Ciphers and Cryptography

Vanderbilt Math Club

April 1, 2019

Codes and secrets

- Since ancient times, people have tried to keep secrets.

Codes and secrets

- Since ancient times, people have tried to keep secrets.
- The ability to keep or steal secrets has changed the tide of war many times.

Codes and secrets

- Since ancient times, people have tried to keep secrets.
- The ability to keep or steal secrets has changed the tide of war many times.
- Today, information is the most valuable resource in the world. Stolen information can lose companies billions of dollars, let someone buy things with your bank account or hack into your computer.

Codes and secrets

- Since ancient times, people have tried to keep secrets.
- The ability to keep or steal secrets has changed the tide of war many times.
- Today, information is the most valuable resource in the world. Stolen information can lose companies billions of dollars, let someone buy things with your bank account or hack into your computer.

Group Question

If you had to send a secret message to a friend, how would you make sure no one else can read it?

History

- In WWII, at the dawn of the age of computers, codes and codebreakers played a huge role in the allied victory.

History

- In WWII, at the dawn of the age of computers, codes and codebreakers played a huge role in the allied victory.
- Here is a short video explaining one method the US used in the war: https://www.youtube.com/watch?v=5rSvm3m8ZUA

History

- In WWII, at the dawn of the age of computers, codes and codebreakers played a huge role in the allied victory.
- Here is a short video explaining one method the US used in the war: https://www.youtube.com/watch?v=5rSvm3m8ZUA
- The Germans had their famous Enigma machine, with daily changes in the code. Possibilities:

$$\approx 3000000000000000000000000000000000000000$$

$$000000000000000000000000000000000000000$$

$$000000000000000000000000000000000000(!)$$

(Photo credit: Alessandro Nassiri (CC BY-SA 4.0))

Steganography

- Two ways to send secrets: Send codes (cyrptography), and hide the *location* of the message (steganography).

Steganography

- Two ways to send secrets: Send codes (cyrptography), and hide the *location* of the message (steganography).
- Example: You shave a monk's head and tattoo a message on their head. Then you wait for their hair to grow. The monk then goes somewhere and the head is shaved again.

Steganography

- Two ways to send secrets: Send codes (cyrptography), and hide the *location* of the message (steganography).
- Example: You shave a monk's head and tattoo a message on their head. Then you wait for their hair to grow. The monk then goes somewhere and the head is shaved again.
- Do you see anything unusual about this image?

Steganography

- Two ways to send secrets: Send codes (cyrptography), and hide the *location* of the message (steganography).
- Example: You shave a monk's head and tattoo a message on their head. Then you wait for their hair to grow. The monk then goes somewhere and the head is shaved again.
- Do you see anything unusual about this image?

Steganography

- Two ways to send secrets: Send codes (cyrptography), and hide the *location* of the message (steganography).
- Example: You shave a monk's head and tattoo a message on their head. Then you wait for their hair to grow. The monk then goes somewhere and the head is shaved again.
- Do you see anything unusual about this image?

- Pixels were changed to hide the picture of a cat, but its unnoticeable! (Photo Credit: Wiki user Cyp (CC BY-SA 3.0))

Basic terminology

- To get started with our own codes, we need a few *terms*.

Basic terminology

- To get started with our own codes, we need a few *terms*.
- Plaintext: The message you want to send, anyone can read!

Basic terminology

- To get started with our own codes, we need a few *terms*.
- Plaintext: The message you want to send, anyone can read!
- Cipher: A method of encrypting a message to hide its meaning.

Basic terminology

- To get started with our own codes, we need a few *terms*.
- Plaintext: The message you want to send, anyone can read!
- Cipher: A method of encrypting a message to hide its meaning.
- Ciphertext: The encrypted message. Looks like nonsense to most!

Basic terminology

- To get started with our own codes, we need a few *terms*.
- Plaintext: The message you want to send, anyone can read!
- Cipher: A method of encrypting a message to hide its meaning.
- Ciphertext: The encrypted message. Looks like nonsense to most!
- Decryption: The process of turning ciphertext back into readable plaintext.

Substitution ciphers

- Caesar Cipher: Shift all letters left by 3 (wrap around at end):

Substitution ciphers

- Caesar Cipher: Shift all letters left by 3 (wrap around at end):

plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M
ciphertext	X	Y	Z	**A**	**B**	**C**	D	E	F	G	H	I	J

plaintext	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ciphertext	K	L	M	N	O	P	Q	R	S	T	U	V	W

Substitution ciphers

- Caesar Cipher: Shift all letters left by 3 (wrap around at end):

plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M
ciphertext	X	Y	Z	**A**	**B**	**C**	D	E	F	G	H	I	J

plaintext	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ciphertext	K	L	M	N	O	P	Q	R	S	T	U	V	W

Group Question

Use this cipher to encryrpt the message "NASHVILLE".

Substitution ciphers

- Caesar Cipher: Shift all letters left by 3 (wrap around at end):

plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M
ciphertext	X	Y	Z	**A**	**B**	**C**	D	E	F	G	H	I	J

plaintext	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ciphertext	K	L	M	N	O	P	Q	R	S	T	U	V	W

Group Question

Use this cipher to encryrpt the message "NASHVILLE".

Group Question

Decrypt the message "OXFPB VLRO OFDEQ EXKA'.

Substitution ciphers

- Caesar Cipher: Shift all letters left by 3 (wrap around at end):

plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M
ciphertext	X	Y	Z	**A**	**B**	**C**	D	E	F	G	H	I	J

plaintext	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ciphertext	K	L	M	N	O	P	Q	R	S	T	U	V	W

Group Question

Use this cipher to encryrpt the message "NASHVILLE".

Group Question

Decrypt the message "OXFPB VLRO OFDEQ EXKA'.

Group Question

Split into pairs. Pick a message, make a shift cipher by shifting by some number of letters, and encrypt your message. Now swap messages with your partner. Can you break their code?

Breaking codes

- This code is not hard to break.

Breaking codes

- This code is not hard to break.
- If you knew your friend used this method, how would you crack the code?

Breaking codes

- This code is not hard to break.
- If you knew your friend used this method, how would you crack the code?
- Basic attack: *Brute force:* Shift by all possibilities; only 26.

Breaking codes

- This code is not hard to break.
- If you knew your friend used this method, how would you crack the code?
- Basic attack: *Brute force:* Shift by all possibilities; only 26.
- Then check which make sense.

Breaking codes

- This code is not hard to break.
- If you knew your friend used this method, how would you crack the code?
- Basic attack: *Brute force:* Shift by all possibilities; only 26.
- Then check which make sense.

Group Question

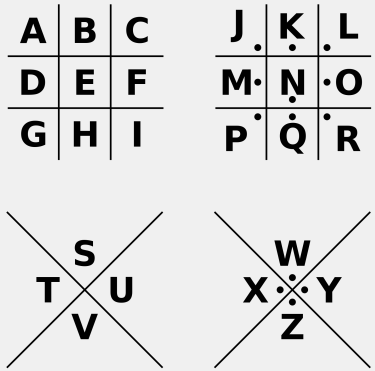
Make a new code and exchange with a friend again. Can you break their code this time if you couldn't last time?

Geometric codes

- Pigpen cipher: replaces letters by simple shapes which can be remembered by a simple rule:

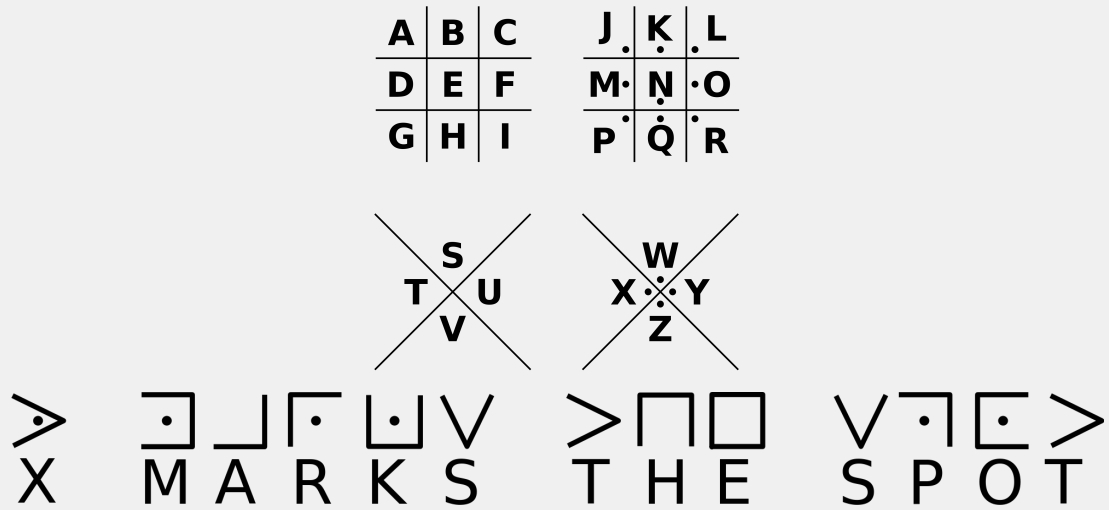
Geometric codes

- Pigpen cipher: replaces letters by simple shapes which can be remembered by a simple rule:



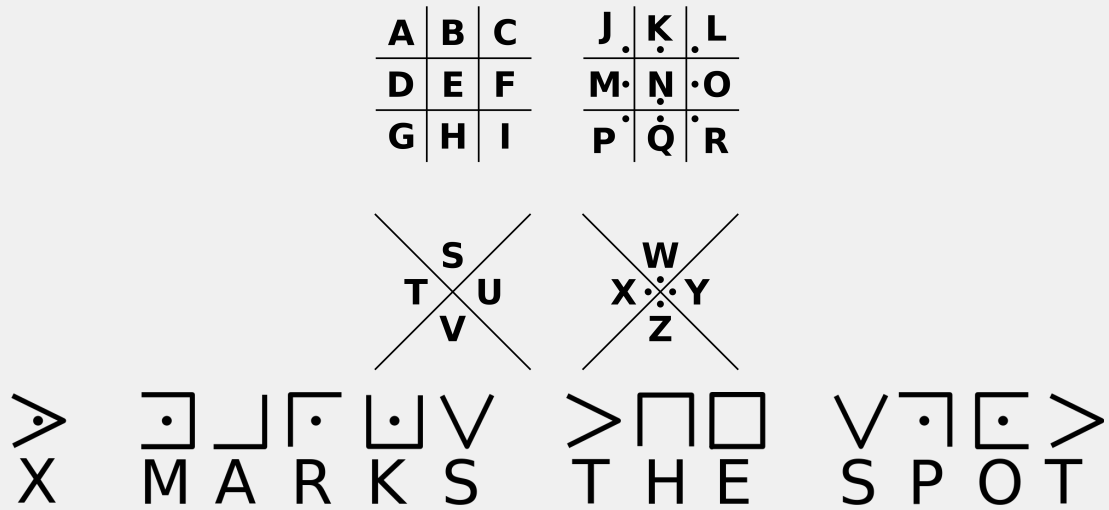
Geometric codes

- Pigpen cipher: replaces letters by simple shapes which can be remembered by a simple rule:



Geometric codes

- Pigpen cipher: replaces letters by simple shapes which can be remembered by a simple rule:



Group Question

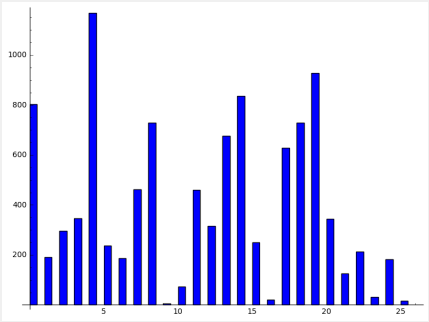
Encrypt the message "Superspy" in pigpen.

Probabilistic attacks

- In any scheme where you map all the letters to other letters or symbols, there is an attack: *frequency analysis*.

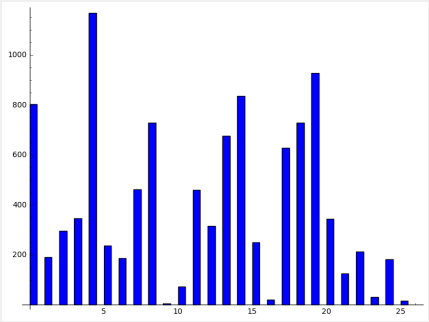
Probabilistic attacks

- In any scheme where you map all the letters to other letters or symbols, there is an attack: *frequency analysis*.
- Bar chart of how often the letters ‘a’ through ‘z’ appear on the current Nashville Math Club “For current students” page:

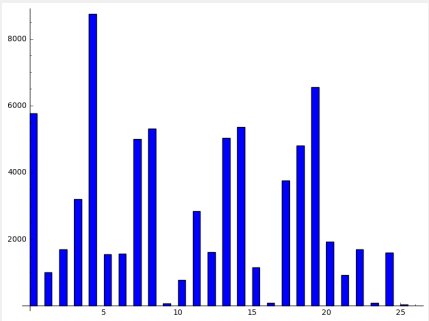


Probabilistic attacks

- In any scheme where you map all the letters to other letters or symbols, there is an attack: *frequency analysis*.
- Bar chart of how often the letters ‘a’ through ‘z’ appear on the current Nashville Math Club “For current students” page:



- Bar chart of how often the letters ‘a’ through ‘z’ appear in the first 10 chapters of Anna Karenina:



Frequency analysis example

- Given a large set of encrypted with the same code, all sets will have a similar "distribution". 'E' is most common.

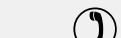
Frequency analysis example

- Given a large set of encrypted with the same code, all sets will have a similar "distribution". 'E' is most common.
- Even if you can guess several letters, you can often figure out the code by context.

Frequency analysis example

- Given a large set of encrypted with the same code, all sets will have a similar "distribution". 'E' is most common.
- Even if you can guess several letters, you can often figure out the code by context.

Group Question

You had a large set of text and drew the bar charts. You are pretty confident that the chart has identified the 7 most common letters as: E=  , T=  , A=, O=  , I=  , N=  , S=  .
The first sentence is given below. What does it say?
      , 
     .

Better codes

- How can we avoid attacks like this?

Better codes

- How can we avoid attacks like this?
- Any system where “all the letters” go “one-by-one” to other letters or symbols can be broken this way eventually.

Better codes

- How can we avoid attacks like this?
- Any system where “all the letters” go “one-by-one” to other letters or symbols can be broken this way eventually.
- We can use numbers to come up with much more complicated ways to encrypt message.

Better codes

- How can we avoid attacks like this?
- Any system where "all the letters" go "one-by-one" to other letters or symbols can be broken this way eventually.
- We can use numbers to come up with much more complicated ways to encrypt message.
- First, we can associate to each letter a number, $A = 1$, $B = 2$, ... $Z = 26$.

Better codes

- How can we avoid attacks like this?
- Any system where "all the letters" go "one-by-one" to other letters or symbols can be broken this way eventually.
- We can use numbers to come up with much more complicated ways to encrypt message.
- First, we can associate to each letter a number, $A = 1$, $B = 2$, ... $Z = 26$.
- Then we can do mathematical operations to the numbers.

Clock Arithmetic

- First, we need a funny way to add and multiply numbers.

Clock Arithmetic

- First, we need a funny way to add and multiply numbers.
- If it is 8:00 now, what time will it be in 5 hours? 11 hours?

Clock Arithmetic

- First, we need a funny way to add and multiply numbers.
- If it is 8:00 now, what time will it be in 5 hours? 11 hours?
- A clock has 12 numbers on it, and each hour the short hand goes up one number. After 12, it wraps around back to 1.

Clock Arithmetic

- First, we need a funny way to add and multiply numbers.
- If it is 8:00 now, what time will it be in 5 hours? 11 hours?
- A clock has 12 numbers on it, and each hour the short hand goes up one number. After 12, it wraps around back to 1.
- We could also make clocks with different numbers of hours.

Clock Arithmetic

- First, we need a funny way to add and multiply numbers.
- If it is 8:00 now, what time will it be in 5 hours? 11 hours?
- A clock has 12 numbers on it, and each hour the short hand goes up one number. After 12, it wraps around back to 1.
- We could also make clocks with different numbers of hours.
- Clock arithmetic rules: to add or multiply numbers "modulo N", add or multiply them as usual. If the number gets outside of the set of numbers $1, 2, \ldots, N$, then shift by N as many times as you need to get back in this range. Instead of writing $=$, we right $\equiv$.

Clock Arithmetic

- First, we need a funny way to add and multiply numbers.
- If it is 8:00 now, what time will it be in 5 hours? 11 hours?
- A clock has 12 numbers on it, and each hour the short hand goes up one number. After 12, it wraps around back to 1.
- We could also make clocks with different numbers of hours.
- Clock arithmetic rules: to add or multiply numbers "modulo N", add or multiply them as usual. If the number gets outside of the set of numbers $1, 2, \ldots, N$, then shift by N as many times as you need to get back in this range. Instead of writing $=$, we right $\equiv$.
- Example: Modulo 5, $3 + 4 = 7 \equiv 2$, and $3 \cdot 4 = 12 \equiv 12 - 5 \equiv 7 \equiv 7 - 5 \equiv 2$. On a 5-hour clock, if you add 3 hours 4 times, you've moved 2 hours ahead.

Clock Arithmetic Problems

Group Question

Find the following numbers in clock arithmetic:

- *Modulo* 2*:*

$$1+1, \qquad 2\cdot 1+3, \qquad 5\cdot 7.$$

Clock Arithmetic Problems

Group Question

Find the following numbers in clock arithmetic:

- *Modulo* 2*:*

$$1+1, \qquad 2\cdot 1+3, \qquad 5\cdot 7.$$

What does the clock arithmetic of a whole number modulo 2 *tell you about the number?*

Clock Arithmetic Problems

Group Question

Find the following numbers in clock arithmetic:

- *Modulo* 2*:*

$$1+1, \qquad 2\cdot 1+3, \qquad 5\cdot 7.$$

What does the clock arithmetic of a whole number modulo 2 *tell you about the number?*

- *Modulo 4:*

$$1+1, \qquad 2\cdot 1+3, \qquad 5\cdot 7.$$

Clock Arithmetic Problems

Group Question

Find the following numbers in clock arithmetic:

- *Modulo 2:*

$$1+1, \qquad 2\cdot 1+3, \qquad 5\cdot 7.$$

What does the clock arithmetic of a whole number modulo 2 tell you about the number?

- *Modulo 4:*

$$1+1, \qquad 2\cdot 1+3, \qquad 5\cdot 7.$$

- *Modulo 6:*

$$4\cdot 5, \qquad -20, \qquad 18.$$

Clock Arithmetic Problems

Group Question

Find the following numbers in clock arithmetic:

- *Modulo* 2*:*

$$1+1, \qquad 2\cdot 1+3, \qquad 5\cdot 7.$$

What does the clock arithmetic of a whole number modulo 2 *tell you about the number?*

- *Modulo 4:*

$$1+1, \qquad 2\cdot 1+3, \qquad 5\cdot 7.$$

- *Modulo 6:*

$$4\cdot 5, \qquad -20, \qquad 18.$$

- *What does it mean for number to be* 0 *in clock arithmetic?*

Caesar cipher again

Caesar cipher again

- Encryption: Turn letters into numbers "modulo" 26. Add a number, like -3 or some shift, to each number modulo 26. Then convert back into letters.

Caesar cipher again

- Encryption: Turn letters into numbers "modulo" 26. Add a number, like -3 or some shift, to each number modulo 26. Then convert back into letters.
- Decryption: Do the same, but add the negative of the first number shift!

Caesar cipher again

- Encryption: Turn letters into numbers "modulo" 26. Add a number, like -3 or some shift, to each number modulo 26. Then convert back into letters.
- Decryption: Do the same, but add the negative of the first number shift!
- Example: Encryption scheme is subtract 3: Plaintext="MATH"$\rightarrow 13, 1, 20, 8 \rightarrow 10, 1 - 3 \equiv 24, 17, 5 \rightarrow$"JXQE"=Ciphertext.

Caesar cipher again

- Encryption: Turn letters into numbers "modulo" 26. Add a number, like -3 or some shift, to each number modulo 26. Then convert back into letters.
- Decryption: Do the same, but add the negative of the first number shift!
- Example: Encryption scheme is subtract 3: Plaintext="MATH"$\to 13, 1, 20, 8 \to 10, 1 - 3 \equiv 24, 17, 5 \to$"JXQE"=Ciphertext.
- Decryption: Convert to numbers, add 3, convert to letters: "JXQE"$\to 10, 24, 17, 5 \to 13, 1, 20, 7 \to$ "MATH".

A better cipher

- Caesar formula: Pick a number D, then send every number x to $x + D$ modulo 26.

A better cipher

- Caesar formula: Pick a number D, then send every number x to $x + D$ modulo 26.
- More complicated choice: *affine cipher*. Pick numbers C and D. Send every x to $Cx + D$ modulo 26.

A better cipher

- Caesar formula: Pick a number D, then send every number x to $x + D$ modulo 26.
- More complicated choice: *affine cipher*. Pick numbers C and D. Send every x to $Cx + D$ modulo 26.
- Example: $C = 5,\ D = 4$.
  Plaintext="CAR" $\to 3, 1, 18 \to 3 \cdot 5 + 4 = 19, 1 \cdot 5 + 4 = 9, 18 \cdot 5 + 4 = 94 \equiv 16 \to$"SIP"=Ciphertext.

A better cipher

- Caesar formula: Pick a number D, then send every number x to $x + D$ modulo 26.
- More complicated choice: *affine cipher*. Pick numbers C and D. Send every x to $Cx + D$ modulo 26.
- Example: $C = 5,\ D = 4$.
  Plaintext="CAR" $\to 3, 1, 18 \to 3 \cdot 5 + 4 = 19, 1 \cdot 5 + 4 = 9, 18 \cdot 5 + 4 = 94 \equiv 16 \to$"SIP"=Ciphertext.
- Bad choice: $C = 2,\ D = 1$. Then $A \to 1 \mapsto 2 \cdot 1 + 1 = 3 \to C$ but $N \to 14 \mapsto 14 \cdot 2 + 1 = 29 \equiv 3 \to C$. Can't be undone!

Decryption

- If you use an affine cipher, then how do you decrypt ciphertext back into plaintext?

Decryption

- If you use an affine cipher, then how do you decrypt ciphertext back into plaintext?
- Caesar cipher: To undo adding D, add $-D$.

Decryption

- If you use an affine cipher, then how do you decrypt ciphertext back into plaintext?
- Caesar cipher: To undo adding D, add $-D$.
- What function "undoes" $f(x) \equiv Cx + D$ modulo 26?

Decryption

- If you use an affine cipher, then how do you decrypt ciphertext back into plaintext?
- Caesar cipher: To undo adding D, add $-D$.
- What function "undoes" $f(x) \equiv Cx + D$ modulo 26?

Group Question

Magic Claim: The $C = 5$, $D = 4$ cipher is undone by applying a $C_2 = -5$, $D_2 = -6$ affine cipher. Check this for any 3 letters.

Decryption

- If you use an affine cipher, then how do you decrypt ciphertext back into plaintext?
- Caesar cipher: To undo adding D, add $-D$.
- What function "undoes" $f(x) \equiv Cx + D$ modulo 26?

Group Question

Magic Claim: The $C = 5$, $D = 4$ cipher is undone by applying a $C_2 = -5$, $D_2 = -6$ affine cipher. Check this for any 3 letters.

Fact (From number theory)

If C is even or a multiple of 13 (note: $26 = 2 \cdot 23$), then there is no way to undo the affine cipher. If C is odd and not a multiple of 13, then there is a magic choice of C_2, D_2 which undoes the cipher.

Affine ciphers can also be broken!

- Take a few minutes and try to crack the following code:

Group Question

"Gwn qzadg unadro zo gwn arrl gr gnii ln gwn hrira rq gwn dfv tngd b hbokv eba".

Affine ciphers can also be broken!

- Take a few minutes and try to crack the following code:

Group Question

"Gwn qzadg unadro zo gwn arrl gr gnii ln gwn hrira rq gwn dfv tngd b hbokv eba".

- Harder challenge if I split the letters into blocks of 5 so you can't guess easy words!

Affine ciphers can also be broken!

- Take a few minutes and try to crack the following code:

Group Question

"Gwn qzadg unadro zo gwn arrl gr gnii ln gwn hrira rq gwn dfv tngd b hbokv eba".

- Harder challenge if I split the letters into blocks of 5 so you can't guess easy words!
- More statistics: what double letters, other patterns are most common in English?

Group analysis (Frequencies: E,T,A,O,I,N,S)

- IWO WBCVO VIBBT BD Q VULPWI ELVO ZCVI BD IWO OTPO BS IWO XLUUQPO. LI VIBBT BD LIV BAD QDT UBBMOT BXOE Q REBQT VYEOQT BS AOVI KBCDIEN SQEHUQDT. DBI Q EOHQEMQRUO WBCVO RN QDN HOQDV LI AQV QRBCI IWLEIN NOQEV BUT, VJCQIILVW, VJCQELVW, HQTO BS RELKM, QDT WQT SBCE ALDTBAV VOI LD IWO SEBDI BS Q VLFO QDT YEBYBEILBD AWLKW HBEO BE UOVV OGQKIUN SQLUOT IB YUOQVO IWO ONO. IWO BDUN YOEVBD SBE AWBH IWO WBCVO AQV LD QDN AQN VYOKLQU AQV QEIWCE TODI, QDT IWQI AQV BDUN ROKQCVO LI WQYYODOT IB RO IWO BDO WO ULXOT LD. WO WQT ULXOT LD LI SBE QRBCI IWEOO NOQEV, OXOE VLDKO WO WQT HBXOT BCI BS UBDTBD ROKQCVO LI HQTO WLH DOEXBCV QDT LEELIQRUO. WO AQV QRBCI IWLEIN QV AOUU, TQEM WQLEOT QDT DOXOE JCLIO QI OQVO ALIW WLHVOUS.

At-home resource

- Fun web applet by Darrin Doud at BYU:
  `https://math.byu.edu/~doud/Substitution/`

One time ciphers

- One-time pad cipher: Pick a key; maybe a word or a phrase you can remember. Must be longer than plaintext.

One time ciphers

- One-time pad cipher: Pick a key; maybe a word or a phrase you can remember. Must be longer than plaintext.
- Add all letters in plaintext to letters in key one at a time.

One time ciphers

- One-time pad cipher: Pick a key; maybe a word or a phrase you can remember. Must be longer than plaintext.
- Add all letters in plaintext to letters in key one at a time.
- Example: Key="Cat"$= 3, 1, 20$, Plaintext="Man"$= 13, 1, 14$. Ciphertext=$3 + 13 = 26, 1 + 1 = 2, 20 + 14 = 34 \equiv 8$=Z,B,H.

One time ciphers

- One-time pad cipher: Pick a key; maybe a word or a phrase you can remember. Must be longer than plaintext.
- Add all letters in plaintext to letters in key one at a time.
- Example: Key="Cat"$= 3, 1, 20$, Plaintext="Man"$= 13, 1, 14$. Ciphertext=$3 + 13 = 26, 1 + 1 = 2, 20 + 14 = 34 \equiv 8$=Z,B,H.

Group Question

Example: Key="Krusty Krab", Plaintext="SPONGEBOBX" (pad with X's to make it same length as key). Encrypt the message.

One time ciphers

- One-time pad cipher: Pick a key; maybe a word or a phrase you can remember. Must be longer than plaintext.
- Add all letters in plaintext to letters in key one at a time.
- Example: Key="Cat"$= 3, 1, 20$, Plaintext="Man"$= 13, 1, 14$. Ciphertext=$3 + 13 = 26, 1 + 1 = 2, 20 + 14 = 34 \equiv 8$=Z,B,H.

Group Question

Example: Key="Krusty Krab", Plaintext="SPONGEBOBX" (pad with X's to make it same length as key). Encrypt the message.

Group Question

Is this secure from spies? Is it time-efficient?

RSA

- This last cipher was better, but you have to only send short messages or remember a long code.

RSA

- This last cipher was better, but you have to only send short messages or remember a long code.
- Modern day application: millions of people need to send credit card numbers to Amazon, and time is crucial.

RSA

- This last cipher was better, but you have to only send short messages or remember a long code.
- Modern day application: millions of people need to send credit card numbers to Amazon, and time is crucial.
- Big idea (1970's): RSA algorithm.

RSA

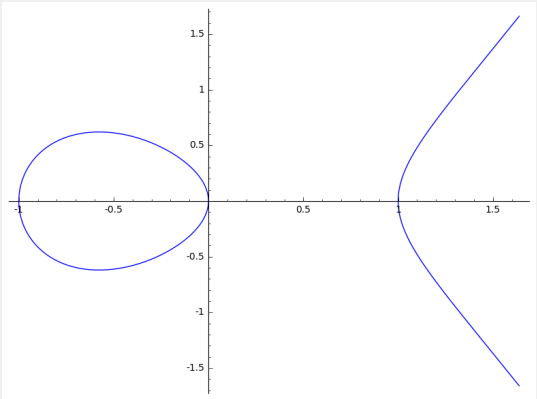
- This last cipher was better, but you have to only send short messages or remember a long code.
- Modern day application: millions of people need to send credit card numbers to Amazon, and time is crucial.
- Big idea (1970's): RSA algorithm.
- More recent ideas (more secure than RSA): use geometry!

RSA

- This last cipher was better, but you have to only send short messages or remember a long code.
- Modern day application: millions of people need to send credit card numbers to Amazon, and time is crucial.
- Big idea (1970's): RSA algorithm.
- More recent ideas (more secure than RSA): use geometry!
- Future: quantum computers can break all these codes, we need new ones!

RSA

- This last cipher was better, but you have to only send short messages or remember a long code.
- Modern day application: millions of people need to send credit card numbers to Amazon, and time is crucial.
- Big idea (1970's): RSA algorithm.
- More recent ideas (more secure than RSA): use geometry!
- Future: quantum computers can break all these codes, we need new ones!



Invent your own cipher!

Group Question

Come up with as many new ciphers as you can! Test these out on the people around you and see if you can invent an unbreakable code.