How to be a Secret Agent

KS4 - Mathematical Codebreaking

Cryptography

- Cryptography and ciphers have been around for thousands of years. Initially these methods used pen and paper or simple machines to protect messages and information from being shared with the wrong people.
- Some of you may have heard of the Enigma machine and the efforts required to break the cipher generated by it during World War 2.
- Modern cryptography is heavily based on mathematical theory and computer science. We can use computer algorithms to calculate hardness assumptions making such algorithms hard to break in practice by anyone who is trying to decipher your message.

Caesar Shift

It is called this because Julius Caesar actually used it to send military messages to his army. (See we told you it had been around a while)

- The Caesar Shift is one of the simplest codes that can be used in cryptography. It is what we call a substitution code. This means that each letter is replaced with another one.
- To encrypt or decrypt a Caesar shift we first list the alphabet, and then move every letter of the alphabet forward a certain number of places. For example, for a Caesar shift of three, each letter moves along three places:

Alphabet:	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
Cipher:	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

- Here we would decode A as X, B as Y etc. So the message KHOOR translates to HELLO.

- Caesar shift codes can be broken once you know how many places you need to shift the letters by.
- You are going to attempt to decipher a code by conducting simple frequency analysis. Frequency analysis looks at how often letters appear in the English language. The table below displays these frequencies from most to least frequent.

E	T	A	O	I	N	S	H	R	D	L	U	C
12.7	9.1	8.2	7.5	7.0	6.7	6.3	6.1	6.0	4.3	4.0	2.8	2.8
M	W	F	Y	G	P	B	V	K	X	J	Q	Z
2.4	2.4	2.2	2.0	2.0	1.9	1.5	1.0	0.8	0.2	0.2	0.1	0.1

- This means for any coded message, our most commonly used letter should relate to one the most commonly used letters when written in English.
- For the message below, work out which letter is the most common and set this as E. Use this information to then work out the rest of the cipher. You will need to write out your alphabet like on the previous page and then use this to decipher the message below.

ITKTEEXE EBGXL ATOX LH FNVA BG VHFFHG, BM'L T LATFX MAXR'EE GXOXK FXXM.

Transposition Ciphers

- Transposition Ciphers are based on a simple idea, but are more difficult to crack that codes like the Caesar shift.
- A transposition means that the letters of the code are simply rearranged into a different order.
- For example, ICBKAOREMDERAEAA, can be rearranged into rows of length 4 to give:

I	C	B	K
A	O	R	E
M	D	E	R
A	E	A	A

- This message is then read down each row; I AM ACODEBREAKER
- Now have a go at the below. This one does not form a 4x4 grid.
- Using squared paper, try different combinations until you find the Maths pun that has been coded.

TLAVURITEAEKASREELTESMLHRDAIEOOTTOMONHGSTTSIQS

COMPETITION TIME!

Prize available for 1st place

Honourable mentions for 2nd and 3rd place

Your Task

- This task is a little more tricky than the previous ciphers.
- In the coded text on the next slide, every letter in the original message was switched with another letter, this is different to that of the two previous ciphers we have looked at. E.g. a>e and e>a
- Points are given for how many letters are correctly identified and the most points are given if you manage to decipher the whole text.

Some hints to help you.

- Use your knowledge of frequency analysis from looking at Caesar Shifts to help decipher this code.
- Think about what letters repeat, follow apostrophe's or are often written on their own and use this to find your initial letters.
- Another hint is that the last line looks like a URL. We know these are usually .com, .org, .edu etc. Use these to try and find some of the letters.

Here is your coded text

Vfj Uzyj fxc pjjw nzkrgwi tjkl fxkc xyy vfj uzkwgwi, qbkgwi-dyjxwgwi fgq ygvvyj fzuj. Hgkqv ngvf pkzzuq, vfjw ngvf cmqvjkq; vfjw zw yxccjkq xwc qvjbq xwc dfxgkq, ngvf x pkmqf xwc x bxgy zh nfgvjnxqf; vgyy fj fxc cmqv gw fgq vfkzxv xwc jljq, xwc qbyxqfjq zh nfgvjnxqf xyy ztjk fgq pyxdr hmk, xwc xw xdfgwi pxdr xwc njxkl xkuq. Qbkgwi nxq uztgwi gw vfj xgk xpztj xwc gw vfj jxkvf pjyzn xwc xkzmwc fgu, bjwjvkxvgwi jtjw fgq cxkr xwc yznyl ygvvyj fzmqj ngvf gvq qbgkgv zh cgtgwj cgqdzwvjwv xwc yzwigwi. Gv nxq quxyy nzwcjk, vfjw, vfxv fj qmccjwyl hymwi cznw fgq pkmqf zw vfj hyzzk, qxgc 'Pzvfjk!' xwc 'Z pyzn!' xwc xyqz 'Fxwi qbkgwi-dyjxwgwi!' xwc pzyvjc zmv zh vfj fzmqj ngvfzmv jtjw nxgvgwi vz bmv zw fgq dzxv. Qzujvfgwi mb xpztj nxq dxyygwi fgu gubjkgzmqyl, xwc fj uxcj hzk vfj qvjjb ygvvyj vmwwjy nfgdf xwqnjkjc gw fgq dxqj vz vfj ixtjyjc dxkkgxij-ckgtj znwjc pl xwguxyq nfzqj kjqgcjwdjq xkj wjxkjk vz vfj qmw xwc xgk. Qz fj qdkxbjc xwc qdkxvdfjc xwc qdkxppyjc xwc qdkzzijc xwc vfjw fj qdkzzijc xixgw xwc qdkxppyjc xwc qdkxvdfjc xwc qdkxbjc, nzkrgwi pmqgyl ngvf fgq ygvvyj bxnq xwc umvvjkgwi vz fguqjyh, 'Mb nj iz! Mb nj iz!' vgyy xv yxqv, bzb! fgq qwzmv dxuj zmv gwvz vfj qmwygifv, xwc fj hzmwc fguqjyh kzyygwi gw vfj nxku ikxqq zh x ikjxv ujxczn. 'Vfgq gq hgwj!' fj qxgc vz fguqjyh. 'Vfgq gq pjvvjk vfxw nfgvjnxqfgwi!' Vfj qmwqfgwj qvkmdr fzv zw fgq hmk, qzhv pkjjojq dxkjqqjc fgq fjxvjc pkzn, xwc xhvjk vfj qjdymqgzw zh vfj djyyxkxij fj fxc ygtjc gw qz yzwi vfj dxkzy zh fxbbl pgkcq hjyy zw fgq cmyyjc fjxkgwi xyuzqv ygrj x qfzmv. Emubgwi zhh xyy fgq hzmk yjiq xv zwdj, gw vfj ezl zh ygtgwi xwc vfj cjygifv zh qbkgwi ngvfzmv gvq dyjxwgwi, fj bmkqmjc fgq nxl xdkzqq vfj ujxczn vgyy fj kjxdfjc vfj fjcij zw vfj hmkvfjk qgcj.

Javkxdv hkzu 'Vfj Ngwc gw vfj Ngyyznq' pl Rjwwjvf Ikxfxuj

Xtxgyxpyj vz kjxc gw hmyy xv nnn.imvjwpjki.zki

Competition Entries

- Email: Competitions@gordons.school
- Send your initial decryptions in addition to your final task for additional points.
- When you email, please use the subject heading ‘KS4 Week 2 – How to be a Secret Agent’
- • Closing date: 9am 5th February 2021
- • Winners will be announced via weekly Schoolcomms