How to be a Secret Agent

KS5 - 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 A CODEBREAKER
- 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, the text has been double encrypted, first using a substitution cipher and then using a transposition cipher. Can you decipher it?

Some hints to help you.

- Use your knowledge of frequency analysis to calculate which letters appear most in your coded text and then compare this to which letters normally appear most in the English Language.
- NRICH has a Cipher Toolkit to help with frequency analysis at https://nrich.maths.org/7983

Here is your coded text

whhujnjwuzlwvvdhgdlkqwdhvdkelqhldwurlhhwklwwuhdwdgqjkhzq
qbrhowkgbqkqywhuovwfzebzlhhzfwrlkwrhddhhhkdqsqhkkuohkrfq
qdujdbjdvulhgoidpwggvhlgvwqdhollduwzudhwqqhhrwqmguqzrzllj
ykrzyaprgxuidlqdwfrhhwlhfdppvhduwwvkerukuwuhvldwqwbkgfkh
gbrdkwsnpgrdkufrdrogpxllkwhhduqhhrrowohrvogrdocpggugouodv
dghzrxvbrhlwderdhqiohddqjdqrwqkquxwggurujbwkphoxdhgluldfhi
qhfvwhdrvubpfhokrqzfqkxddqjvbornghdofkrwlseqgldvlwijgogklqvo
srvffxxykuosozzwyvgrxrrdgehhrddddlhhduvwirovxguqvvewqsqb

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 ‘KS5 Week 9 – How to be a Secret Agent’
- • Closing date: 6th July 2020
- • Winners will be announced via weekly Schoolcomms