technocamps

UNDEB EWROPEAIDD
EUROPEAN UNION

Llywodraeth Cymru
Welsh Government

Cronfa Gymdeithasol Ewrop
European Social Fund

Prifysgol Abertawe
Swansea University

CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD

PRIFYSGOL BANGOR UNIVERSITY

Cardiff Metropolitan University
Prifysgol Metropolitan Caerdydd

i.t.wales

PRIFYSGOL ABERYSTWYTH UNIVERSITY

PRIFYSGOL glyndŵr Wrecsam
Wrexham glyndŵr UNIVERSITY

University of South Wales
Prifysgol De Cymru

technocamps

Cryptography

Activity: Spider Diagram

What is Steganography?

Steganography

Steganography is the practice of concealing messages or information within other non-secret messages or information. **Steganography** comes from the Greek **Steganos**, meaning concealed or covered, and **Graphein**, meaning writing.

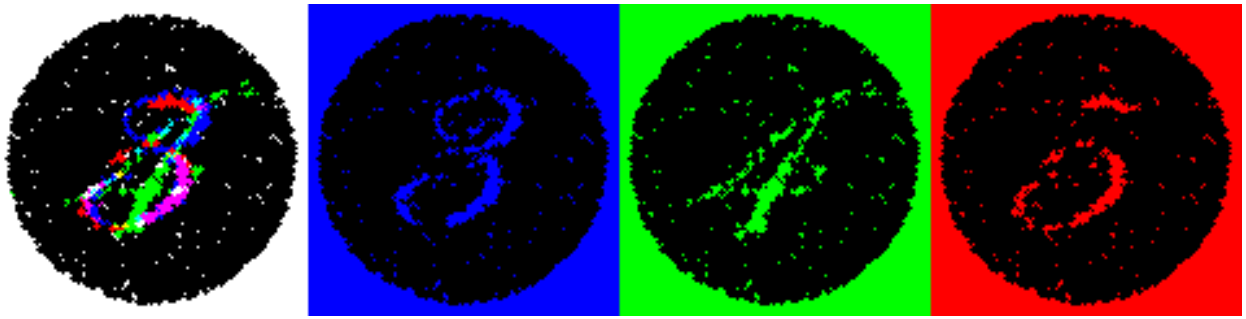
Steganography is used to digitally watermark videos and pictures and sometimes used to **send hidden messages**.

Here are some examples when **Steganography** is used:

T***hi***s is ***an*** e***xa***mple ***o***f h***o***w to ***hid***e a ***mes***s***ag***e ***wi***th***in a*** messag***e*** u***si***n***g*** th***e*** Ba***co***n c***o***de

Steganography

Steganography works because the eavesdropper does not know where the message is hidden and maybe does not know there is even a hidden message in the first place!



Activity: Define Steganography

Histiaeus's Servant

Back in ancient Greece, Histiaeus wanted to send a message to his friend.

But he was worried the message would be intercepted and read by his enemies.

If the message was written on a plain piece of paper, it would be quickly found and read if the messenger was captured and searched.

Histiaeus's Servant

So Histiaeus needed to hide the message.

He shaved the head of his most trusted servant and tattooed the message on the back of their head.

When the servant's hair had grown back, the message would be concealed.

If the messenger was captured and searched it wouldn't be found.

Activity: Histiaeus's Servant

Problems with the System?

Sir Francis Bacon

He came up the idea that knowledge should be based only on inductive reasoning and observations, also known as **the scientific method**.

He came up with a Steganographic method of hiding messages by using different fonts.

The Bacon Cipher

The **Bacon cipher** is a method of hiding a message inside another message by **changing fonts**.

1. Write out the message we want to hide.
2. Choose 2 different font types, A and B, such as **bold** and *italic* or **Comic Sans** and *Edwardian Script*.
3. Write out a boring message with at least 5 times as many letters in it as the hidden message.
4. Change the font of the boring message from style A to B for each of the corresponding letters in the hidden message.

Example

a: AAAAA	h: AABBB	o: ABBBA	v: BABAB
b: AAAAB	i: ABAAA	p: ABBBB	w: BABBA
c: AAABA	j: ABAAB	q: BAAAA	x: BABBB
d: AAABB	k: ABABA	r: BAAAB	y: BBAAA
e: AABAA	l: ABABB	s: BAABA	z: BBAAB
f: AABAB	m: ABBAA	t: BAABB	
g: AABBA	n: ABBAB	u: BABAA	

Bacon message: I WENt TO SCHOOL tODay, iT Was RaInING.
nO I dO NOt llKe it WHen iT RAIns

Example

a: AAAAA	h: AABBB	o: ABBBA	v: BABAB
b: AAAAB	i: ABAAA	p: ABBBB	w: BABBA
c: AAABA	j: ABAAB	q: BAAAA	x: BABBB
d: AAABB	k: ABABA	r: BAAAB	y: BBAAA
e: AABAA	l: ABABB	s: BAABA	z: BBAAB
f: AABAB	m: ABBAA	t: BAABB	
g: AABBA	n: ABBAB	u: BABAA	

Bacon message: I WENt TO SCHOOL tODay, iT Was RaInING. nO I dO NOt lIKe it WHen iT RAIns

Font type A: Uppercase

Font type B: lowercase

Example

a: AAAAA	h: AABBB	o: ABBBA	v: BABAB
b: AAAAB	i: ABAAA	p: ABBBB	w: BABBA
c: AAABA	j: ABAAB	q: BAAAA	x: BABBB
d: AAABB	k: ABABA	r: BAAAB	y: BBAAA
e: AABAA	l: ABABB	s: BAABA	z: BBAAB
f: AABAB	m: ABBAA	t: BAABB	
g: AABBA	n: ABBAB	u: BABAA	

Bacon message: I WENt TO SCHOOL tODay, iT Was RaInING. nO I dO NOt lIKe it WHen iT RAIns

Font type A: Uppercase

Font type B: lowercase

Translated: AAAAB

Hidden message: B

Example

a: AAAAA	h: AABBB	o: ABBBA	v: BABAB
b: AAAAB	i: ABAAA	p: ABBBB	w: BABBA
c: AAABA	j: ABAAB	q: BAAAA	x: BABBB
d: AAABB	k: ABABA	r: BAAAB	y: BBAAA
e: AABAA	l: ABABB	s: BAABA	z: BBAAB
f: AABAB	m: ABBAA	t: BAABB	
g: AABBA	n: ABBAB	u: BABAA	

Bacon message: I WENt TO SCHOOL tODay, iT Was RaInING. nO I dO NOt lIKe it WHen iT RAIns

Font type A: Uppercase

Font type B: lowercase

Translated: AAAAB AAAAA

Hidden message: Ba

Example

a: AAAAA	h: AABBB	o: ABBBA	v: BABAB
b: AAAAB	i: ABAAA	p: ABBBB	w: BABBA
c: AAABA	j: ABAAB	q: BAAAA	x: BABBB
d: AAABB	k: ABABA	r: BAAAB	y: BBAAA
e: AABAA	l: ABABB	s: BAABA	z: BBAAB
f: AABAB	m: ABBAA	t: BAABB	
g: AABBA	n: ABBAB	u: BABAA	

Bacon message: I WENt TO SCHOOL tODay, iT Was RaInING. nO I dO NOt lIKe it WHen iT RAIns

Font type A: Uppercase

Font type B: lowercase

Translated: AAAAB AAAAA AAABA

Hidden message: Bac

Example

a: AAAAA	h: AABBB	o: ABBBA	v: BABAB
b: AAAAB	i: ABAAA	p: ABBBB	w: BABBA
c: AAABA	j: ABAAB	q: BAAAA	x: BABBB
d: AAABB	k: ABABA	r: BAAAB	y: BBAAA
e: AABAA	l: ABABB	s: BAABA	z: BBAAB
f: AABAB	m: ABBAA	t: BAABB	
g: AABBA	n: ABBAB	u: BABAA	

Bacon message: I WENt TO SCHOOL tODay, iT Was RaInING. nO I dO NOt lIKe it WHen iT RAIns

Font type A: Uppercase

Font type B: lowercase

Translated: AAAAB AAAAA AAABA ABBBA

Hidden message: Baco

Example

a: AAAAA	h: AABBB	o: ABBBA	v: BABAB
b: AAAAB	i: ABAAA	p: ABBBB	w: BABBA
c: AAABA	j: ABAAB	q: BAAAA	x: BABBB
d: AAABB	k: ABABA	r: BAAAB	y: BBAAA
e: AABAA	l: ABABB	s: BAABA	z: BBAAB
f: AABAB	m: ABBAA	t: BAABB	
g: AABBA	n: ABBAB	u: BABAA	

Bacon message: I WENt TO SCHOOL tODay, iT Was RaInING.
nO I dO NOt lIKe it WHen iT RAIns

Font type A: Uppercase

Font type B: lowercase

Translated: AAAAB AAAAA AAABA ABBBA ABBAB

Hidden message: Bacon

Example

a: AAAAA	h: AABBB	o: ABBBA	v: BABAB
b: AAAAB	i: ABAAA	p: ABBBB	w: BABBA
c: AAABA	j: ABAAB	q: BAAAA	x: BABBB
d: AAABB	k: ABABA	r: BAAAB	y: BBAAA
e: AABAA	l: ABABB	s: BAABA	z: BBAAB
f: AABAB	m: ABBAA	t: BAABB	
g: AABBA	n: ABBAB	u: BABAA	

Bacon message: I WENt TO SCHOOL tODay, iT Was RaInING.
nO I dO NOt lIKe it WHen iT RAIns

Font type A: Uppercase

Font type B: lowercase

Translated: AAAAB AAAAA AAABA ABBBA ABBAB …

Hidden message: Bacon is good

Activity: Bacon Cipher Practice

a: AAAAA	h: AABBB	o: ABBBA	v: BABAB
b: AAAAB	i: ABAAA	p: ABBBB	w: BABBA
c: AAABA	j: ABAAB	q: BAAAA	x: BABBB
d: AAABB	k: ABABA	r: BAAAB	y: BBAAA
e: AABAA	l: ABABB	s: BAABA	z: BBAAB
f: AABAB	m: ABBAA	t: BAABB	
g: AABBA	n: ABBAB	u: BABAA	

1. ChoCOLAtE CaKEs ArE TaSTY WE ALSo lOVE plE

2. THe grAsS IS GREenEr WHERe yOu WAteR

3. ChEeSEY cHlps YUM

4. tHe qUICk brOWn FOX juMpS oVER tHE lAZy Dog aNd SO Did I. iT IS vERY fun

Problems with the Bacon Cipher?

Extension: Road Runner

Extension Activity: Make Your Own Invisible Ink

RECAP

Activity: What Is Cryptography?

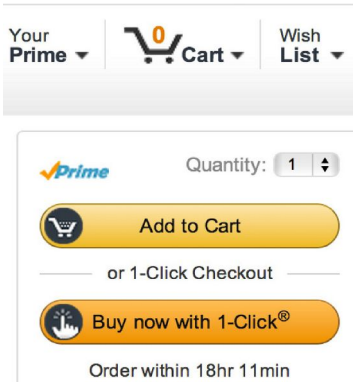
Cryptography

Cryptography is the practice and study of techniques for secure communication.

Cryptography comes from the Greek **Kryptos**, meaning secret or hidden, and **Graphein**, meaning writing.

Cryptographic techniques are used all the time in day to day life without you even noticing.

Here are some examples of when **Cryptography** is used:

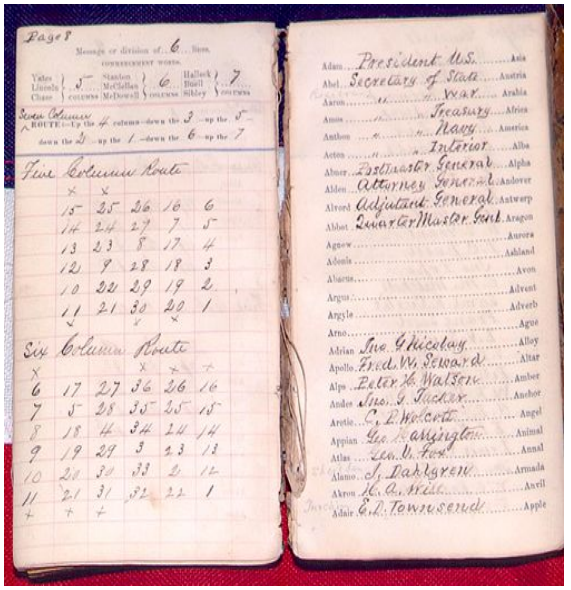


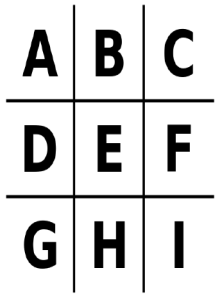
Cryptography

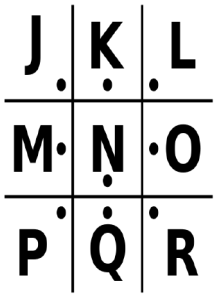
Cryptography is different from **Steganography**.

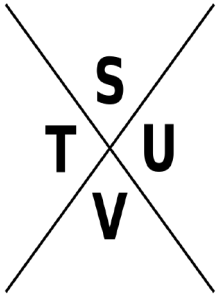
In Cryptography, everyone can tell that a secret message has been sent.

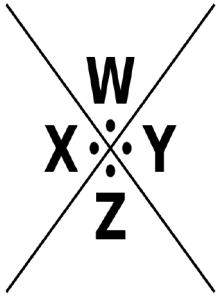
The security comes from the difficulty in **decrypting** the message without knowing the specific **key** that has been used.











Activity: Define Cryptography

Code Books

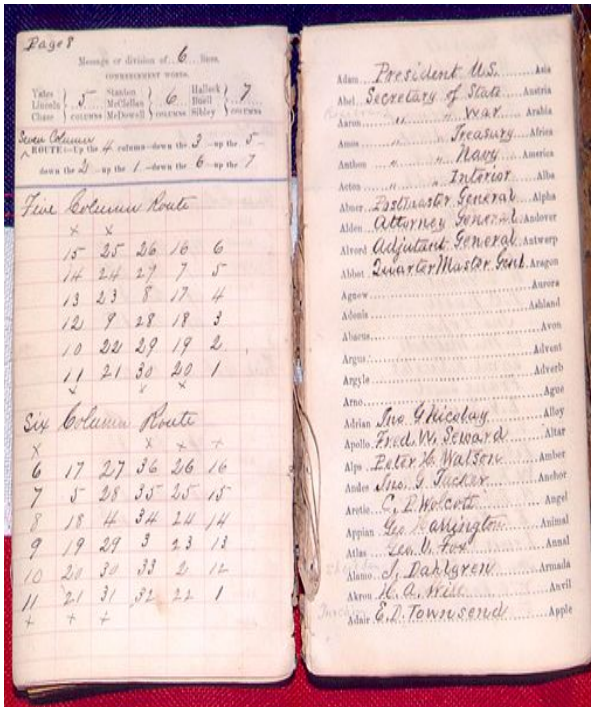
One **Cryptographic** method that is commonly used is based on **code books**.

We write an entire dictionary type book that changes the meaning of words or phrases.

We have a copy and the receiver has a copy.

We write out our message and **encrypt** each word or phrase in the message according to our **code book**.

Our receiver decrypts the message using an identical copy of the **code book**.



Activity: Make Your Own Code Book

Code Talkers

Code books are like translating to another language, assuming that someone who intercepts the message doesn't speak the **encrypted** language.

This idea has been used during both world wars as an encryption technique.

Amazingly, even Welsh has been used for these purposes as not many people outside of Wales can speak Welsh.

Navajo

The most prevalent use of translating to another language was with Navajo people.

In WWII, members of the Navajo population were put into different platoons to send **encrypted** messages by translating the English message to Navajo.

As very few people outside of the small Navajo community can speak Navajo, the Japanese found the **code** impossible to break.

NAVAJO CODES
NAME OF SHIPS

SHIPS	TOH-DINEH-IH	SEA FORCE
BATTLESHIP	LO-TSO	WHALE
AIRCRAFT	TSIDI-MOFFA-YE-HI	BIRD CARRIER
SUBMARINE	BESH-LO	IRON FISH
MINE SWEEPER	CHA	BEAVER
DESTROYER	CA-LO	SHARK
TRANSPORT	DINEH-NAY-YE-HI	MAN CARRIER
CRUISER	LO-TSO-YAZZIE	SMALL WHALE
MOSQUITO BOAT	TSE-E	MOSQUITO

NAVAJO CODES
NAME OF PLANES

PLANES	WO-TAH-DE-NE-IH	AIR FORCE
DIVE BOMBER	GINI	CHICKEN HAWK
TORPEDO PLANE	TAS-CHIZZIE	SWALLOW
OBS. PLAN	NE-AS-JAH	OWL
FIGHTER PLANE	DA-HE-TIH-HI	HUMMING BIRD
BOMBER PLANE	JAY-SHO	BUZZARD
PATROL PLANE	GA-GIH	CROW
TRANSPORT	ATSAH	EAGLE

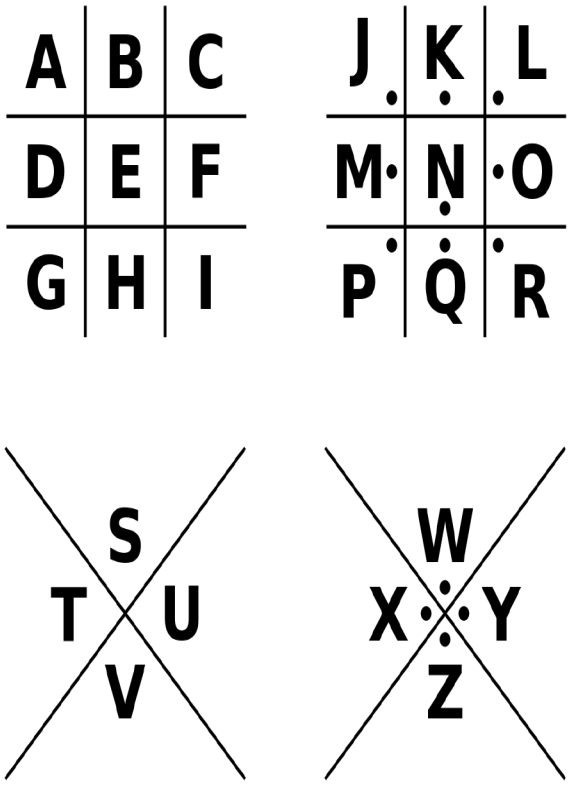
Pig Pen Cipher

The **Pig Pen cipher** has been used throughout history by a secret group called the Freemasons.

The Freemasons are kind of like a secret club. They have secret handshakes, codes and rituals that they aren't supposed to share with the outside world.

Each letter in your **plaintext** message is **encrypted** using the grid.

The weird symbols are sent as the message and the receiver **decrypts** them.



Activity: Pig Pen Practice

Codes vs. Ciphers

Codes vs. Ciphers

Codes encrypt entire words and/or phrases in the **plaintext** and **decrypt** entire words and/or phrases in the **ciphertext**.

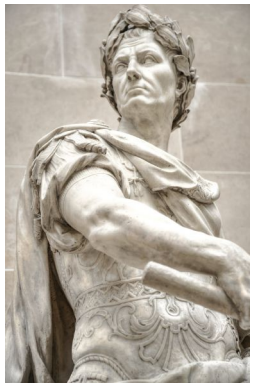
Ciphers encrypt individual letters in the **plaintext** and **decrypt** individual letters in the **ciphertext**.

Code:

Hello my name is Luke -> Shwmae Luke ydw i

Cipher:

Hello my name is Luke -> 



Julius Caesar

Gaius Julius Caesar:

- 100BC - 44 BC.
- A Roman politician, dictator, military general and historian.
- Led 2 expeditions to Britain in 55 BC and 54 BC.
- Elected to Consul, the highest rank in the Roman army, when he was 40 years old.
- In his 20s he was captured by pirates.
- Assassinated in the senate by republican senators.
- As a military general he devised a method of **encryption** which is called the **Caesar cipher**.

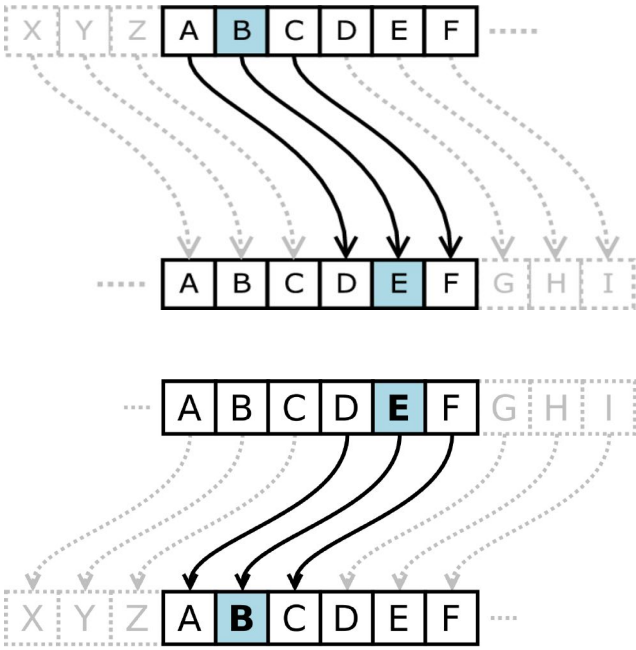
Activity: Julius Caesar Fact File

The Caesar Cipher

The **Caesar Cipher** is a **shift cipher** with **key 3**.

During encryption every letter in the **plaintext** message is shifted forward 3 letters in the alphabet. The letter "A" is **encrypted** as the letter "D".

During decryption, the receiver shifts each letter in **ciphertext** backward 3 letters. The letter "E" is **decrypted** to mean the letter "B".



For example:

Plaintext: Hello world

Ciphertext: Khoor zruog

Activity: Cipher Wheel Cut Out

Activity: Shift Cipher Practice

Caesar cipher, Key= 3:

- **Whfkqrfdpsv Iv ehwwhu wkdq vfkrro zrun**
- **Brx'uh jrqqd qhhg d eljjhu erdw**

Key = 9:

- **Cxcx r'en j onnurwp fn'an wxc rw tjwbjb jwhvxan**

Key = 21:

- **Yj jm yj ijo. Oczmz dn ij omt**

Extension: Key not given

- **Z druv r gifdzjv di wifuf. R gifdzjv. "Ufe'k pfl cvrmv yzd jrdnzjv xrdxvv" reu z ufe'k dvre kf**

How Hard is it to Break a Shift Cipher?

technocamps

Transposition Ciphers

All of the **cryptographic techniques** so far have involved replacing words or letters with other words or letters. These can be thought of as **substitution methods**.

What about if we instead jumbled up the order of the letters?

We would create a very hard anagram that needs to be broken, unless you knew how we jumbled them up.

These are know as **transposition ciphers**.

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

Scytale

Back in ancient Sparta, **transposition ciphers** were used to send messages using a wooden cylinder called a **Scytale**.

1. Two identical cylinders were created.

2. A long and narrow piece of material, normally leather, was wrapped around the **Scytale** and the message was written across it.

3. After the message had been written, the material was unwound and sent as one long list of letters.

4. The recipient wrapped the message around their identical **Scytale** and read the message.

Extension Activity: Scytale

Rail Fence Cipher

The **Rail Fence cipher** is another **transposition cipher**.

1. Write out the message in a zig zag like pattern on a certain number of "rails".
2. Read the message along the rails and send it to the receiver.
3. The receiver writes the message back out across the same number of rails and reads the message.

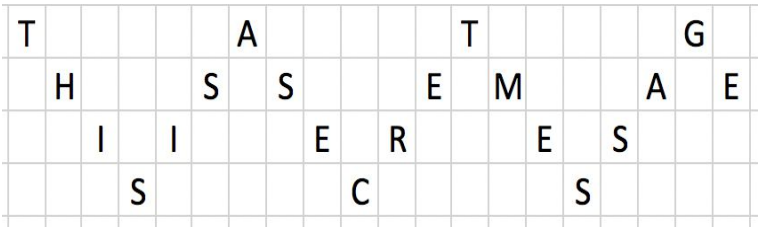
The number of rails acts as the **key** in this system.

For example:

Key = 4

Plaintext: this is a secret message

Ciphertext: tatghssemaeiieresscs



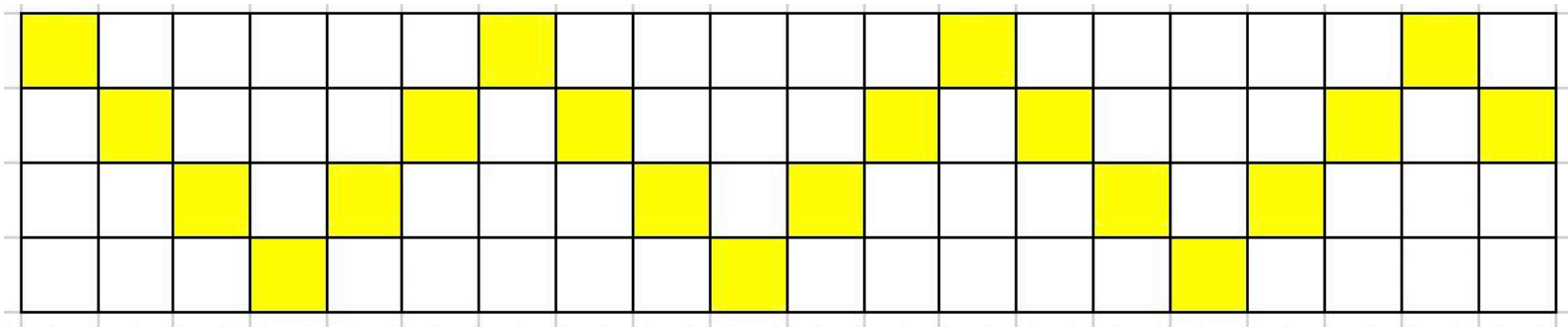
Rail Fence Cipher Example

Let's say the message we received was "TATGHSSEMAEIIERESSCS" and the key was four.

Rail Fence Cipher Example

Let's say the message we received was "TATGHSSEMAEIIERESSCS" and the key was four.

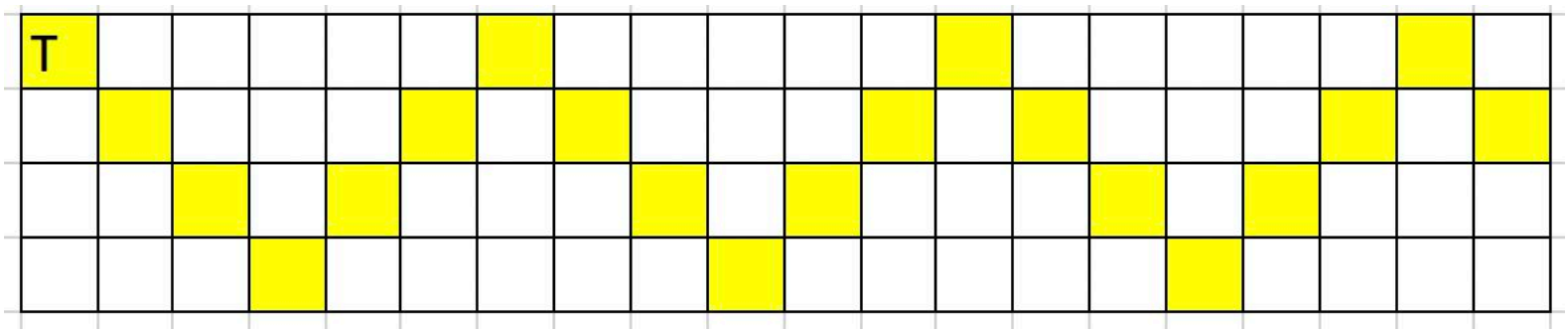
Draw a zig zag out along the 4 rails with as many boxes as letters in the message.



Rail Fence Cipher Example

We write out the message along four rails in the correct boxes given to us by a zig zag pattern.

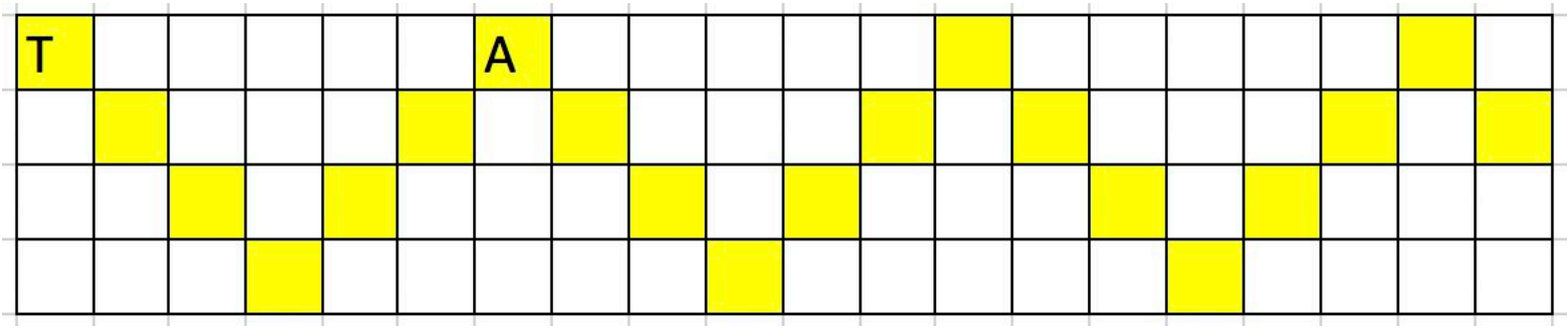
Message: “TATGHSSEMAEIIERESSCS”



Rail Fence Cipher Example

We write out the message along four rails in the correct boxes given to us by a zig zag pattern.

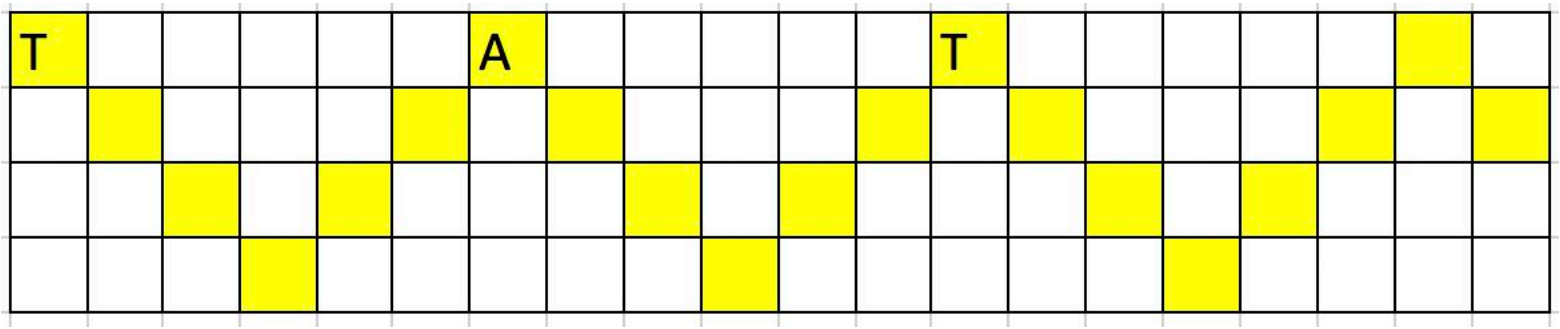
Message: "TATGHSSEMAEIIERESSCS"



Rail Fence Cipher Example

We write out the message along four rails in the correct boxes given to us by a zig zag pattern.

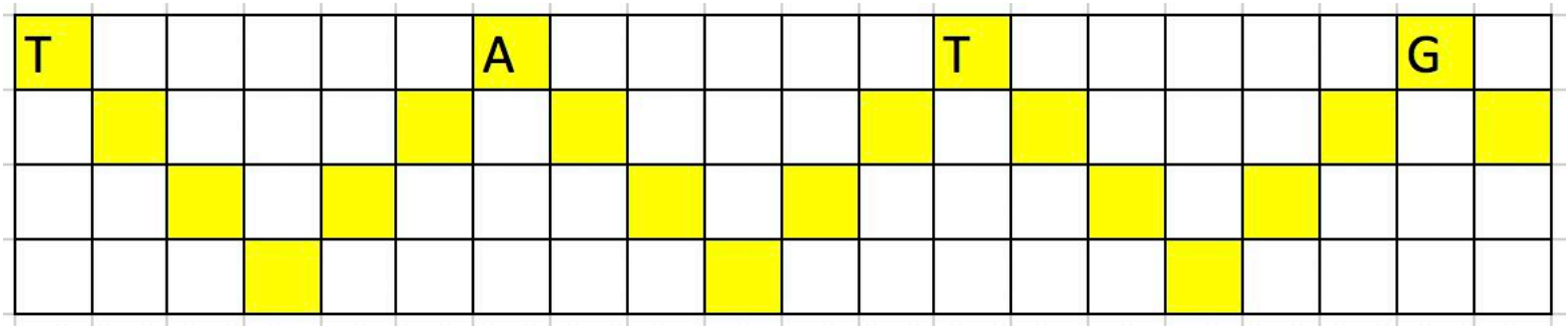
Message: "TATGHSSEMAEIIERESSCS"



Rail Fence Cipher Example

We write out the message along four rails in the correct boxes given to us by a zig zag pattern.

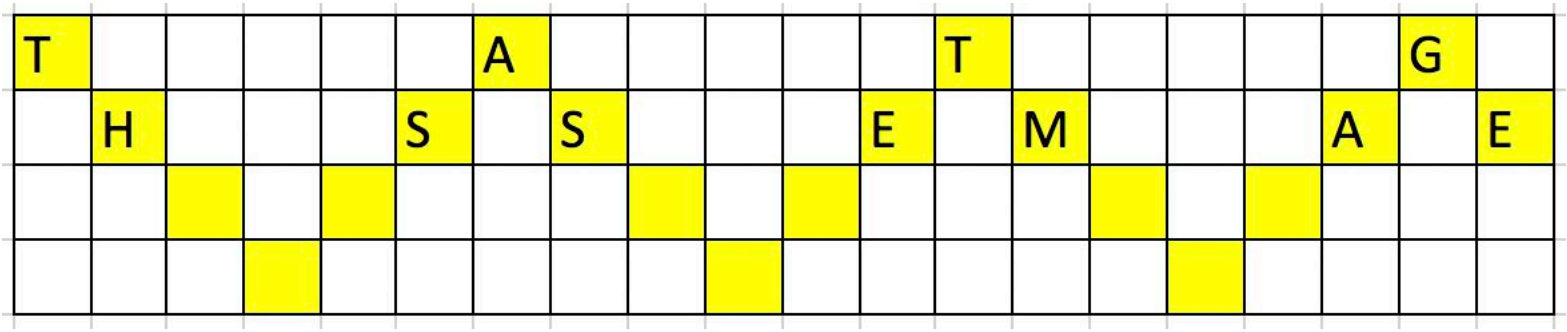
Message: "TATGHSSEMAEIIERESSCS"



Rail Fence Cipher Example

We write out the message along four rails in the correct boxes given to us by a zig zag pattern.

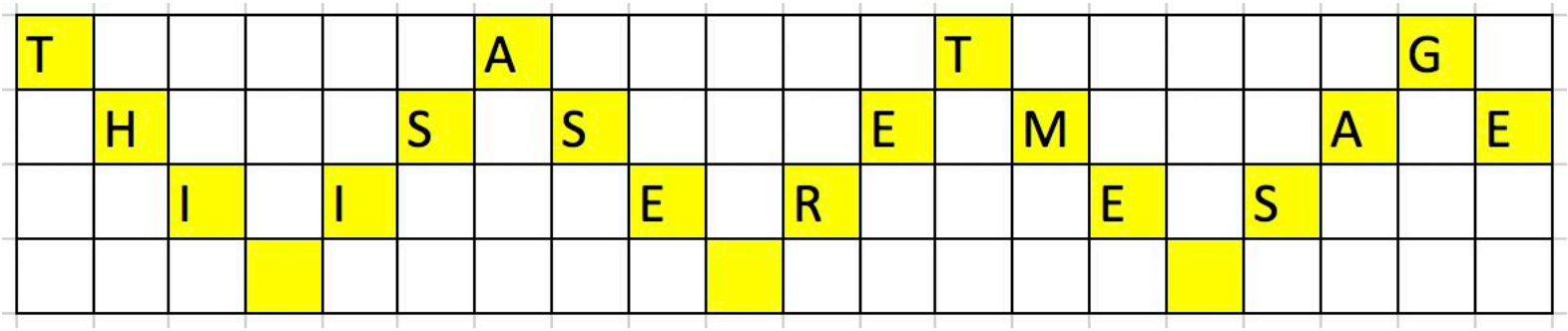
Message: "TATGHSSEMAEIIERESSCS"



Rail Fence Cipher Example

We write out the message along four rails in the correct boxes given to us by a zig zag pattern.

Message: "TATGHSSEMAEIIERESSCS"



Rail Fence Cipher Example

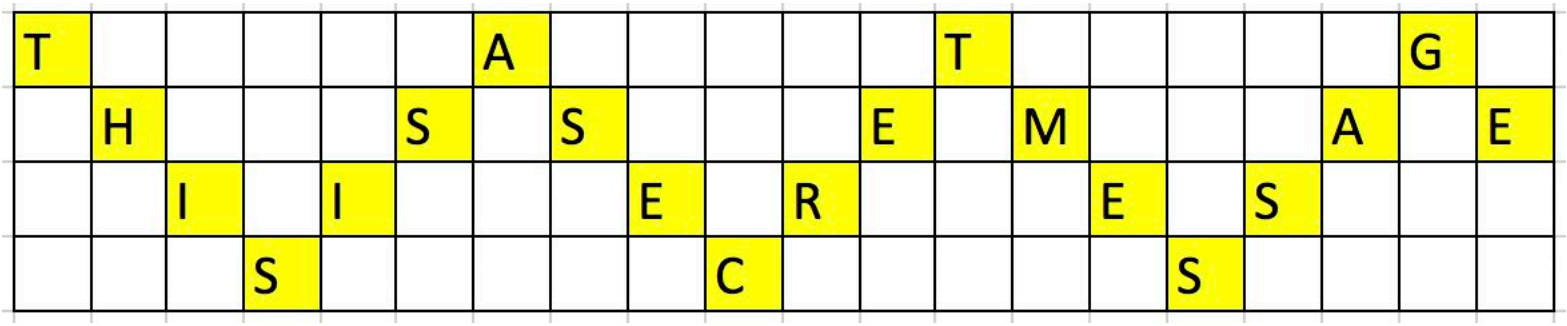
We write out the message along four rails in the correct boxes given to us by a zig zag pattern.

Message: "TATGHSSEMAEIIERESSCS"

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

Rail Fence Cipher Example

The decrypted message is then read along the zig zag and we get "This is a secret message"



Activity: Rail Fence Cipher Practice

Decrypt These Messages

Key = 4:

- **Tytiwghmsecanlanraseratiayaytcpms**
- **Tnddoiinbniftaeonyy**

Key = 2:

- **Loamiteatinwoktemhcpano**
- **Myhodeebiyufvuatedsvrenoraor**

Key = 3:

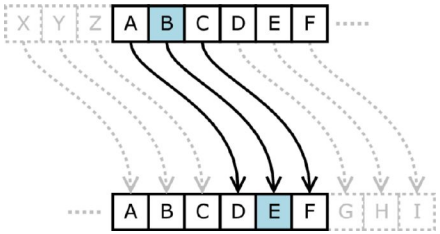
- **Wittuvaoeeldnwntsriewntlvloaoviti**
- **Jksmutepwmigsein**

Extension: Key not given

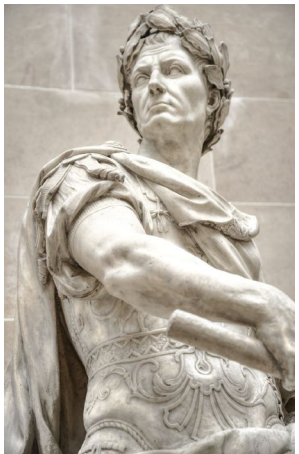
- **Mdsriolosknegttreeodafo**

RECAP

Steganography is hiding messages inside other messages. Examples include: Invisible ink, Histiaeus's servant and the Bacon cipher.

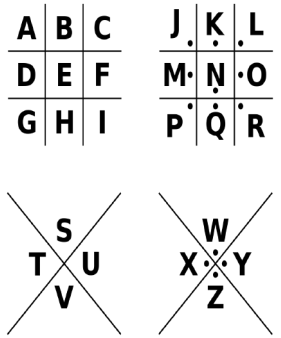


Cryptography is sending messages securely. Split into two main groups: Substitution and Transposition.



Examples of Substitution methods include: Caesar cipher, Pig-pen cipher and Code books.

Examples of transposition methods include: Rail-fence cipher and Scytale.



Activity: Escape the Box