*Transposition Ciphers - **ANSWERS***

Caesar Shift Cipher

Assignment 1

CONTINUE TO ENCIPHER THIS MESSAGE YOU NEED TO REPLACE
FRQWLQXH WR HQFLSKHU *WKLV PHVVDJH BRX QHHG WR UHSODFH*

EACH LETTER USING THE CIPHER GRID
HDF*K OHWWHU XVLQJ WKH FLSKHU JULG*

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
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

Using the same grid decipher the following – remember to decipher from the lower grid to the upper.

Assignment 2

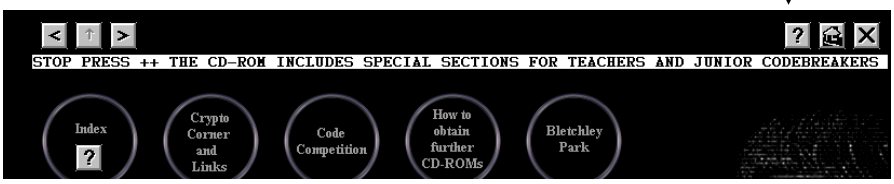
JHQLXV LV RQH SHU FHQW LQVSLUDWLRQ DQG QLQHWB QLQH SHU FHQW SHUVSLUDWLRQ TXRWH IURP WKRPDV HGLVRQ

'Genius is one per cent inspiration and ninety nine per cent perspiration' quote from Thomas Edison

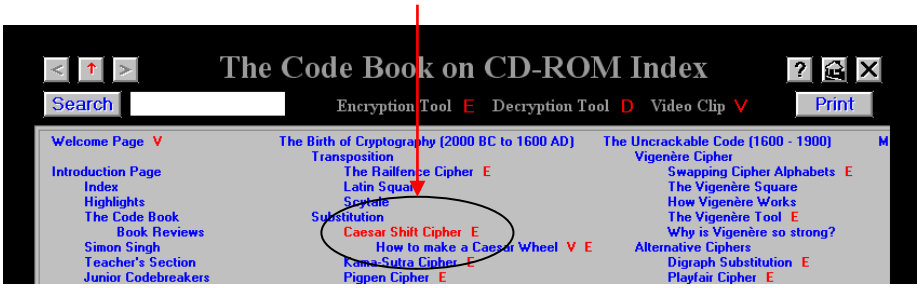
Shift Cipher

Similar to the example above, can you crack the cipher? How much does it shift?

To find the Caesar Shift on the computer click on the question mark on the homepage



Then select Caesar Shift - Copy the text into the right hand side box and decipher – Try different shift values until the message makes sense.



Assignment 3

RCTQCA KIMAIZ AMVB BPM NQZAB SVWEV MVKQXPMZML UMAAIOMA NWZ UQTQBIZG XCZXWAMA PM LQL QB QV I AGABMUIBQK EIG JG APQNBQVO BPM ITXPIJMB NWZEIZL BPZMM XTIKMA BPQA XZWDML ZMTIBQDMTG MIAG BW LMKQXPMZ ZMXTIKQVO MIKP TMBBMZ EQBP WVM BPZMM XTIKMA JIKSEIZLA LQNNMZMVB KIMAIZ APQNBA KQXPMZA MFQAB JG UWDQVO I LQNNMZMVB VCUJMZ WN XTIKMA QN GWCZ MVMUG QVBMZKMXBML GWCZ UMAAIOM QB EIA VWB BWW LQNNQKCTB NWZ BPMU BW LMKQXPMZ

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
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*

Julius Caesar sent the first known enciphered messages, for military purposes. He did it in a systematic way by shifting the alphabet forward three places, this proved relatively easy to decipher, replacing each letter with one three places backwards. Different Caesar shifts ciphers exist by moving a different number of places; if your enemy intercepted your message it was not too difficult for them to decipher. Shift 8

Assignment 4

Encipher the following using a 6 shift

HE WHO MAKES NO MISTAKE NEVER LEARNS ANYTHING. ENGLISH PROVERB

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
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*

NK CNU SGQKY TU SOYZGQK TKBKX RKGXTY GTEZNOTM KTMROYN VXUBKXH

Shift Cipher

Decipher the following, notice that there are no spaces shown between the words, which makes it harder. What techniques can you use to decipher? Do you know what is the most commonly used letter in the English Language?

Assignment 5

PDANASWOWJKHZIWJSEPDWXAWNZ
SDKOWEZEPEOFQOPWOEBAWNAZ
PSKKSHOWJZWDAJBKQNHWNGOWJZWSNAJ
DWRAWHHXQEHPPDAENJAOPOEJIUXAWNZ
XUAZSWNZHAWN

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
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

There was an old man with a beard,
Who said, 'It is just as I feared! -
Two Owls and a Hen, four Larks and a Wren,
Have all built their nests in my beard!'
By Edward Lear shift -4

Substitution Ciphers

Keyword Cipher

Decipher the following using the cipher grid below. The cipher has a key word **SPY** notice how the rest of the alphabet is coded.

Assignment 6

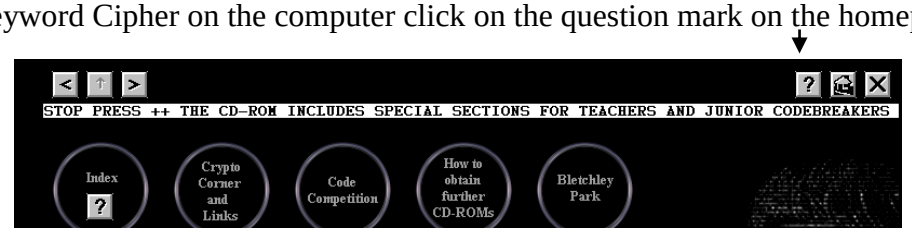
DFUB JB PTR LKB CFOJ QMLR LK VEFYE RL QRSKA SKA F VFII JLUB REB BSORE NTLRB COLJ SOYEFJBABQ

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

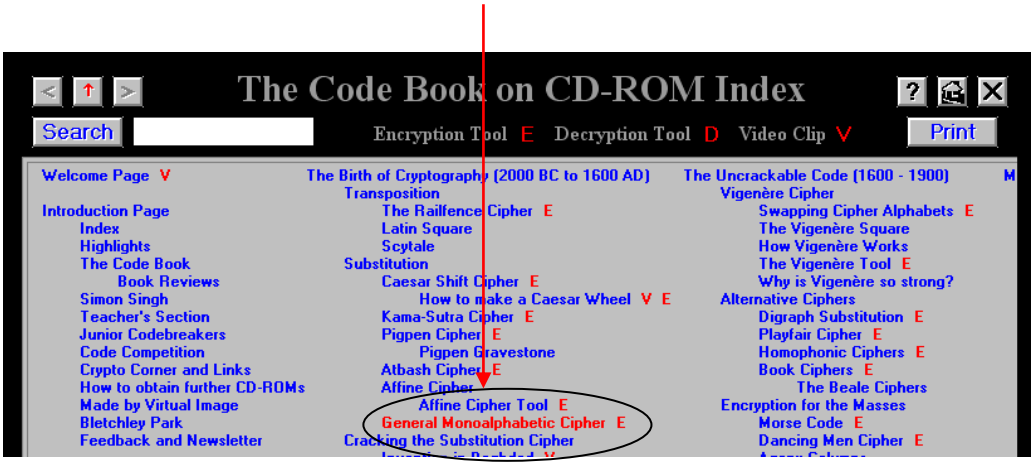
'Give me but one firm spot on which to stand and I will move the earth' quote from Archimedes

The following message for deciphering uses the keyword **AGENT** – can you crack the cipher.

To find the Keyword Cipher on the computer click on the question mark on the homepage



Then select General Cipher and clear the clear the Cipher already present and enter the alphabet beginning with the letters **AGENT**. Copy the text into the right hand side box and decipher



Assignment 7

RMKT KTRRACTR AQT ITOS RTEQTS LMS GTEAURT SDTY AQT WQFSSTL FL EMNT GUS GTEAURT SDTY AQT DFNNTL SDFR FR ILMWL AR RSTCALMCQAODY FLVFRFGJT FLI ALN RDQFLIFLC KTRRACTR SM SDT RFZT MB A KFEQMNMS AQT WTJJ ILMWL KTSDMNR MB RSTCALMCQAODY MLT MB SDT KMRS ULURUAJ KTSDMNR URTN GY SDT CQTTIR WAR SM RDAVT SDT DTAN MB SDT KTRRTLCTQ SASSMM SDT KTRRACT ML DFR REAJO ALN SDTL NTROASED DFK MLET SDT DAFQ DAN CQMWL TVTL FB SDT TLTKY NFREMVTQTN ALN RTAQEDTN DFK LM KTRRACT WMUJN GT BMULN DMWTVTQ SDFR WAR EJTAQJY FL A OTQFMN MB DFRSMQY SDAS SMJTQASTN A JAEI MB UQCTLEY

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

Some messages are kept secret not because they are written in code, but because they are hidden, this is known as steganography. Invisible ink and shrinking messages to the size of a microdot are well known methods of steganography. One of the most unusual methods, used by the Greeks, was to

shave the head of the messenger, tattoo the message on his scalp and then despatch him once the hair had grown. Even if the enemy discovered and searched him no message would be found; however this was clearly in a period of history that tolerated a lack of urgency! Keyword: agent

FREQUENCY ANALYSIS

Cryptanalysis

Many codes are cracked using **Frequency Analysis** because certain letters are used more often than others. In English E then T are the two most frequently used letters; here is a grid with the relative frequencies of each letter i.e. the percentage of occurrences of each letter in English

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
8	2	3	4	13	2	2	6	7	0	1	4	2	7	8	2	0	6	6	9	3	1	2	0	2	0

The Babington Plot

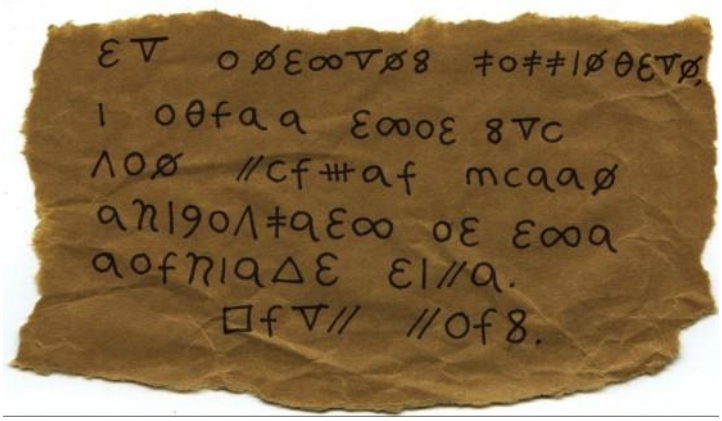
In the Sixteenth Century, there was an attempt to overthrow Elizabeth, Queen of England. Elizabeth had kept Mary, Queen of Scots, prisoner for many years. Some English Catholics were unhappy that England was led by a Protestant monarch and plotted to assassinate Elizabeth and rescue Mary, a Catholic, and have her instated as Queen of England. Babington led the plotters; they used both steganography and a substitution code. Unknown to the plotters the carrier of the message (who was unable to read the code) was a double agent and gave copies of the code to Elizabeth's minister Walsingham, who used frequency analysis on the symbols to crack the code.

Assignment 8

The Babington Plot

The following note has been coded using the cipher actually used by Mary Queen of Scots.

Can you crack it?



Carry out an analysis of the frequency of each character
De-code the message

Frequency table

Symbol	Tally	Frequency
/		
Δ		
Ø		
O		
8		
C		
≠		
∞		
θ		
∇		
f		
//		
m		
9		
q		
η		
Ɛ		
□		
⫴		
∧		
	Total	81

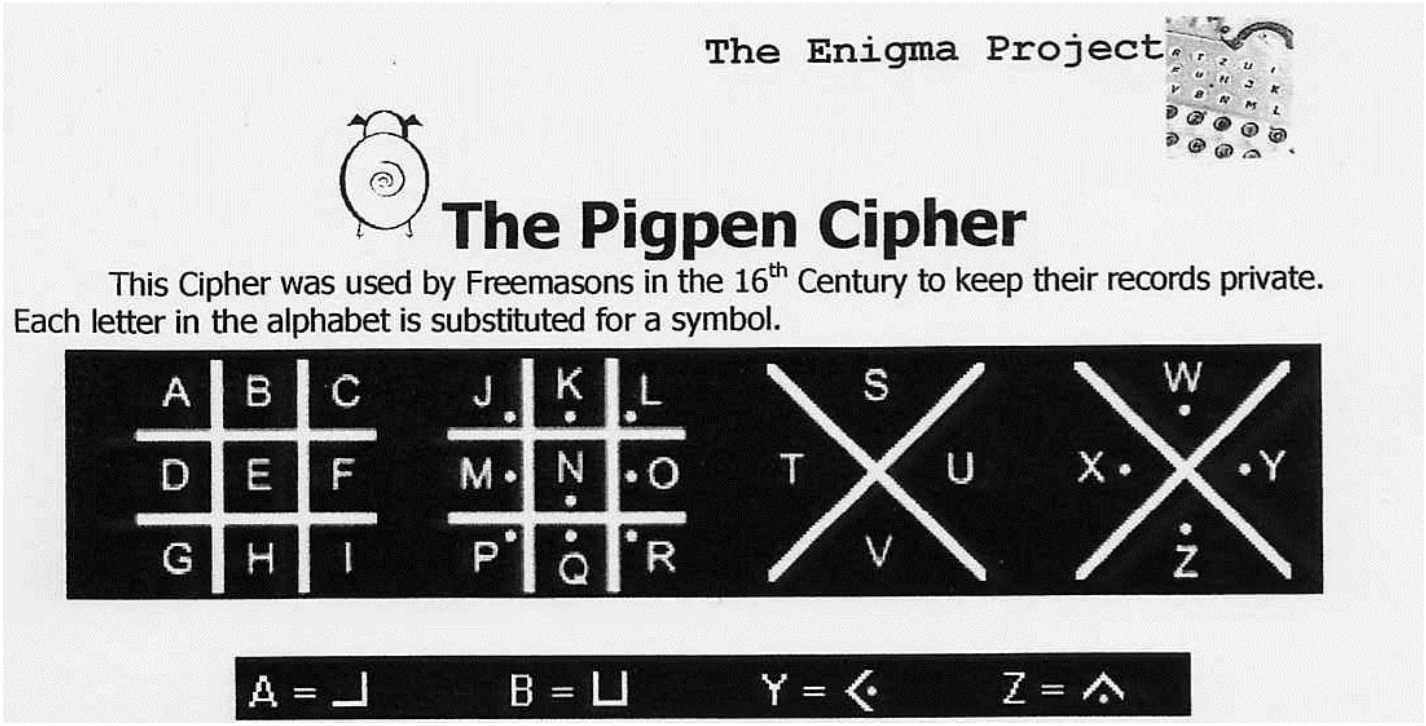
Frequency table - answers

Symbol	Tally	Frequency
/		5
Δ		1
Ø		6
O		9
8		3
C		3
≠		4
∞		4
θ		2
∇		5
f		6
//		4
m		1
9		1
q		11
η		2
ε		10
□		1
⫲		1
∧		2
	Total	81

The text says

To Anthony Babington, I agree that you can murder Queen Elizabeth at the earliest time. From Mary.

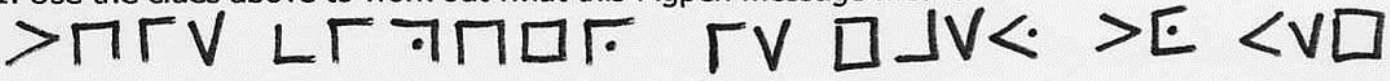
Pig-Pen Code



Pig-pen code was developed in the Eighteenth Century and was used by the Freemasons; it had limited use since it was so awkward. Later in the Eighteenth Century the admiralty in Whitehall, London, needed to send messages quickly and efficiently to the Navy based in Portsmouth. The usual method had been to send a horse and rider, which were prone to kidnapping and took a lot of valuable time. A system of visual telegraphs, using semaphore, was set up relaying messages via thirteen strategically placed stations. One of which has recently been renovated near Guildford, in Effingham. When sensitive information was relayed it could be transmitted in code in case an enemy was watching.

Assignment 9

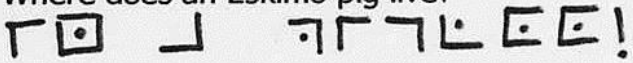
1. Use the clues above to work out what this Pigpen message means.



2. Write your own name in Pigpen, and then the name of the person sitting next to you.

3. Decipher the punch lines to these Pigpen jokes, and you'll squeal with laughter!

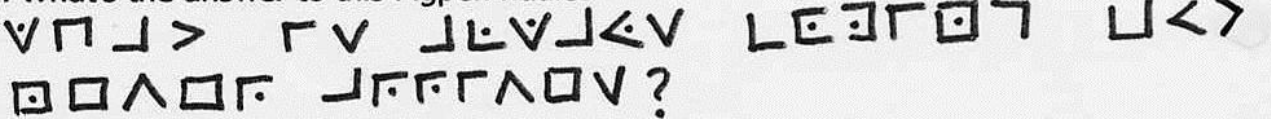
Where does an Eskimo pig live?



What did the alien say to the gardener?

What tools do you need in a Maths class?

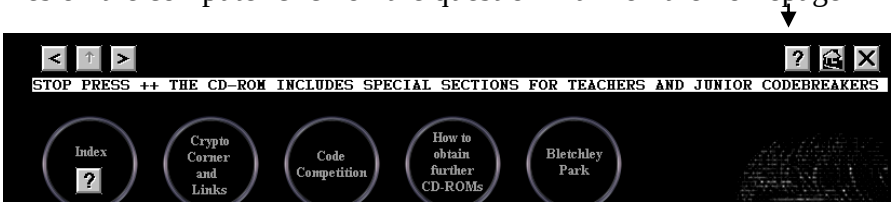
4. What's the answer to this Pigpen riddle?



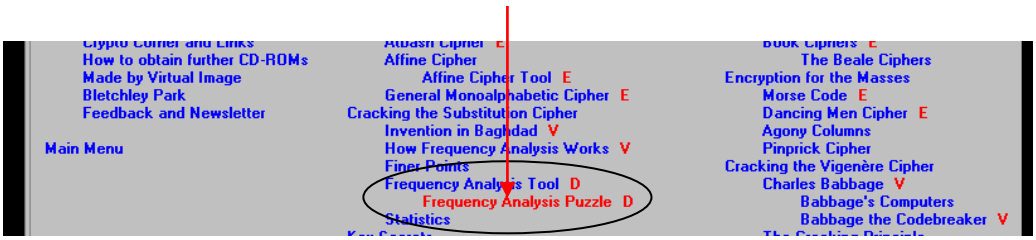
Assignment 10

Try one of the Junior Frequency Analysis Puzzles

To find the Puzzles on the computer click on the question mark on the homepage



Then select Frequency Analysis Puzzle and Select



Select Pick Cipher Text and the bottom of the screen

then use the analysis tools at

In the early Nineteenth century the advent of the telegraph inspired Morse code. Later the invention of radio meant messages could be sent quickly, but could be intercepted by anyone. The use of codes escalated during World War One. Armies needed to relay signals from Headquarters to the troops in the field. The enemy could easily listen to the radio signals so armies needed a code that was easy to encipher and decipher but difficult to crack. Coding became more sophisticated but it meant that valuable time was lost encrypting and decrypting messages for your own troops.