Queen Mary University of London

Herod's Secret Message

Did King Herod know about **cryptography**? It is a way to keep things secret by swapping letters for others using a **cipher**, so only those with the **key** can read the message. Perhaps, if he did, Herod might have sent a *sinister christmas message* like this. Can you work out what it says?

GUR ER VF GNYX BS N ONOL UN

IVAT ORRA OBEA GUNG JVYY O

R N SHGHER XVAT N EHZBHE V

F GUNG UR VF VA N FGNOYR J

VFR ZRA NER GENIRYYVAT SEB

Z GUR RNFG SVAQ GUR ONOL X

VAT UREBQ

You need to fill out the grid below writing the **plaintext** (the original message in english) below the **ciphertext** (the secret version) as you crack it.

G	U	R	E	R		V	F		G	N	Y	X		B	S		N		O	N	O	L		U	N

I	V	A	T		O	R	R	A		O	B	E	A		G	U	N	G		J	V	Y	Y		O

R		N		S	H	G	H	E	R		X	V	A	T		N		E	H	Z	B	H	E		V

F		G	U	N	G		U	R		V	F		V	A		N		F	G	N	O	Y	R		J

V	F	R		Z	R	A		N	E	R		G	E	N	I	R	Y	Y	V	A	T		S	E	B

Z		G	U	R		R	N	F	G		S	V	A	Q		G	U	R		O	N	O	L		X

V	A	T		U	R	E	B	Q																	

If you need help (you probably do!) then read on … (and the answer is on the final page).

What kind of cipher might it be?

Herod lived in Roman times. A kind of cipher that was known then involved substituting different letters for the ones in the original message. For example an E might always be changed to an S, an F always to a Z and so on. Roman Emperor, Julius Caesar, used cryptography to keep his personal military messages secret. The version he used is now called a Caesar cipher after him. He swapped every letter for one three places earlier in the alphabet: D became A, E became B and so on, with A jumping back to X, B to Y and C to Z. Augustus Caesar who was the Roman Emperor when Jesus was born used a simpler variation of a Caesar cipher shifting letters by one place in the other direction so A became B, B became C and so on, but with Z becoming AA rather than A.

The key to solving Caesar cipher is to work out how far a shift has been made then write the alphabet above another copy but shifted by different amounts. For example for Julius Caesar's cipher you would create the grid:

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	ciphertext
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	plaintext

To encript a message - the plaintext - find the letter from your message in the bottom row and write the letter above it in the ciphertext row. To decrypt a message that is written using the Caesar cipher, work the other way. Find the letter from the encrypted message in the top row and write down the letter in the bottom row. Do this a letter at a time to recover the original message. To do that you need to know how big a shift has been used

So to decrypt the message you need to be able to fill in the grid below with the alphabet shifted the right amount.

																										ciphertext
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	plaintext

To crack Herod's cipher you could just try all 26 possibilities of the Caesar Cipher in turn. FIrst shift by one place and try and decipher the message. Then shift by two places and try again… and so on. All but one attempt will continue to give gobbledygook, but when you get the right one, a message in english will appear. You do not have to decrypt the whole message each time - one word might be enough. If it gives nonsense try a different shift. If it makes a word decrypt another word that way to check if it really works, and so on.

That will work, but perhaps it is too slow or too much work for you! If so perhaps you can think of a better way. If you want to try another way then read on …

Cribs

If you are lucky, the person writing the message may have given you a way to decrypt it because of what they wrote. If you can guess what any of the words might be then you can try putting that in the message. For example, people often start letters “Dear …” or end them with their name. Guesses of a word that might be in the message at a given place like this are called **cribs**. Try putting the crib (like DEAR) in as that bit of the message, then you can see if the letters of the crib fit. Do those letters fit the pattern of a Caesar cipher (i.e. do they all correspond to the same number shift)? If so you have worked out which key to try first. Try it and see if the message emerges. If it does your guess was right. If not, back tot he drawing board.

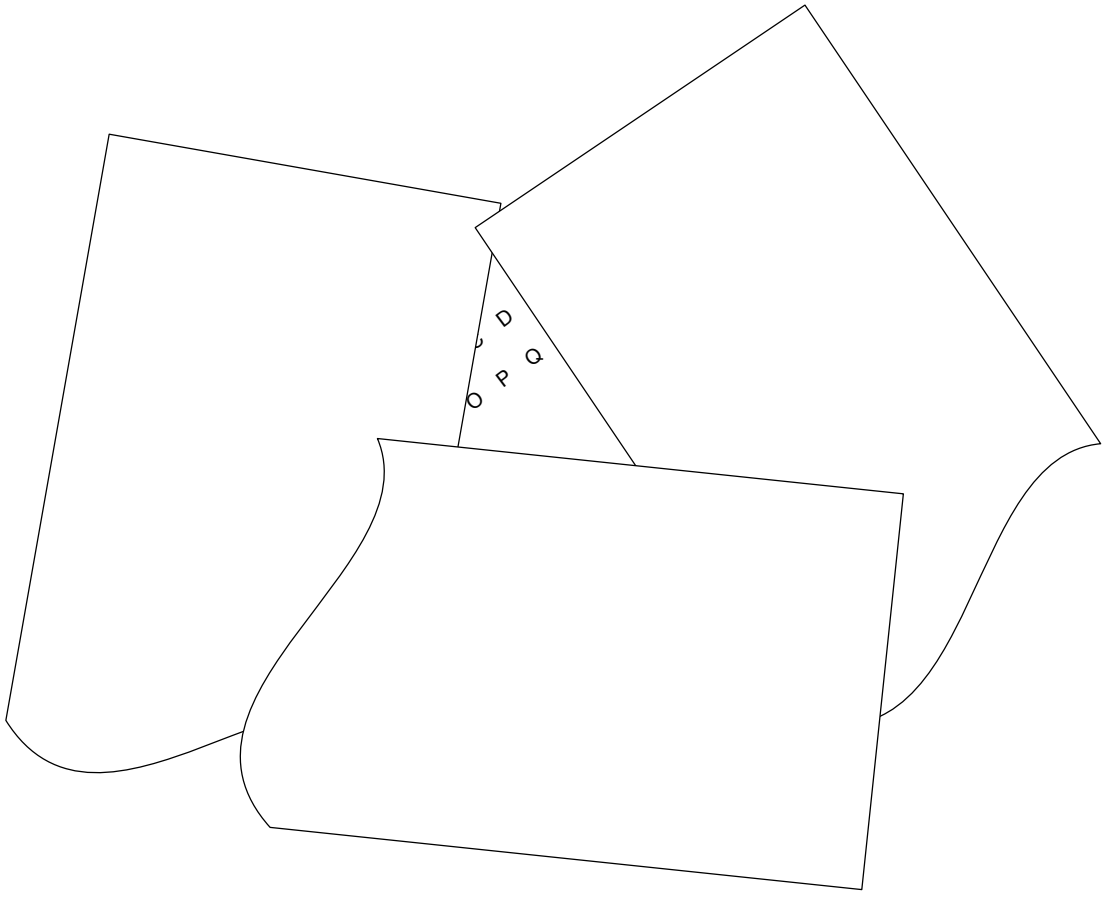
Can you crack Herod’s message using a crib?

If not then read on to find another way.

Stealing the Key

Another way is to use old fashioned spying and try and steal the key. If either the sender or receiver have written it down then it may be possible for you to get a copy. Obviously this is dangerous unless you have a reason to be there! However, if you have intercepted the message perhaps you have a chance. Look for grids amongst the papyrus, like the ones earlier. Even seeing a fragment may be enough to work out what the key is.

For example perhaps you saw the following written in a pile of papyrus in the home of the person the message was for.



Perhaps you can work out what the full key must be from this glimpse of just a part of it?

If not, then read on to get the full key.

Queen Mary University of London

The Key

If you haven't cracked the message yet, then perhaps you will be lucky enough to get the chance to steal the whole key. From the glimpse above though it is clear that Q turns in to D. They are 13 letters apart. Perhaps it is a Caesar cipher where every letter is shifted by 13 places.

Here it is:

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	ciphertext
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	plaintext

A Caesar cipher with a shift of 13 places, actually means you use the same substitution to encrypt and decrypt messages as A becomes N but also N becomes A.

Can you decrypt the message now using the key? Find the answer overleaf.

Queen Mary University of London

The decrypted message

Here is the final decrypted message. Did you manage to work it out?

G	U	R	E	R		V	F		G	N	Y	X		B	S		N		O	N	O	L		U	N
T	H	E	R	E		I	S		T	A	L	K		O	F		A		B	A	B	Y		H	A

I	V	A	T		O	R	R	A		O	B	E	A		G	U	N	G		J	V	Y	Y		O
V	I	N	G		B	E	E	N		B	O	R	N		T	H	A	T		W	I	L	L		B

R		N		S	H	G	H	E	R		X	V	A	T		N		E	H	Z	B	H	E		V
E		A		F	U	T	U	R	E		K	I	N	G		A		R	U	M	O	U	R		I

F		G	U	N	G		U	R		V	F		V	A		N		F	G	N	O	Y	R		J
S		T	H	A	T		H	E		I	S		I	N		A		S	T	A	B	L	E		W

V	F	R		Z	R	A		N	E	R		G	E	N	I	R	Y	Y	V	A	T		S	E	B
I	S	E		M	E	N		A	R	E		T	R	A	V	E	L	L	I	N	G		F	R	O

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

V	A	T		U	R	E	B	Q																	
I	N	G		H	E	R	O	D																	

Encryption is massively important in the modern world, though we leave computers to do the encryption and decryption. It allows people to send private messages to each other that stay private even though the messages pass through lots of other computers as they are delivered. Encryption acts like a sealed envelope for a normal letter.

It is also used to transfer electronic money. In fact the modern banking system could not work at all without strong encryption that cannot be cracked unless you actually have the key. Modern ciphers are far, far harder to crack than the ones used in Roman times like the one we cracked above.