CIPHER HUNT

Guidance brochure

http://cipherhunt.info

EUYSRA **PSMG**

Hidden Messages

Codes and ciphers don't have to be complicated. Messages have been hidden in simple ways for thousands of years.

Steganography is the practice of concealing your message (rather than ***encrypting*** it). For example, the ancient Greeks wrote about a message tattooed on someone's head (which they hid by letting the hair grow over it).

Invisible ink is another example, perhaps the writing only shows up under UV light or with special glasses.

Spy stories often used to mention '**microdots**' where information was hidden in very small dots. Perhaps the dot of this letter **"i"** contains a microscopic message?

Basics

The first few ciphers will make for an easy introduction. They are closer to **steganography** than **cryptography**.

If you are ever stuck, and feel like you are at a dead end… you may need to reverse and try again.

Your initial ideas might not be correct, but they're always worth trying.

Knowing your alphabet is going to be important.

The very first cipher is at the end of this brochure.

Not all of the methods in this brochure are necessarily used in the ciphers.

Vocabulary

Steganography is the practice of hiding a message.

Cryptography is the practice of code making and breaking.

A **Code** replaces one word or phrase with a ‘code-word’ or phrase.

A **Cipher** replaces one letter with another symbol.

`plaintext` is the text which you can read as normal – it is usually written in `lower case`.

`CIPHERTEXT` is the encrypted text, usually written in `UPPER CASE`.

Encrypting means turning `plaintext` into `CIPHERTEXT`

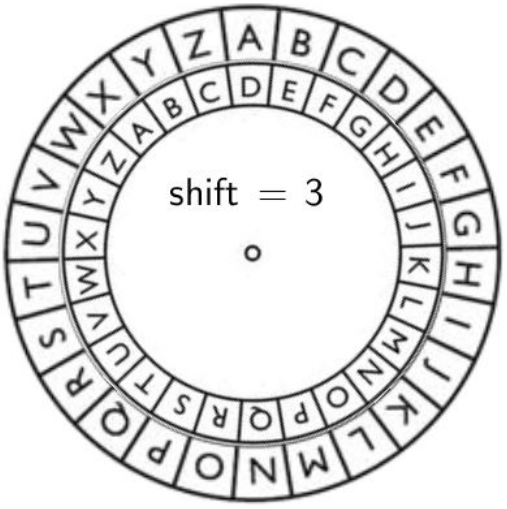
Decrypting means turning `CIPHERTEXT` into `plaintext`.

Cryptanalysis is the process of breaking a code, without knowing the key/method. This is what codebreakers must do.

Caesar Ciphers

The idea of switching one letter for another letter (or symbol) is the most basic idea of creating a **cipher.**

The most famous simple cipher is the **CAESAR SHIFT CIPHER.** Letters are replaced with a letter a certain number of places further along the alphabet. A Caesar Wheel is a good way to see this.



Julius Caesar used this with a shift of 3 to communicate with his Roman Army generals. It's pretty easy to break this code with a pen and paper.

Vsof opcih hvs ghohwghwqwob □kvc rfckbsr qfcggwbu o fwjsf? Wh □kog hvfss tssh rssd cb ojsfous.

Substitution Ciphers

Obviously you don't have to just switch letters in a cycle like the Caesar Shift. You could use a **Substitution Cipher.**

For example, put the letters in a table:

PLAINTEXT	CIPHERTEXT
a	B
b	A
c	T
d	H
e	C
f	D
g	E
h	F
i	G
j	I
k	J
l	K
m	L
n	M
o	N
p	O
q	P
r	Q
s	R
t	S
u	U
v	V
w	W
x	X
y	Y
z	Z

Now a message such as

`take me to your leader`

becomes

`SBJC LC SN YNUQ KCBHCQ`

The 'key' on the right is the word `BATH`. If you write that down first (and ignore any repeated letters), then continue the alphabet (leaving out letters you've already used) you create a substitution table.

To encrypt turn the lower case letters (`plaintext`) into UPPER CASE (`CIPHERTEXT`) by reading from left to right.

To decrypt turn the `CIPHERTEXT` into `plaintext` by translating from right to left.

Cryptanalysis

For ciphers such as the Caesar and Substitution you can begin cryptanalysis by looking at which letters or symbols turn up most often.

This is called **FREQUENCY ANALYSIS.**

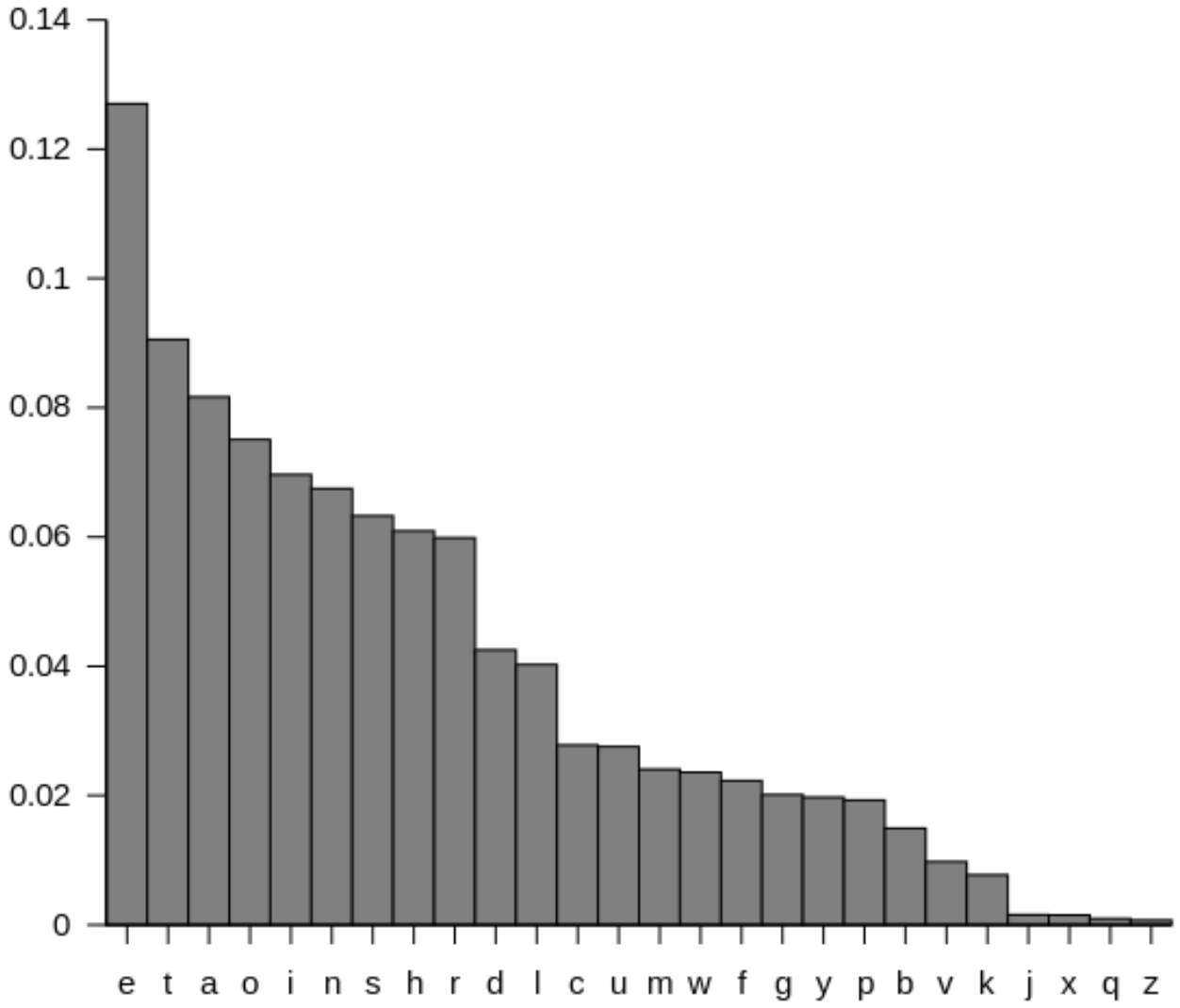
You probably already know that “e” is the most common letter in the English language

If a message contains more of one letter than any other, it *might* be representing the letter “e”.

The next most common letters are (roughly in order) t, a, o, i, n, s, h, r – but there is no guarantee that a short message contains letters in this order of frequency.

At the other extreme it is (usually) unlikely that letters like j, x, q, and z will turn up very often!

ENGLISH LANGUAGE LETTER FREQUENCY



Poly-alphabetic Ciphers

Any **monoalphabetic** (‘one alphabet’) cipher is susceptible to cryptanalysis by frequency analysis, but there are relatively simple ways to conceal the frequencies.

For example, if the letter ‘e’ was encrypted as an ‘A’ sometimes, but also as a ‘B’ sometimes, it would be much harder to spot.

This is the basic idea of a **polyalphabetic** cipher (‘many alphabets’) – where more than one encryption is used for an individual letter.

Good examples are the **Vigenère Cipher**, and the **Enigma Cipher** (see separate sheets).

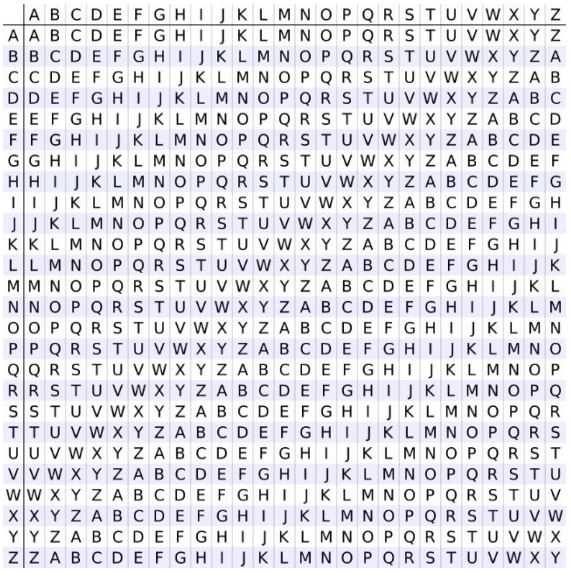
Frequency analysis will probably not help crack these ciphers (or at least not at first), so more advanced techniques are required…

Vigenère Cipher

In the 16th century **Giovan Battista Bellaso** published the first description of this cipher.

Unfortunately for Bellaso, it was misattributed to **Blaise de Vigenère** in the 19th century after he published a slightly different version.

The simple idea of encryption with a Vigenère cipher is to use a Caesar shift, but a different one for each letter in the 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
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

This table contains all 26 possible Caesar Shifts.

All that is needed beyond the table is a key or keyword (e.g. `BATH`)

For the first letter in the `plaintext` use the `B` from the keyword to tell you which row of the table to use, and encrypt your letter as the appropriate entry in that row.

For the second letter in the `plaintext` use the `A` row.

For the third, use the `T` row, and the fourth, the `H` row. Then for the sixth letter, use the `B` row again. Repeat as needed.

Vigenère Cipher Example

To encrypt:

itwasbellasosideafirst

with a key of “BATH”, you would write your keyword above the message repeatedly

BATHBATHBATHBATHBATHBA
itwasbellasosideafirst

Then use the appropriate row from the Vigenère Table to encrypt your message.

Find the letter underneath the letter i in row B (J)

Find the letter underneath the letter t in row A (T)

Find the letter underneath the letter w in row T (P)

So the encryption eventually becomes:

BATHBATHBATHBATHBATHBA
itwasbellasosideafirst
JTPHTBXSMALVTIWLBFBYTT

You can see how “e” became “X” and then later “L”

To start decryption (with the key) look for row B, then find the letter at the top of the column where J appears (I). Repeat.

	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

Transposition Cipher

Transposition ciphers are very simple, but can still be an effective way of concealing a message.

Here's an example with plaintext (25 characters):

myverysecretmessageisthis

Write it in a grid (e.g. with 5 columns), working across from left to right.

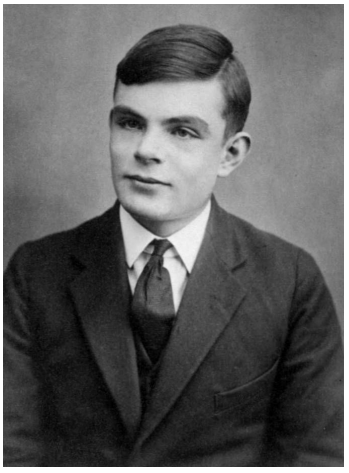
m	y	v	e	r
y	s	e	c	r
e	t	m	e	s
s	a	g	e	i
s	t	h	i	s

Re-write the message as ciphertext by reading down the columns. MYESSYSTATVEMGHECEEIRRSIS

This is basically an anagram of the plaintext, so frequency analysis will not help since the all the original letters are still there.

Without knowing the size of grid it is hard to read. You can further conceal things by reordering the columns, then the 'key' is the just the number and order of columns.

Alan Turing



Alan Turing (1912-1954) was, among other things, an English cryptoanalyst and mathematician, and is regarded the father of theoretical computer science and artificial intelligence. His paper “On Computable Numbers” published in 1936 considered the hypothetical concept of a “universal computing machine”, and Turing proved that such a machine could execute any conceivable mathematical operation that could be represented as an algorithm, leading to the central concept of modern computers. When World War II arrived, Turing was a leading participant in breaking the German “enigma” ciphers, at Bletchley Park - the UK institute dedicated for deciphering the secret messages of the enemies of the Allies. His work involved the improvement of the so-called Bombe, an electro-mechanical machine which through logical deductions was able to find the settings of the Enigma decryption device. After the war, he worked at the National Physical Laboratory, designing one of the first computers able to store programs, called the Automatic Computing Engine. If you want to know more about Alan Turing, you can read his biography “Alan Turing: The Enigma” written by Andrew Hodges.

Source: https://en.wikipedia.org/wiki/Alan_Turing

ENIGMA

The ENIGMA machine was used by the Nazis in WWII to send secret military messages. Cracking the code was obviously very very valuable to the Allies, in order to find out what the Germans were doing.

Alan Turing (among others at Bletchley Park) helped the British Intelligence service to crack the ENIGMA ciphers. The story is given the Hollywood treatment in the film **The Imitation Game**.

Just like the **Vigenère** cipher, each letter in the plaintext could be encrypted differently each time. This means that frequency analysis is unhelpful.

By far the easiest way to read an Enigma code is to find the **key** (the settings used on the ENIGMA machine to send the message).

Elizebeth Friedman

Elizebeth Friedman (1892-1980) was an American cryptoanalyst and an author, and a pioneer in U.S. cryptotechnology. After studying English literature at university, her expertise in Shakespeare led her to Riverbank Laboratories - a facility dedicated to decrypting enciphered messages. After leaving Riverbank, Friedman was employed by the U.S. Treasury Department to fight international smuggling and drug-running into the country. Using well-known techniques and some of her own invention, she decoded a total of 80,000 secret radio messages between smugglers which she forwarded to the Coast Guard offices. At the advent of World War II, Friedman and her codebreaking unit provided FBI with messages sent between Nazi spies in South America, leading to the downfall of every Nazi spy network on the continent. Her husband William Friedman went on to become the chief cryptologist of the NSA, which he helped to create, in 1952. After retirement, the Friedmans together wrote a manuscript dismissing the idea that Francis Bacon had played any part in writing the works of Shakespeare, which had initially brought the two together at Riverbank. If you want to know more about Elizebeth Friedman, you can read her biography ”The Woman Who Smashed Codes” written by Jason Fagone.

Sources: National Geographic, Military Wiki

RSA Encryption

RSA stands for (Ron) **Rivest**, (Adi) **Shamir**, and (Leonard) **Adleman** - the Americans who first publicly described the algorithm in 1977.

An Englishman named **Clifford Cocks** had discovered the process three years earlier. Unfortunately he was working for **GCHQ** and his work was classified, and not revealed until 1997!

RSA encryption relies on the fact that it is **easy** to multiply two large numbers together, but **hard** to reverse the process (i.e. factorise large numbers).

The RSA system contains a public key – which anyone can see, and a private key (which is kept private by the person wanting to receive a message). Encryption is done with the public key, but only the receiver has the private key, which helps them read the message.

If you can factorise the large **semi-prime** in the public key then you, in theory, can deduce the private key, and so decrypt the message.

You'll need to read more to fully understand!

https://en.wikipedia.org/wiki/RSA_(cryptosystem)

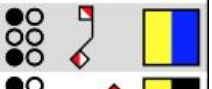
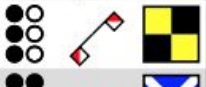
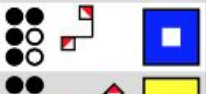
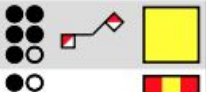
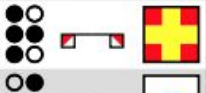
Breaking unfamiliar codes/ciphers

You are going to encounter codes/ciphers that encode the message in no well-known method.

To crack these, you will need a mix of creativity, logic, pattern-recognition, acumen and perhaps a good idea! This may also need to be combined with good research skills…

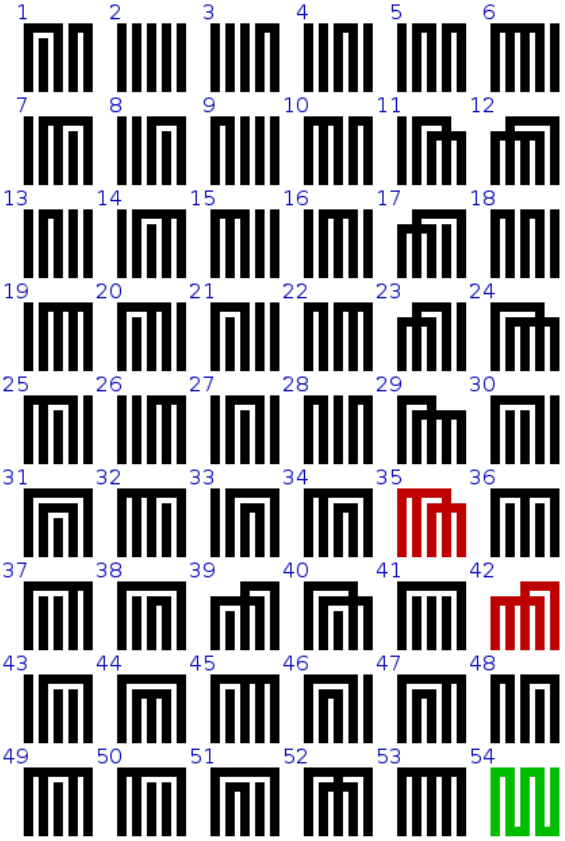
It is always a good idea to look for foreign number/alphabet systems in your cipher!

You may find helpful the following picture showing the most common encodings of letters.

1	A	•-	
2	B	-•••	
3	C	-•-•	
4	D	-••	
5	E	•	
6	F	••-•	
7	G	--•	
8	H	••••	
9	I	••	
10	J	•---	
11	K	-•-	
12	L	•-••	
13	M	--	
14	N	-•	
15	O	---	
16	P	•--•	
17	Q	--•-	
18	R	•-•	
19	S	•••	
20	T	-	
21	U	••-	
22	V	•••-	
23	W	•--	
24	X	-••-	
25	Y	-•--	
26	Z	--••	

Genji symbols

One example of (quite a hard) non-traditional code could be the use of traditional Japanese symbols for the chapters of the Tale of Genji.



52 of these symbols may be seen to represent the 52 possible partitions of a 5-element set. Notice that this is twice 26 - if we were to impose a reasonable ordering on the 5-element set partitions, we would obtain an encoding of ‘a,b,c,...,z,a,b,c,...z’ with the chapter symbols.

The fact that each letter would be represented by two symbols would also discard the frequency analysis as a mean of decoding your message!

The first cipher

#1

THE FIFTH WORD OF THIS SENTENCE.

THE ANSWER TO THE FIRST CIPHER IS

Credit for many parts of this brochure:
Ben Sparks, The University of Bath