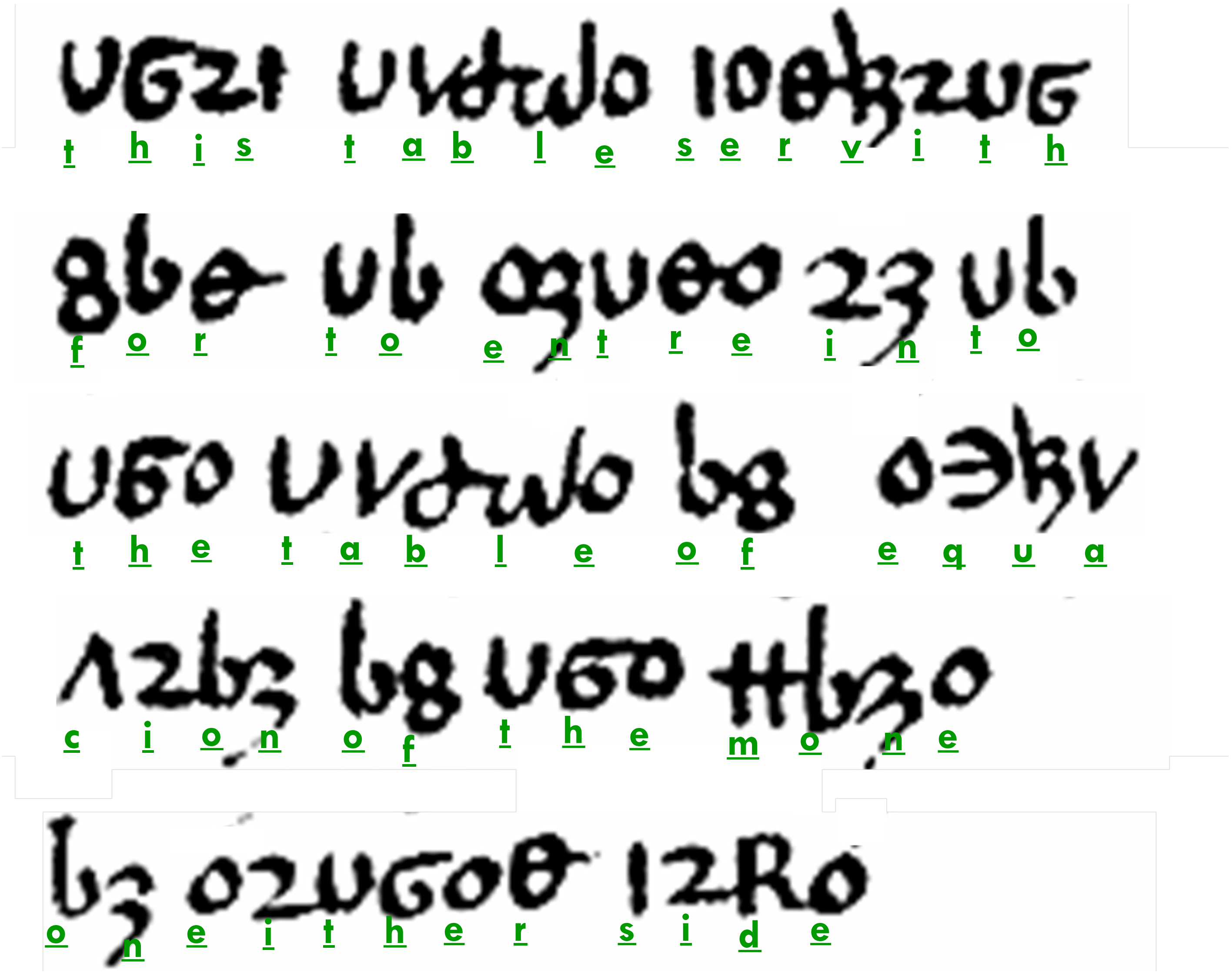


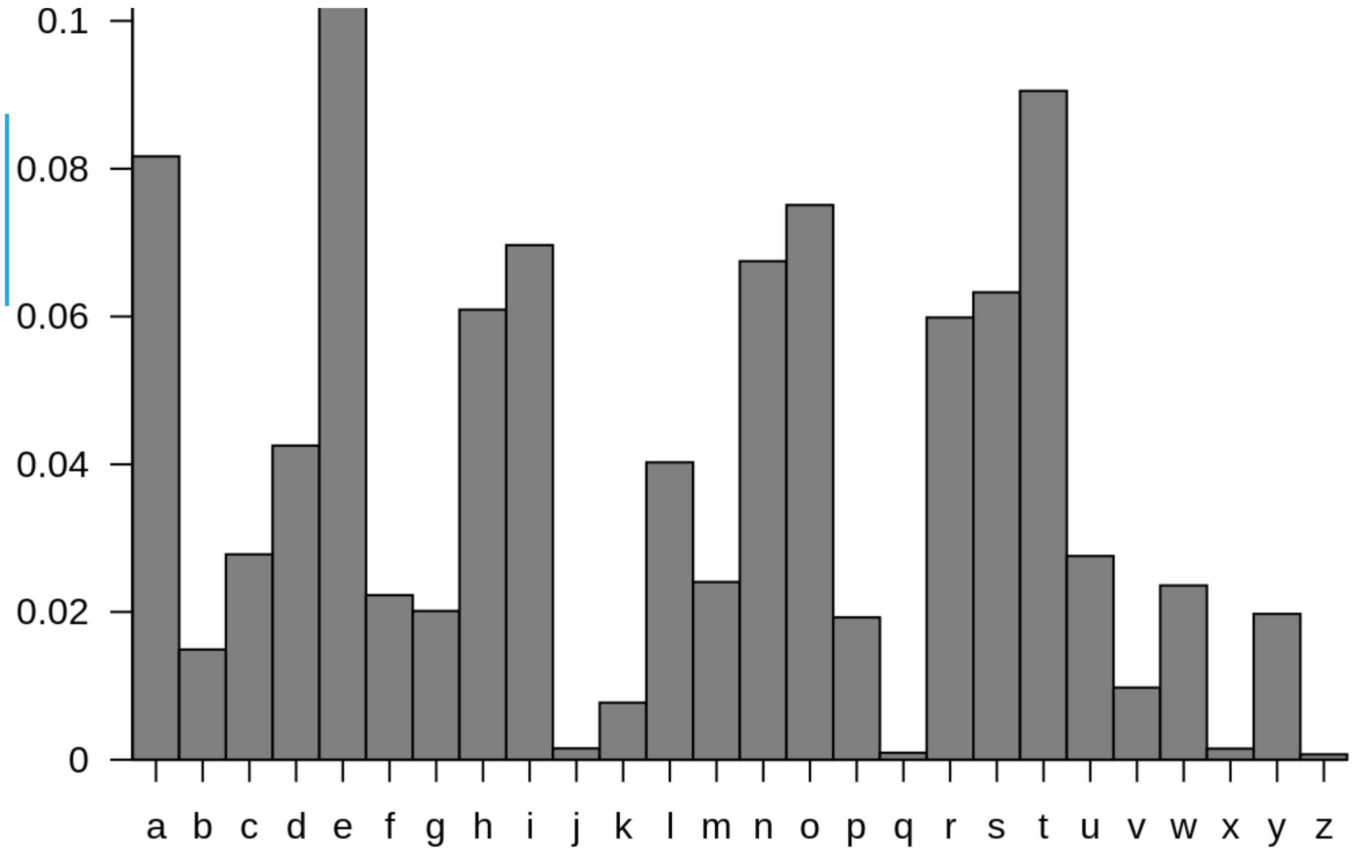


Let’s guess that the most common letter is “e”






this table servith
for to entre into
the table of equa
cion of the mone
on either side



FREQUENCY ATTACK!

- English has some letters far more common than others

FREQUENCY ATTACK!

- English has some letters far more common than others
- Give us tons of information about the likely cipher
- Breakable even by hand!
- Even if we try to hide by (say) mapping E to several characters

FREQUENCY ATTACK!

Key

Plaintext:	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
Ciphertext:	C	R	Y	P	T	O	G	R	A	M	5	6	7	8	9	B	D	E	F	H	I	J	K	L	N	Q
	1				2				3						4						S					
	U				V				W						X											
					Z																					

Message

Plaintext: THIS IS A SECRET MESSAGE

Ciphertext: HRAF AF C FTYE2H 7VFF1GZ

TRY IT OUT, EVE

- Message 1: gsv ovggvi v rh uivjfvmg rm gsrh nvhhztv dsrxs hslfow nzpv rg vzhrvi gl wvxlwv

- Message 2: gibrmt gl zelrw xlnnlm xszizxgvih nrtsg nzpv wvxibkgrlm nliv wruurxfog

https://www.guballa.de/substitution-solver

WHY IS THIS BAD?

- We’re not really mixing things up!
- E always stays the same (or mostly does)
- Words still stay together
  - If Eve decodes “the” it’s a big problem!

VIGENERE CIPHER

- Last of the “by-hand” ciphers
- Remained secure for 300 years!
  - WAY longer than any modern method

VIGENERE CIPHER

- Choose a long password
- Duplicate the password until it’s as long as the main text
- Use the letter in the password to encode the corresponding character in the main text

	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

VIGENERE CIPHER EXAMPLE

- Simple password: “PASSWORD”
- Text: WE LET THE LETTERS IN THE TEXT MAP TO DIFFERENT LETTERS

WE LET THE LETTERS IN THE TEXT MAP TO DIFFERENT LETTERS
PA SSW ORD PASSWOR DP ASS WORD PAS SW ORDPASSWO RDPASSW

LE DWP HYH AELLAFJ LC TZW PSOW BAH LK RZIUEJWJH CHITWJO

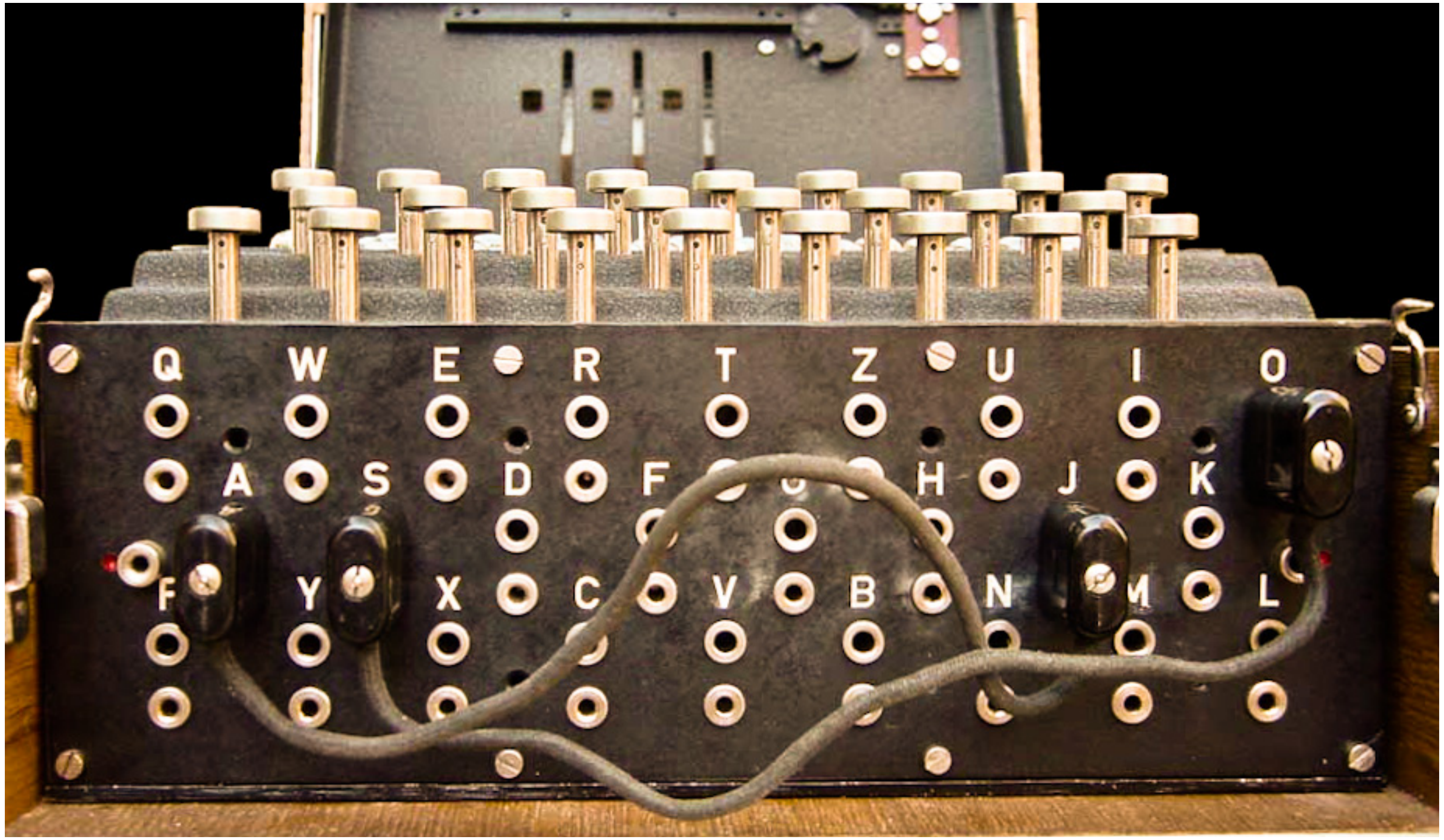
HOW TO DECRYPT?

- If the same word appears two times, AND it hits the same part of the password, then it's just a substitution cipher!

- If the password is as long as the text this is not a problem. (And, in fact, it cannot be decoded)
  - Cumbersome! Need to spend as much time exchanging keys as communicating

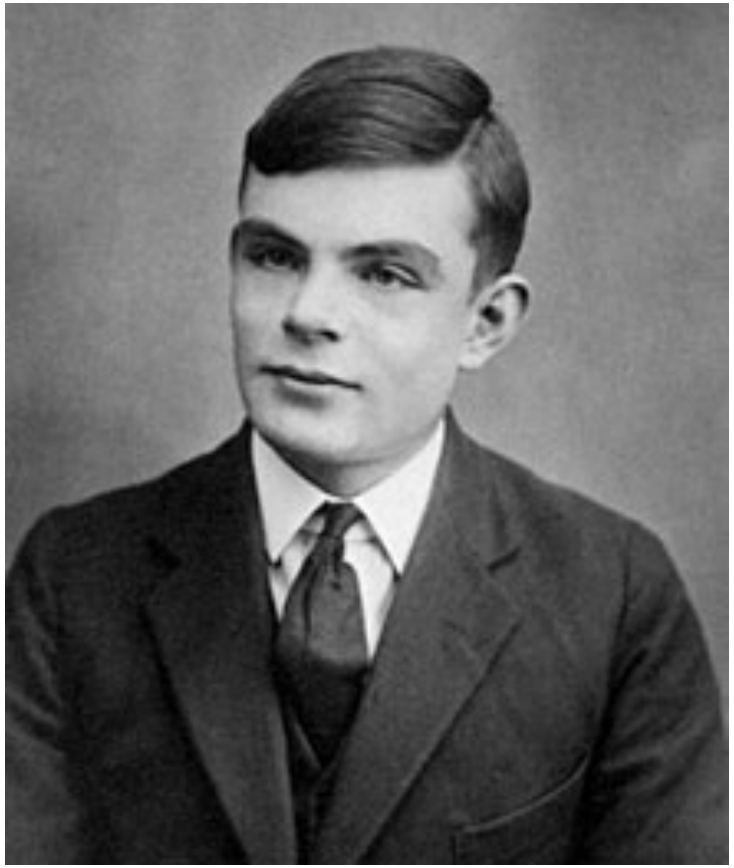
ENIGMA MACHINE

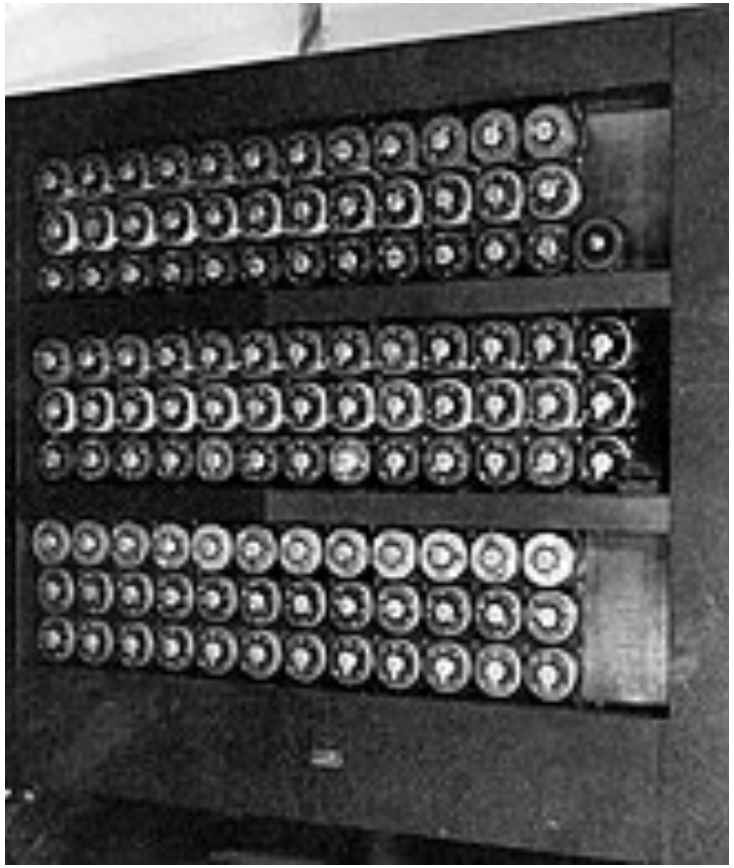
- Mechanical method used by Germany in WW2
- Each letter in the text changes the key (using rotating wheels)!
- Repeats every 17000 letters (never within one message)



ENIGMA MACHINE

- Also had wires on the back to change how the wheels interacted
- 159 quintillion possibilities





ATTACKING ENIGMA

- One of the first computer usages
- Alan Turing
- Poland, then Britain
- Broke the code!

ATTACKING ENIGMA

- Guess a likely message, try many many settings
- Missions recovered enigma machines and manuals
- Key mistakes:
  - The next day’s passcode (3 letters) was sent twice in a row at the beginning of a message
  - Letters could not be encoded to themselves
  - Frequent retransmissions using different codes

ATTACKING ENGIMA

- One story: Mavis Lever found a ciphertext that did not contain the letter L
- What can you learn from that?
- Probably: test message LLLLLLLLLLL….

ENIGMA VS BOMBE

- Key to the war effort
- Major early computer usage
- Now machines do cryptography
- But they decrypt too!

MODERN PRIVATE-KEY CRYPTOGRAPHY: DES

- Developed at IBM in the 70s
- NSA made suggestions for improvement
- Suggested 56 bit key instead of 128 bit key for efficiency
- Too small! By 1998, a key could be cracked for $250,000

MODERN PRIVATE-KEY CRYPTOGRAPHY: AES

- Won a contest by NIST in 2001
- Approved by NSA for sensitive data
- Key: 128, 192, or 256 bits
- Known attacks are not much better than brute force

- You have used this many many many times today.
- Built into computers

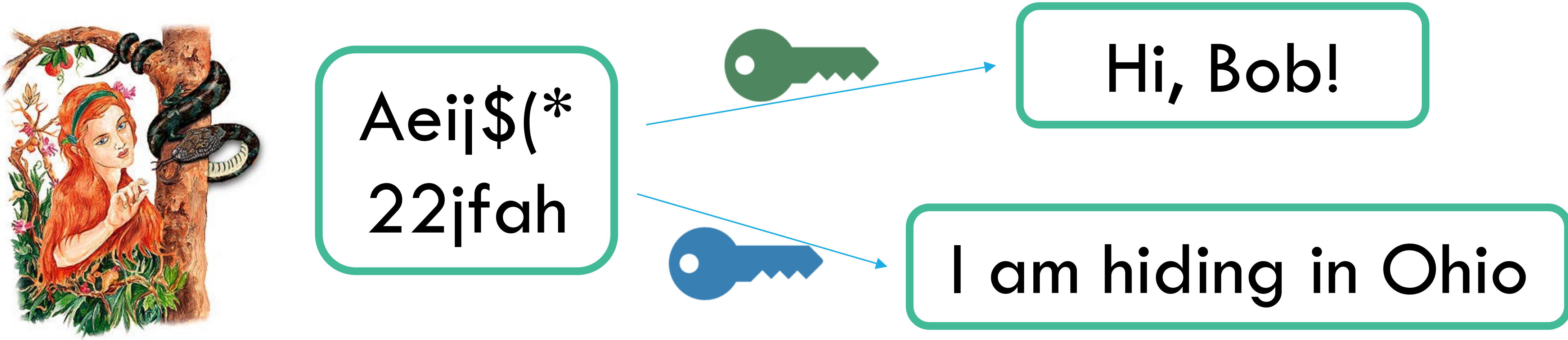
AES VISUALIZATION

- https://www.youtube.com/watch?v=mlzxpkdXP58
- https://aesencryption.net/

CAN WE EVER KNOW ENCRYPTION IS PERFECT?

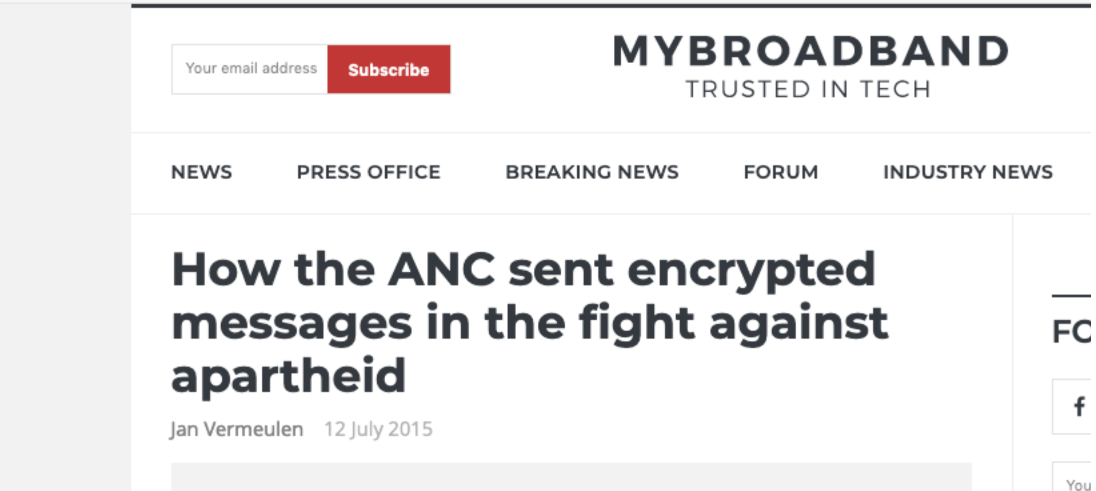
ONE-TIME PAD

- If key is as long as the message, AND only used once, it is impossible to recover the original text
- More formally: if Eve has a ciphertext C, there is uniform probability that any message M mapped to C



ONE-TIME PAD

- Why not use this??
- Tradeoff of efficiency
- Truly important messages (actual spies) are likely to use this



SOMETHING IS MISSING

- AES requires a (small) key
- How do you and Amazon exchange a key so that you can send them your credit card?

PUBLIC KEY CRYPTOGRAPHY

PUBLIC-KEY CRYPTOGRAPHY

- Goal: Alice and Bob publicly exchange messages
- Eve can see everything!
- But at the end, Alice and Bob share a key, Eve does not

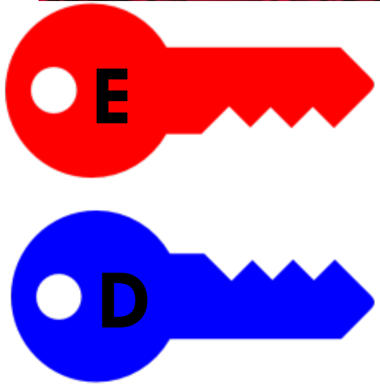
PRIVATE KEY CRYPTOGRAPHY REMINDER

- Need a key to get from an message (plaintext) to a difficult-to-decode cyphertext
- And back

- Insight: these can be different keys!
- Second insight: only one has to be private!

PUBLIC KEY ENCRYPTION

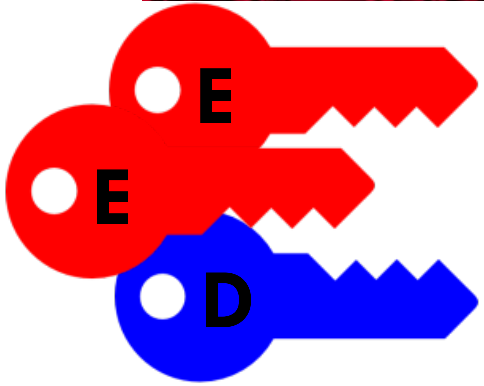
Hi,
Bob!



PUBLIC KEY ENCRYPTION

Alice can encrypt.
Eve can encrypt!
Alice cannot decrypt.
Eve cannot decrypt.

Hi,
Bob!

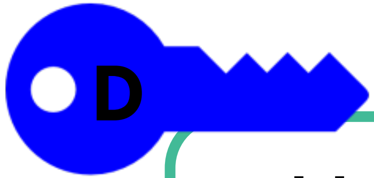


PUBLIC KEY ENCRYPTION

Hi, Bob!

Aeij$(* 22jfah

Aeij$(* 22jfah



Hi, Bob!

KEY EXCHANGE

- One important application of public-key cryptography
- Exchange messages to agree on a secret key
- Then, use this key for AES
  - Fast and secure

KEY EXCHANGE: HOW DOES IT WORK?

- Diffie-Helman as an example
- Diffie-Helman uses numbers
- We'll use Play-Doh
  - It's much more accurate then you'd think
- Split into two groups
- Goal: agree on a secret Play-Doh color

STEP 1: CREATE A SECRET COLOR

- Any color you want.
- Make 3 equal sized pieces of it.
- .5 inch sphere
- Don't show it to Eve!

STEP 2: MIX YOUR SECRET COLOR WITH THE PUBLIC COLOR

- Make sure it is .5 in
- Keep one of your 3 pieces unmixed. Mix the other two.
- This mixture is public

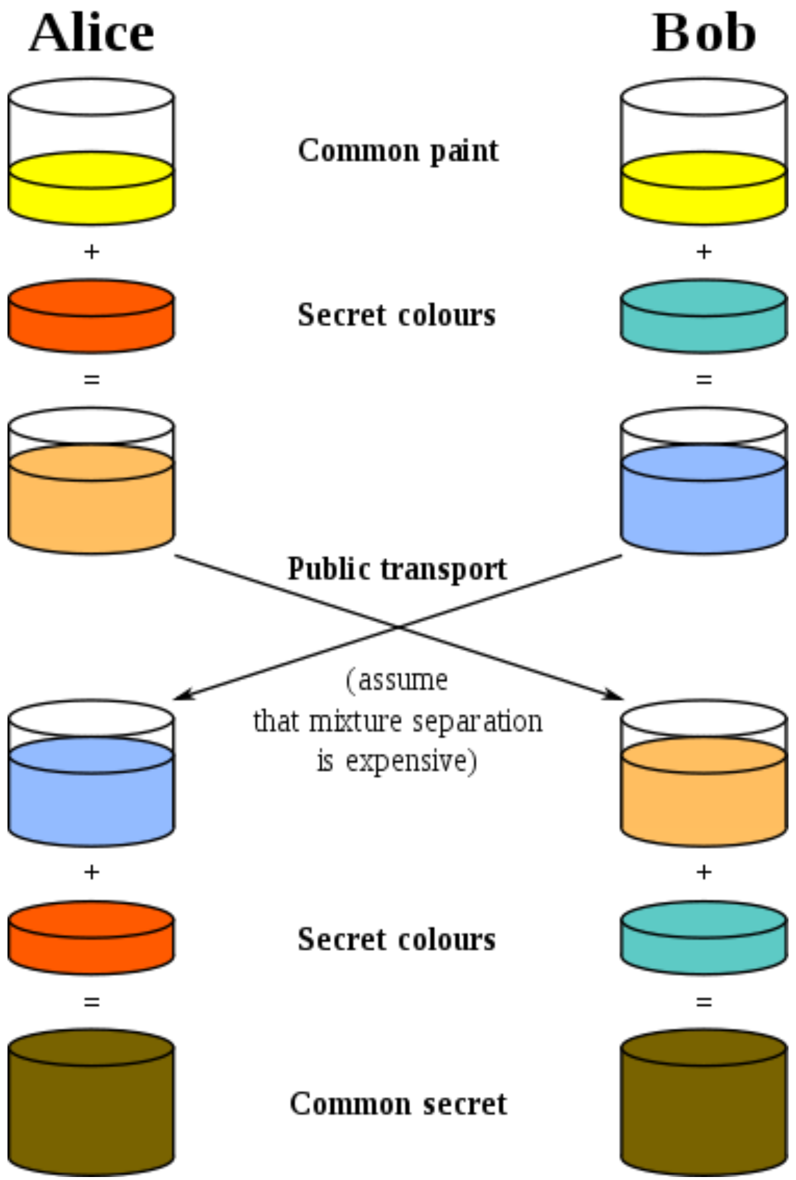
STEP 3: SEND YOUR MIXTURE TO THE OTHER GROUP

- Over the “network”---meaning through Eve!
- Eve can see the mixture (and take a piece)
- She can’t add to the mixture or modify it

STEP 4: COMBINE THE OTHER GROUP'S MIXTURE WITH YOUR SECRET MIXTURE

- What does your mixture consist of now?
  - 1 part your secret mixture
  - 1 part the other group's secret mixture
  - 1 part the public color
- The other group has the same final mixture!

DIAGRAM OF WHAT WE DID



HOW IT WORKS IN PRACTICE

- Instead of colors, we have numbers
- Rather than mixing, we use "modular exponentiation"
  - raise to a power and then take a modulo (meaning remainder)

- Diffie-Hellman was the first public "key exchange" system. It works *exactly* like our class activity, with these changes!

WHY DOES THIS WORK?

- Can't unmix paint!
- Even though Eve knows that what you sent was a combination of your secret color, mixed with the public color, she can't "unmix" it to get your secret color

- Does anyone have ideas for what Eve can do to try to get the shared secret mixture? Do they work?

INSTEAD OF PAINT: ONE-WAY COMPUTATION

- Easy to compute,
  Hard to reverse computation

- Easy: What is 28487532223 * 72342452989?
  - Easy on a computer -- about 100 digit-by-digit multiplications

- Hard: What are the factors of 2060857961121397335477?
  - Seems to require vast numbers of trial divisions

- NOTE: https does not use simple multiplication,
  it uses exponentiation in modulo arithmetic

$$f(a) = q^a \pmod{p}$$