How to be a Secret Agent

KS3 - 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.

COMPETITION TIME!

Prize available for 1st place

Honourable mentions for 2nd and 3rd place

Your Task

- On the next slide you will have some encrypted text to decipher.
- Use your knowledge of frequency analysis and other clues to try and workout what Caesar Shift has been used, once you know how it has been shifted you should be able to decipher the whole text.
- Think about what letters sometimes repeat or are often written on their own and use this to help you find your first letter.
- You can send your partially or completed decrypted text as your competition entry, plus the bonus part which is hidden within the encrypted text.

Here is your coded text

“Xu iwxh atiitg upaah xcid ndjg wpcsh, iwxcz rpgtujaan pqdji lwpi xi hpnh. Qn bn qxgiw X gpcz pqdkt ndj, qji sdc’i qt pugpxs du bn vgtpicthh. Hdbt pgt qdgc vgtpi, hdbt prwxtkt vgtpicthh, pcs hdbt wpkt vgtpicthh iwgjhi jedc iwtb. Ndjg upit plpxih ndj.”

Ltaa sdct udg strxewtgxcv iwt itmi. Ndj wpkt yjhi hjrrthhujaan jhts iwt Rpthpg Hwxui rxewtg pcs iwxh itmi wps p Rpthpg Hwxui du tatktc. X pahd rwpaatcvt ndj id uxcs dji lwxrw upbdjh eapnlgxvwi lgdit iwt fjdit pqdkt pcs lwxrw eapn xi xh ugdb.

Competition Entries

- Email: Competitions@gordons.school
- When you email, please use the subject heading ‘KS3 Week 2 – How to be a Secret Agent’
- • Closing date: 9am 5th February 2021
- • Winners will be announced via weekly Schoolcomms