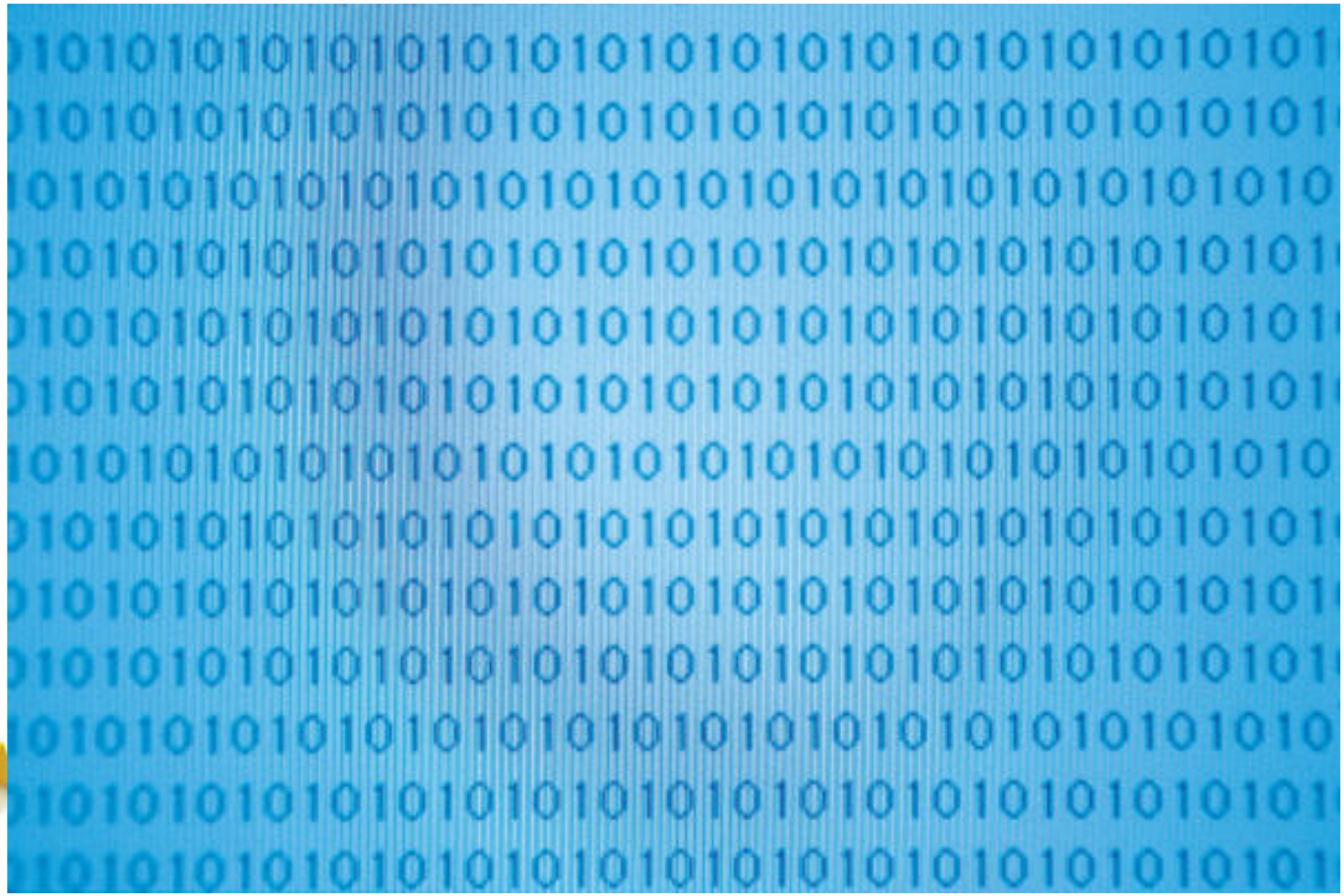
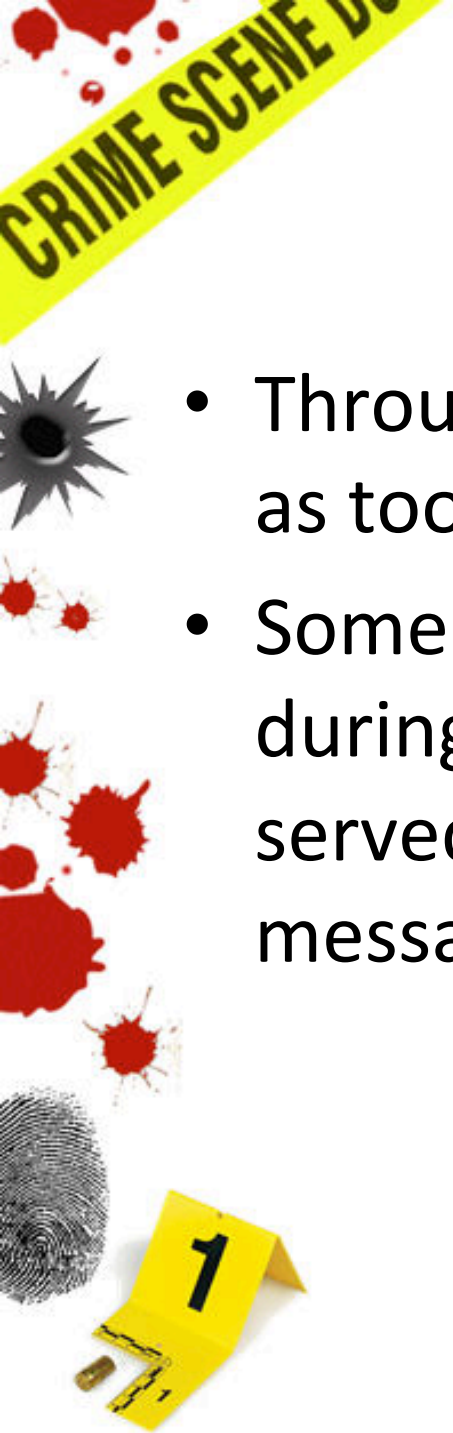
Code Making & Breaking

Let’s try to create and break some codes!



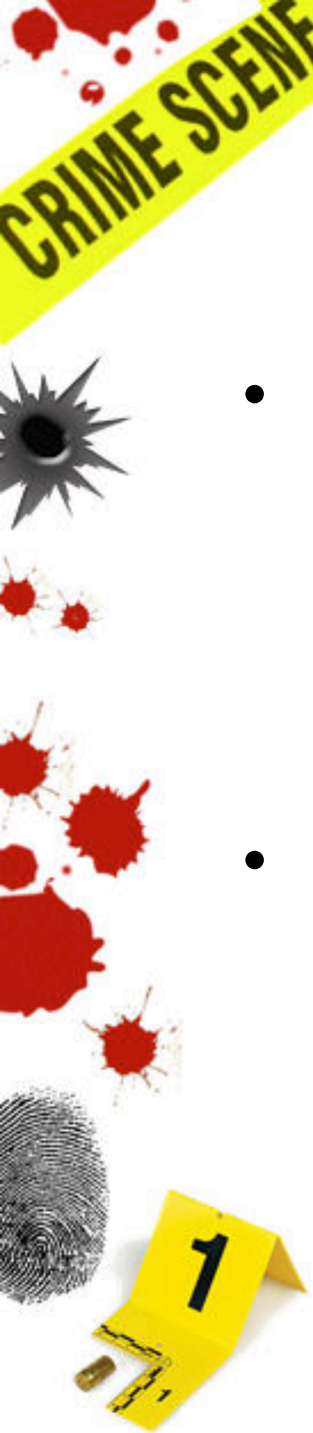
Vocabulary

- **Cryptography:** The practice and study of techniques for writing or solving codes.
- **Cipher**: Any method of transforming a message to conceal its meaning.
- **Encrypt:** Convert information into a cipher
- **Decrypt:** Something that has been decoded
- **Ciphertext:** Ciphertext is encrypted text.
- **Plaintext**: Plaintext is what you have before encryption
- **Key**: Number of “shifts” to decrypt a message



Cryptography Throughout History

- Throughout history, ciphers have been used as tools to convey secret messages.
- Some are ancient, and some were created during the birth of our country, but all have served the same purpose; to send secret messages!

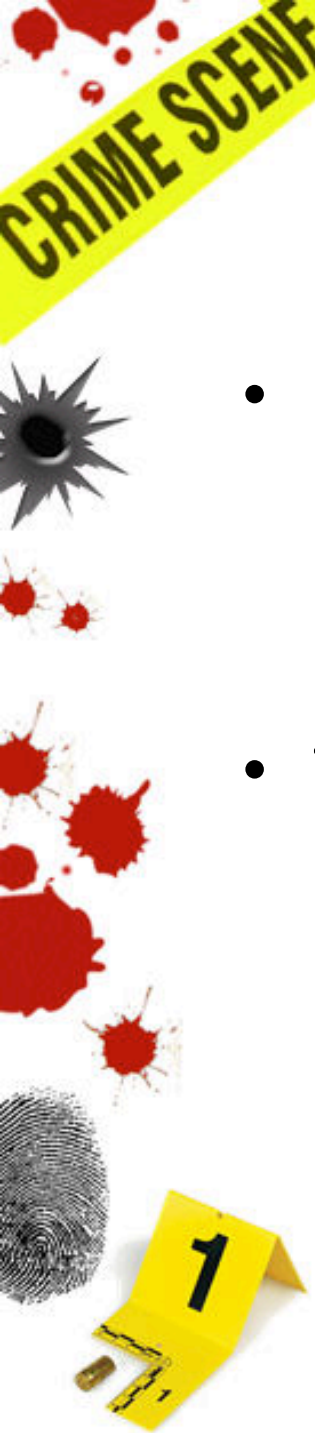


Cryptography Throughout History

- Let's go back to the American Revolutionary War for a quick example. Suppose that a valuable piece of information regarding the British Army's plan to attack an American encampment was intercepted by local militia.
- Since this is 1776 and therefore pre-iPhone, General Washington couldn't just shoot a quick text to the commanding officers at the encampment in question.

Cryptography Throughout History

- He would have to send a messenger who would either transport some form of written correspondence, or have the messenger memorize the message.
- The messenger must now travel through miles and miles of enemy territory risking capture and death in order to relay the message.

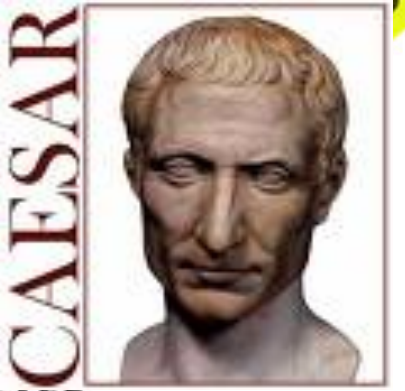


Cryptography Throughout History

- And what if he was intercepted? The British captors could have simply killed the messenger on sight, putting an end to the communication.
- They could have “persuaded” him to share the contents of the message, which would then render the information useless.
- Or, if the messenger was a friend of Benedict Arnold’s, the British could have simply bribed the messenger to spread false information, resulting in the deaths of thousands of American militia.

Cryptography Throughout History

- However, with the careful application of cryptography, Washington could have applied an encryption method known as a cipher to keep the contents of the message safe from enemy hands.
- Assuming that he entrusted the cipher to only his most loyal officers, this tactic would ensure that even if the message was intercepted, the messenger would have no knowledge of its contents.
- The data would therefore be indecipherable and useless to the enemy.



Other Codes in History

A *Caesar cipher*

- Caesar, Emperor of Rome 100-44B.C.
- His cipher used letters that are replaced by other letters a certain distance, or shift, ahead in the alphabet.
- He used this method to communicate with Roman army.
- His generals knew the shift so they would be the only ones who could read the encrypted message

Other Codes in History

World War II German Enigma Machine:

During World War II, the Germans were using an encryption code called Enigma – which was basically an encryption machine that encrypted messages for transmission.

Most communications were sent via radio, which means that allied forces could listen in on their communications – hence the need for encryption.

Other Codes in History

The Enigma code went many years unbroken – until the code breakers at London's Bletchley Park (including the Alan Turing) discovered a fatal flaw in the Enigma system, and eventually aided in the victory over the Nazi's.

It has been claimed that as a result of the information gained by breaking the Enigma code, hostilities between Germany and the Allied forces were shortened by two years.

Other Codes in History

Navajo Code-Talkers WW2:

- Syntax, tonal qualities, dialects make it unintelligible to anyone without extensive exposure and training.
- It used no alphabet or symbols
- Spoken only on the Navajo lands of the American Southwest.
- Less than 30 non-Navajos, none of them Japanese, could understand the language at the outbreak of World War II.
- Each “talker” had a body guard to protect him

NAMES OF ORGANIZATIONS (Con't)

MILITARY MEANING	NAVAJO PRONUNCIATION	NAVAJO MEANING
Battalion	Tacheene	Red Boil
Company	Nakia	Mexican
Platoon	Haa-clish-nih	Mud
Section	Yo-ih	Beads
Squad	Debeh-li-zini	Black Sheep

COMMUNICATION NAMES

MILITARY MEANING	NAVAJO PRONUNCIATION	NAVAJO MEANING
Telephone	Besh-hal-ne-ih	Telephone
Switchboard	Ya-ih-e-tih-ih	Central
Wire	Besh-le-chee-ih	Copper
Telegraph	Besh-le-chee-ih-beh-hane-ih	Comm by copper wire
Semaphore	Dah-na-a-tah-ih-beh-hane-ih	Flag Signals
Blinker	Coh-nil-kol-lih	Fire Blinder
Radio	Nil-chi-hal-ne-ih	Radio
Panels	Az-kad-be-ha-ne-ih	Carpet Signals

OFFICERS NAMES

MILITARY MEANING	NAVAJO PRONUNCIATION	NAVAJO MEANING
Officers	A-la-jih-na-zini	Headmen
Major General	So-na-kih	Two stars
Brigadier General	So-a-la-ih	One star
Colonel	Atsah-besh-le-gai	Silver Eagle
Lt.Colonel	Che-chil-be-tah-besh-legai	Silver Oak Leaf
Major	Che-chil-be-tah-ola	Gold Oak Leaf
Captain	Besh-legai-na-kih	Two Silver Bars
1st Lieutenant	Besh-legai-a-lah-ih	One Silver Bar
2d Lieutenant	Ola-alah-ih-ni-ahi	One Gold Bar

AIRPLANE NAMES

MILITARY MEANING	NAVAJO PRONUNCIATION	NAVAJO MEANING
Airplanes	Wo-tah-de-ne-ih	Air Force
Dive Bomber	Gini	Chicken Hawk
Torpedo Plane	Taa-chizzie	Swallow
Observation Plane	Ne-as-jah	Owl
Fighter Plane	Da-he-tih-hi	Humming Bird
Bomber	Jay-sho	Buzzard
Patrol Plane	Ga-gih	Crow
Transport Plane	Atsah	Eagle

SHIPS NAMES

MILITARY MEANING	NAVAJO PRONUNCIATION	NAVAJO MEANING
Ships	Toh-dineh-ih	Sea Force
Battleship	Lo-tso	Whale
Aircraft Carrier	Tsidi-ney-ye-hi	Bird Carrier
Submarine	Besh-lo	Iron Fish

Footnote on Code Talkers

- The U.S. Army used Choctaw code talkers to relay communications on the battlefields in France in World War I.
- So effective were these code talkers that after the war ended, Germany sent people to the United States to learn the languages of the American tribes.
- In particular, Adolf Hitler pursued experts in American Indian dialects in preparation for conquering Europe.

A Modern Day Use of Cryptography

- Now let's look at a more modern example: banking.
- Every day, sensitive financial records are transmitted between banks and their customers. And whether you realize it or not, all of these records have to be stored at some point in a large database.
- Without cryptography, this would be a problem, a very big problem.
- If any of these records were stored or transmitted without encryption, it would be open season for hackers and your bank account would quickly dwindle down to $0. ***BUMMER!***

A Modern Day Use of Cryptography

- However, the banks know this and have gone through an extensive process to apply advanced encryption methods to keep your information out of the hands of hackers and food on your table.

What methods have you seen for encoding secret messages?

Some examples could be:

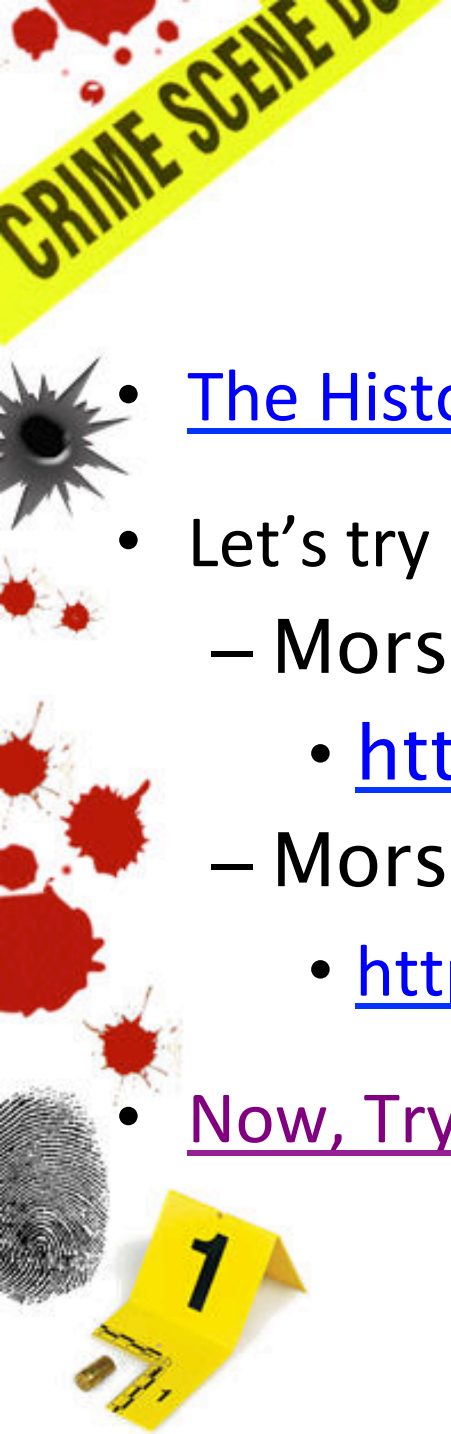
- Morse code
- Decoder rings
- Bar Codes
- Binary code

MORSE CODE

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

Morse Code

- The History of Morse Code
- Let's try it out….
  - Morse Code Practice:
    - http://bit.do/morse-code-practice
  - Morse Code Translator
    - http://bit.do/morse-code-translator
- Now, Try this video!



Let's Look at Another Type of Code

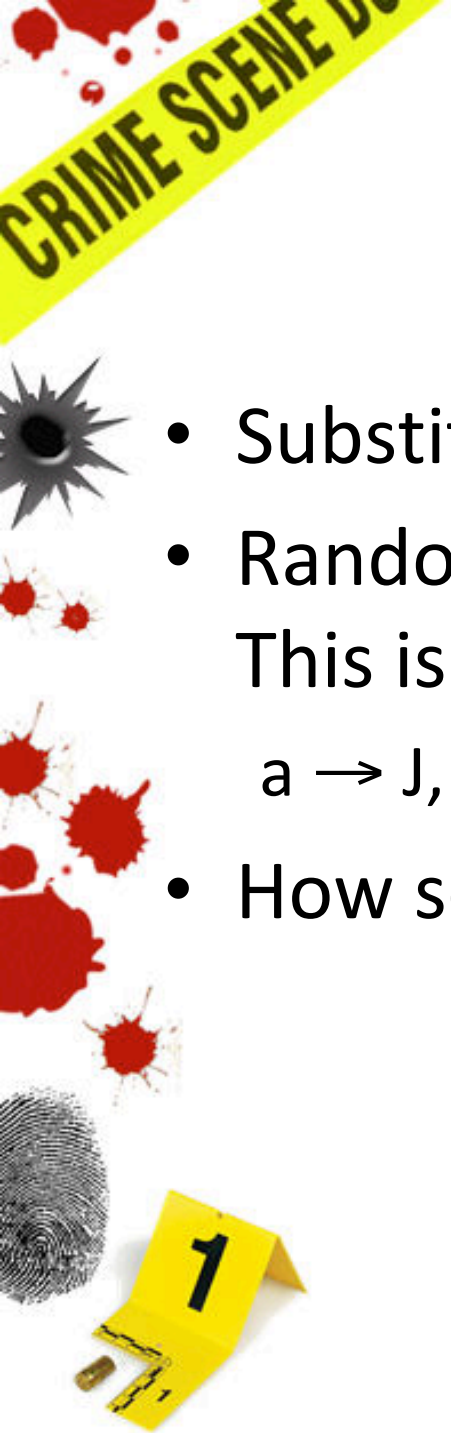
What do you think it says?

20-15-4-1-25 25-15-21 23-9-12-12

12-5-1-18-14 1-2-15-21-20 3-15-4-5-19

Hint

A = 1, B = 2, C = 3, ..., Z = 26

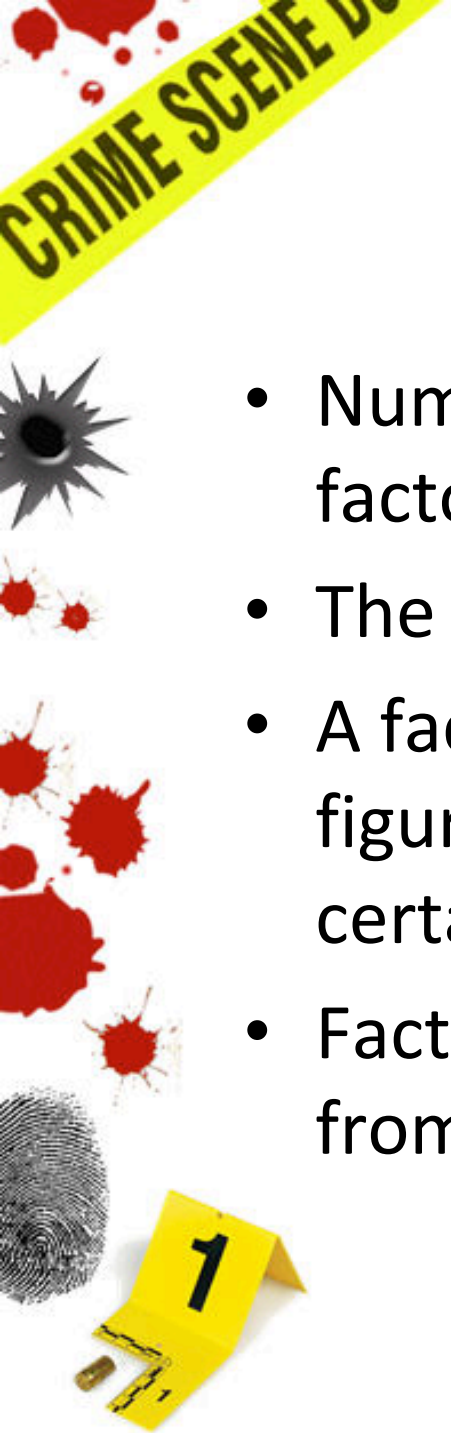


Substitution Cipher

- Substitute each letter based on mapping
- Randomly assign a letter to another letter. This is called your "***key***":

  a → J, b → L, c → B, d → R, ..., z → F

- How secure do you think this cipher is?



How Secure?

- Number of possible keys is 26! (called “26 factorial”)
- The explanation point is called a “factorial”
- A factorial is a math equation that is used to figure out how many ways you can arrange certain things in a specific sequence.
- Factorial says to multiply all whole numbers from our chosen number down to 1.

How Secure?

Examples:

- If I want to arrange 3 students in a certain way, I would use factorial to figure it out. Let's try it out!
- 3! = 3 x 2 x 1 = 6
  - There would be 6 ways to arrange them.

- Other Examples:
- What would 4! be?

  4! = 4 x 3 x 2 x 1 = 24
- How about 7!

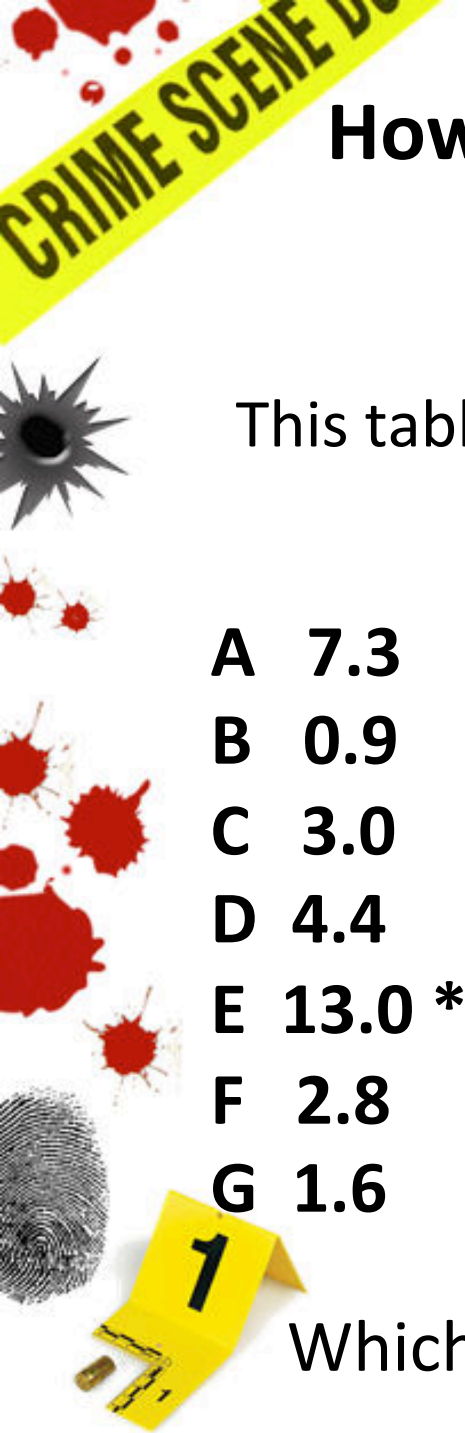
  7! = 7 × 6 × 5 × 4 × 3 × 2 × 1 = 5040

So, Really…. How Secure is the Substitution Cipher?

- Number of possible keys is 26!

26 (ways to choose what a maps to)
* 25 (b can map to anything else)
* 24 (c can map to anything else)
… * 1 (only one choice left for z)
= 26! = 403,291,461,126,605,635,584,000,000

This would mean that if **every** person on earth tried one per second, it would take 5 billion years to try them all.



How Can We Make it Easier to Decode?

Use Letter Frequency Analysis

This table shows the percent frequency of each letter in the English alphabet.

A 7.3	**H 3.5**	**O 7.4**	**V 1.3**
B 0.9	**I 7.4**	**P 2.7**	**W 1.6**
C 3.0	**J 0.2**	**Q 0.3**	**X 0.5**
D 4.4	**K 0.3**	**R 7.7**	**Y 1.9**
E 13.0 *	**L 3.5**	**S 6.3**	**Z 1.0**
F 2.8	**M 2.5**	**T 9.3**	
G 1.6	**N 7.8**	**U 2.7**	

Which letter statistically shows up the most often?

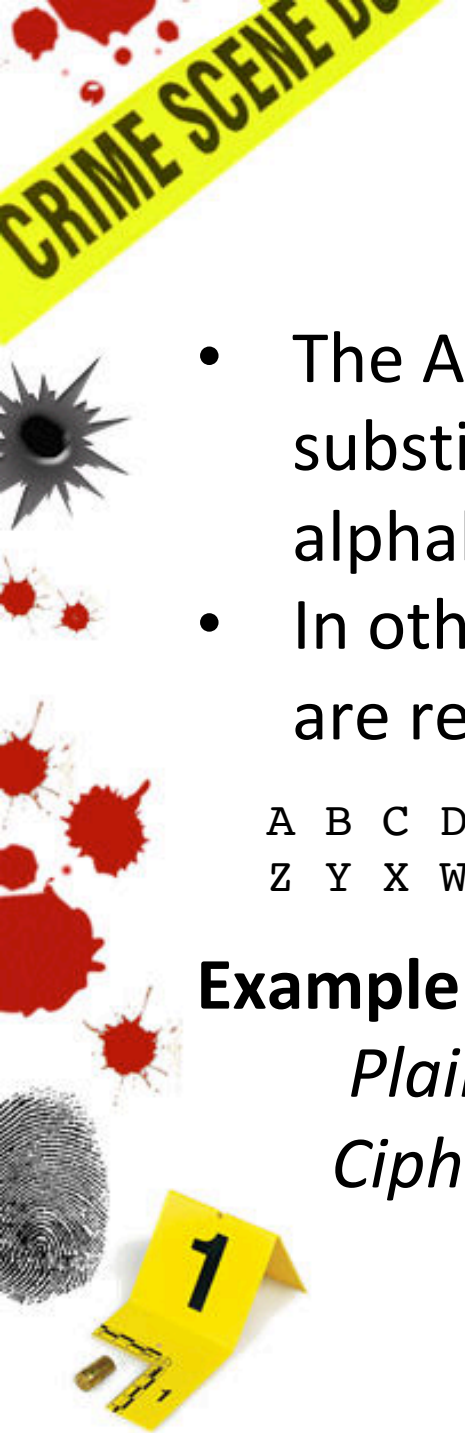
See if You Can Decipher This Using Letter Frequency!

R’UU WNENA CDAW CX CQN MJAT BRMN. HXD’EN OJRUNM, HXDA QRPQWNBB.

R JV J SNMR, URTN VH OJCQNA KNOXAN VN.

Solution

- I’ll never turn to the dark side. You’ve failed, your highness. I am a Jedi, like my father before me.



Atbash Cipher

- The Atbash cipher is a very specific case of a substitution cipher where the letters of the alphabet are reversed.
- In other words, all As are replaced with Zs, all Bs are replaced with Ys, and so on.

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

Example:

Plaintext: This is a secret message

Ciphertext: Gsrh rh z hvxivg nvhhztv

Polybius Square

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

- A Polybius Square is a table that allows someone to translate letters into numbers.
- In order to fit the 26 letters of the alphabet into the 25 spots created by the table, the letters i and j are usually combined.
- To encipher a message you replace each letter with the row and column in which it appears. *For example, D would be replaced with 14.*
- To decipher a message you find the letter that intersects the specified row and column.

Example:

Plaintext: This is a secret message

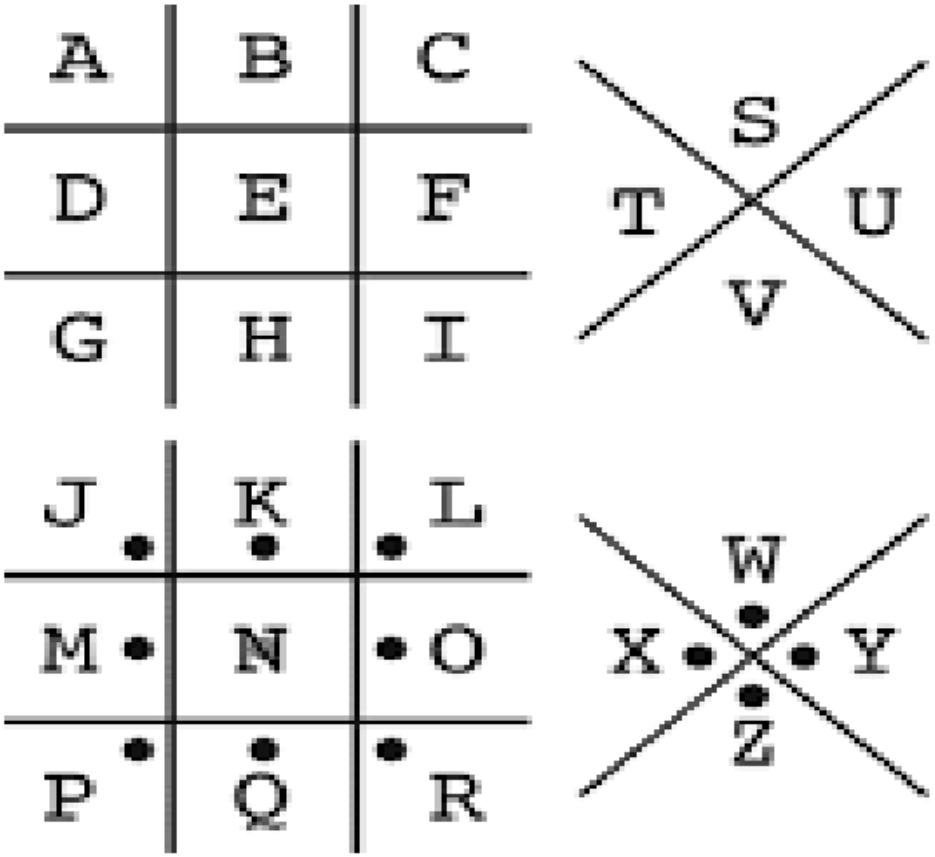
Ciphertext: 44232443 2443 11 431513421544 32154343112215

Pig Pen Cipher

- The Pig Pen Cipher has been around for a long time - over 800 years to be exact!
- It was originally used during the Crusades, but then it disappeared until the 1700's when the Freemasons picked it up.
- For this reason, the Pig Pen Cipher is also known as the Freemason Cipher.
- It also resurfaced during the Civil War, when a postal worker found the symbols on an envelope addressed to a suspected Confederate spy.

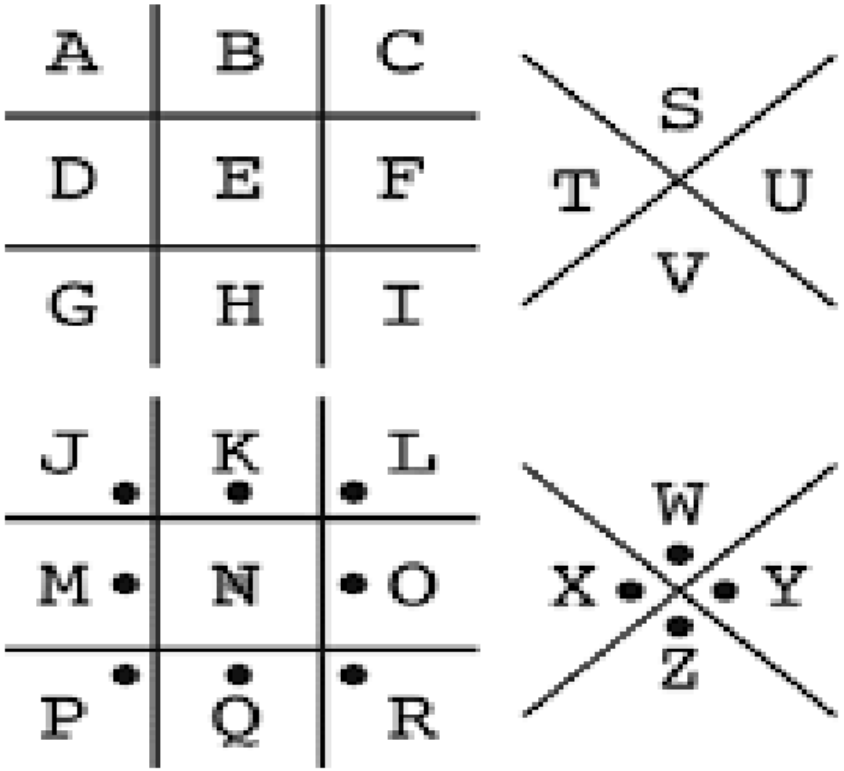
Pig Pen Cipher

- Here's what the Pig Pen Cipher looks like.



To encipher one of these messages, simply use the part of the drawing that corresponds to the letters that you want to encipher.

Pig Pen Cipher

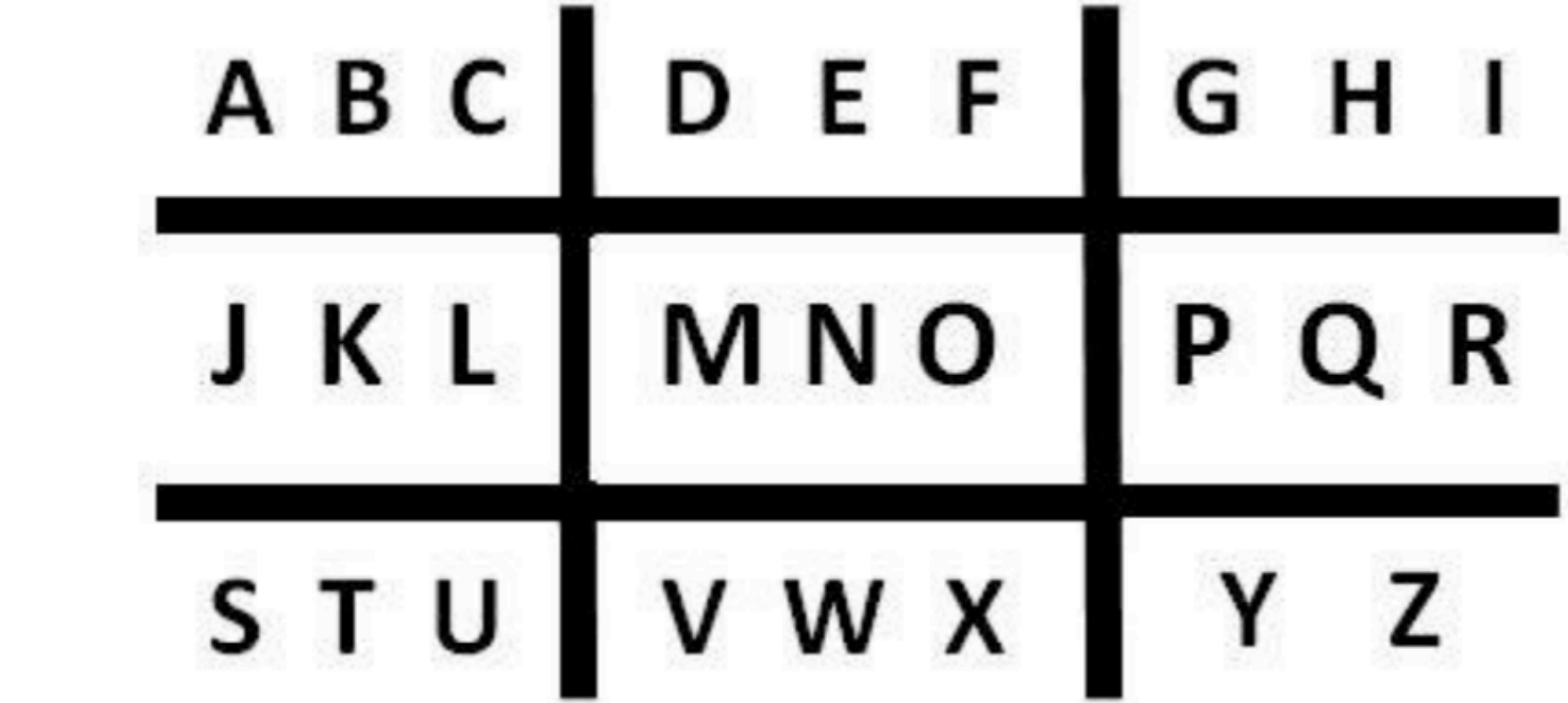


What do you think this says?

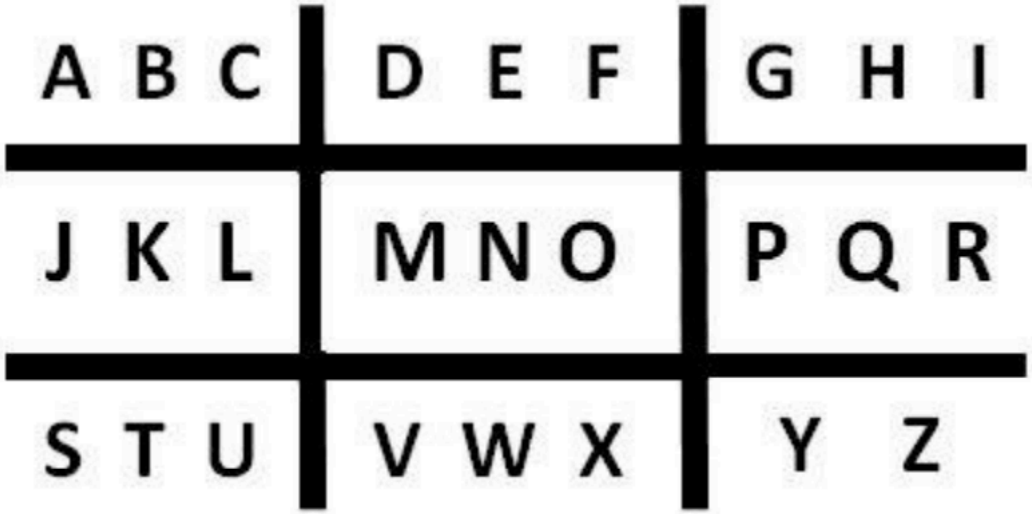
Rosicrucian Cipher

- While the Pig Pen is very useful and easy to remember, a similar, more compact cipher is available.
- This one is called the **Rosicrucian Cipher**. It uses the same concept as the pigpen cipher, except this one depends on the ***location*** of the dot in the code bracket.

Rosicrucian Cipher



Rosicrucian Cipher



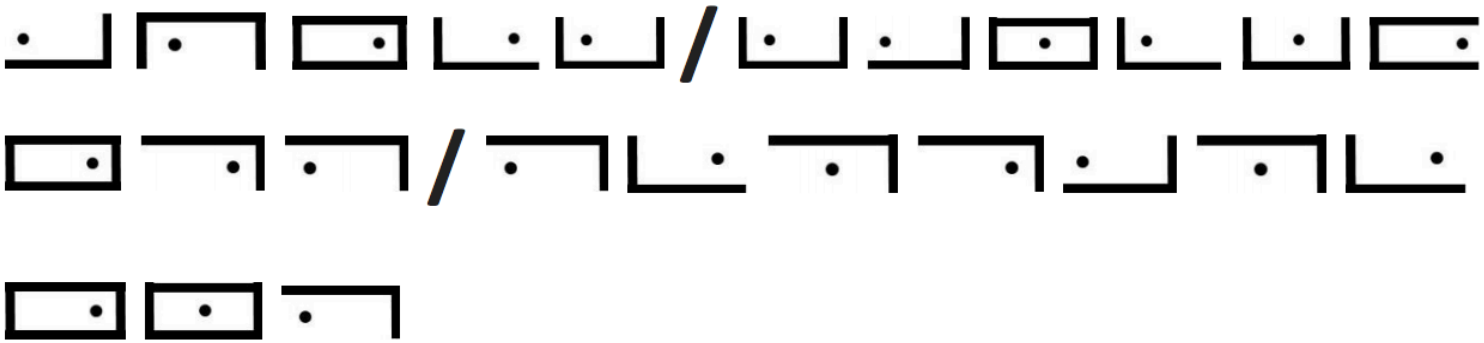
Here are some examples of letters:

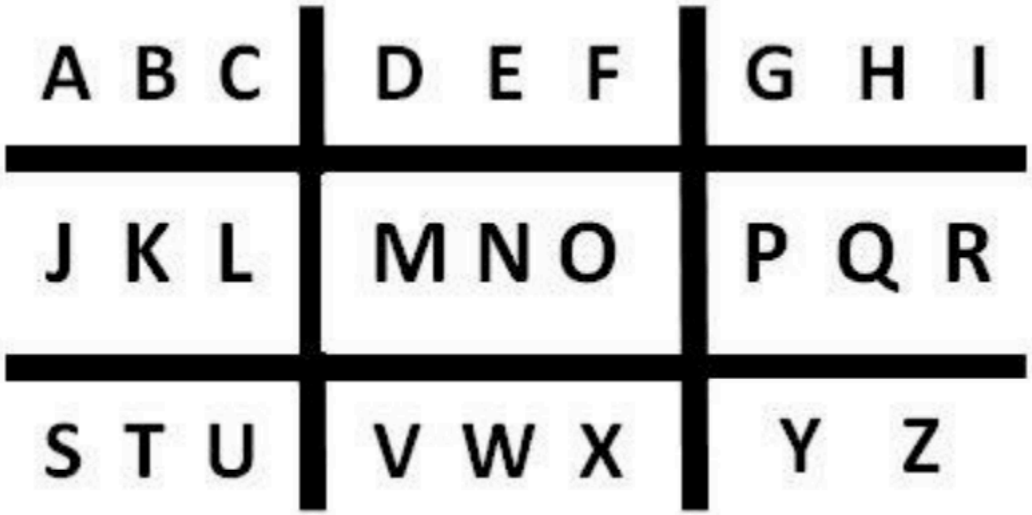
Z N G

Rosicrucian Cipher

Practice!

Here is a message to decode using the Rosicrucian cipher:





Rail Fence Cipher

- This cipher is a very simple transposition process based off of the design of the “split rail” fences that dotted the American countryside in the nineteenth century.
- This one splits the message up into two separate gibberish words that can be quickly unscrambled using a zigzagging line.

Rail Fence Cipher

- For example, you would write a message like:

DO NOT DELAY IN ESCAPING

- And then you would arrange the letters like this:

D N T E A I E C P N

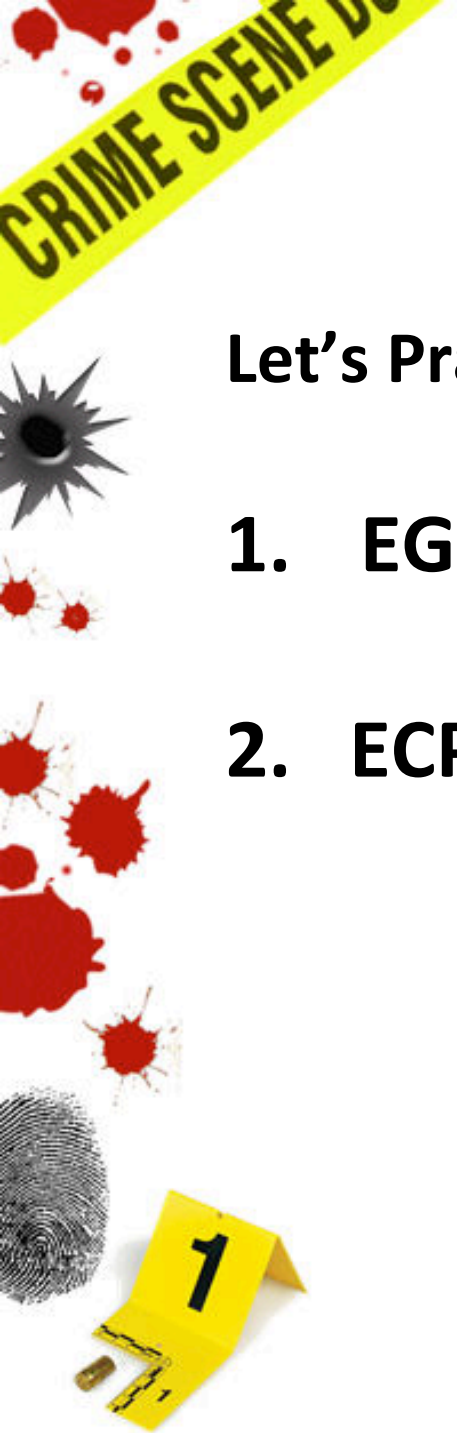
O O D L Y N S A I G

Rail Fence Cipher

Now, to send it as a ciphered message, write the top line, and then the bottom like this:

DNTEAIECPN OODLYNSAIG

Then, just reverse the process to decipher it!



Rail Fence Cipher

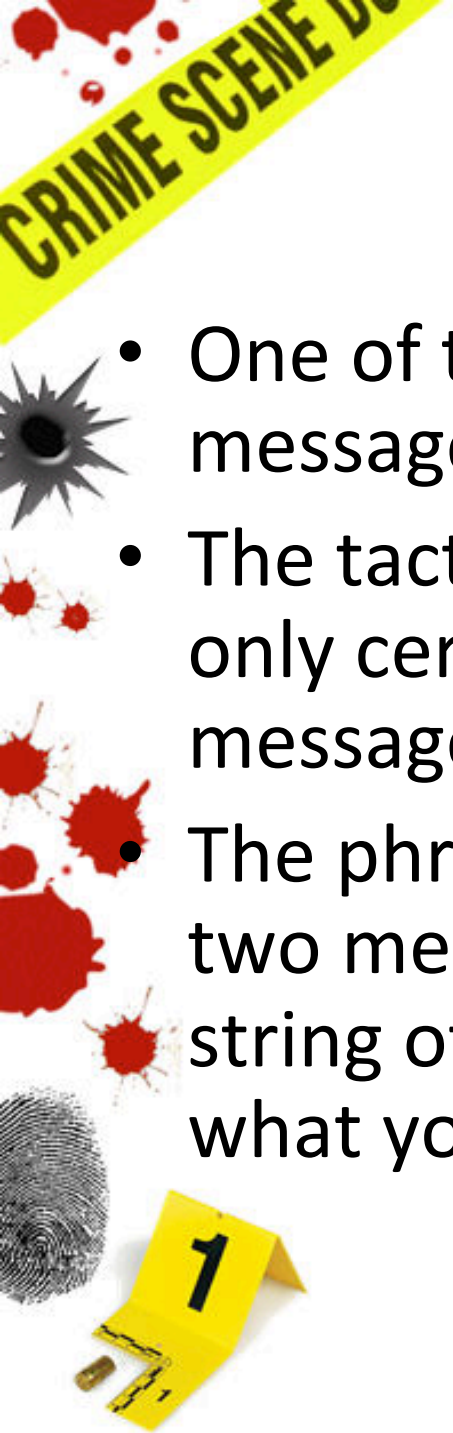
Let's Practice!

1. **EGRLAPESDIHR DAALNOUECPES**

2. **ECPNWEOELILS SAEOBFRALSOT**

Null Cipher

- One of the most basic ways of concealing a message is the null cipher.
- The tactic used here is making a phrase where only certain letters mean something in the message.
- The phrase could be a well-crafted letter with two meanings, or it could be a meaningless string of nonsense words. It all depends on what you plan on doing with the letter.



Null Cipher

Let's Practice:

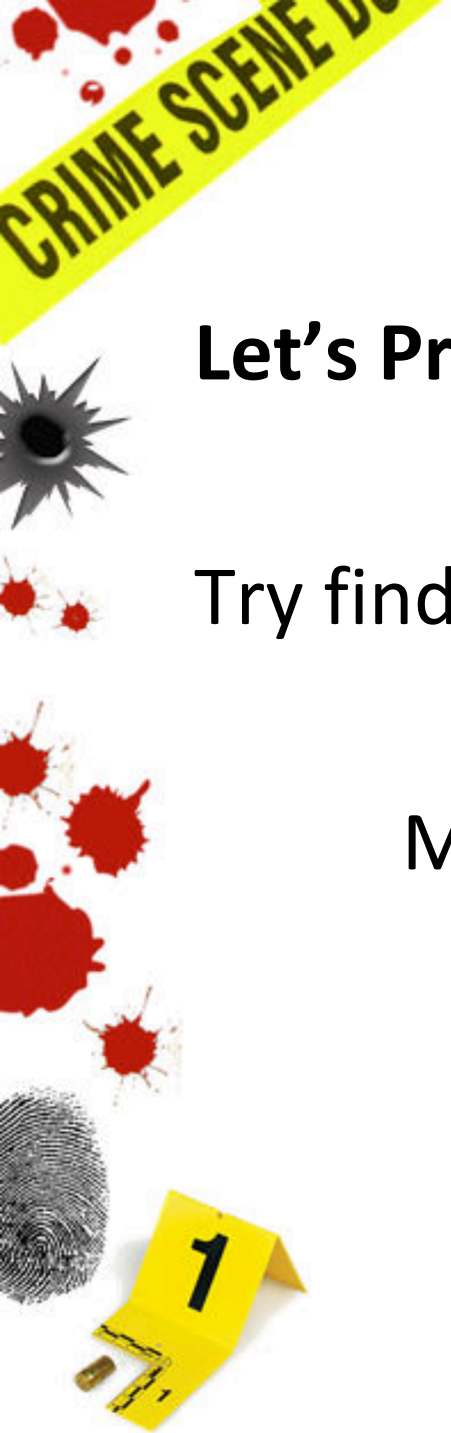
Try finding a meaning in this message:

SKUNK AVALANCHE VERTICAL EASY YESTERDAY OCTOBER USUALLY REMOVE SERIOUS EVERLASTING LAP FOREVER

Did you get it? Here's a hint: look at the *first* letter of each word in the phrase. It spells out

"s a v e y o u r s e l f"

To use this cipher, you can use any letter in the word, and you can be as creative as you want.

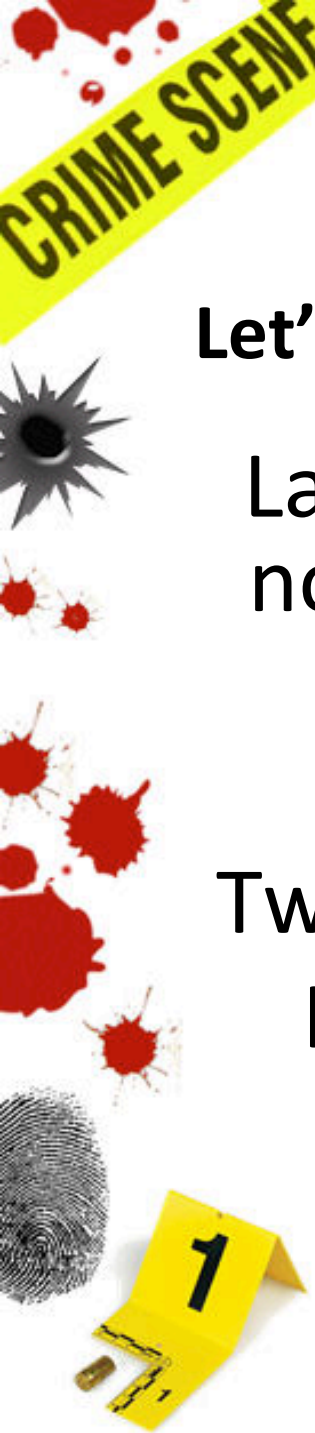


Null Cipher

Let's Practice once again:

Try finding a meaning in this message:

My antelope is not supposed to read enigmatic eulogies tonight.



Null Cipher

Let's Practice Again: (Try different techniques)

Large orange opals kill underappreciated noseless dragons. Eventually, Remus the hat eater returns umbrella guns.

Two rats stared achingly through boar fur.

Its afraid to arrive at the mental smile restaurant in Tinytown and

about sledding fast ace skates.

Spartan Cipher

Spies need to keep their messages secret. This activity demonstrates a simple low-tech way of encrypting data.

To build this at home, you'll need:

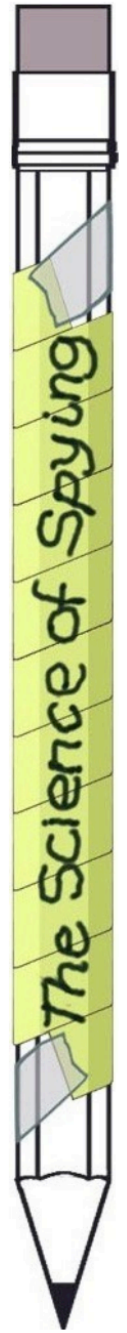
- pencils, copy paper, rulers
- tape and scissors for sharing
- some kind of rod (like a pencil).

1. This coding method may have been used by ancient Greeks in military campaigns. It is often called the 'Spartan cipher'.
2. To create a Spartan Cipher, you would cut a sheet of paper into a strip about a centimeter wide. It is important the paper strips are straight.

1. Attach a paper strip to the rod with a small piece of tape.

2. Wrap the paper strip tightly around rod making sure edges meet but don't overlap.

3. Fix the strip in place.



4. Write your message on the paper along the length of the rod.

Caesar Cipher

- Let’s build a Caesar Cipher!
- Please follow all directions exactly!