Cryptography

Advanced Math Circle

May 5, 2016

Today we are going to be learning about cryptography, with an emphasis on some fun, games and code . After all, the whole point cryptography make and also break codes!

So let's learn about perhaps the simplest type of cypher, called the Ceaser Cypher. For encrypt a message, all that you have to do is pick a number n between 1 and 25, and replace each letter in your message with the letter that comes n letters later (wrapping around back to 'a' if you were going to go past 'z').

1. Do the following, all related to the Ceaser cypher

   (a) Encrypt the message "Retreat!" with a Ceaser cypher with $n = 1$

   (b) Encrypt the message "There is a sucker born every minute" with a Ceaser Cypher $n = 3$

   (c) Decrypt "GJTIB SFGSJ FOETO PUGPP E" if you know that it was made with a Ceaser Cypher with $n = 1$

(d) Decrypt the message: ”P KVU’A AOPUR DL’YL PU RHUZHZ HUFTVYL!” Hint, this is a Ceaser Cypher with $3 < n < 11$. Hint, Toto

(e) You can make code breaking much more difficult if you get rid of all spaces and punctuation, and break the letters into 5 letter blocks. Try and decrypt the following message ”FGBCG ELVAT GBZNX RSRGP UUNCC RAVGF ABGTB VATGB UNCCR A”. Hint, this is classic Regina George.

Ceaser Cyphers are part of a more general class of cyphers called substitution cyphers. In a substitution cypher, is one where a table is formed, that pairs each letter with another letter. When you want to encrypt a message, just replace each letter with it's pair.

2. Super quick combinatorics questions.

   (a) How many different Ceaser cyphers are there?

   (b) How many different substitution cyphers are there?

   (c) If you had a computer that could try 1 trillion (10^{12}) substitution cyphers per second, how long would it take on average until you found the right cypher? Hint, $26! \approx 4 \times 10^{26}$, and there are 31557600 seconds in a year.

3. Even if trying to 'brute force' a substitution cypher is useless, you can still break them with a little time, and some clever thinking. Paradoxically, the longer a message is, the easier it is to break.

   (a) On the last page of the hangout, you can see a list that orders the letters in English by how often they occur. Use that decrypt the following substitution cyphered message: "OC OMOM MFWMCU UMEY FELA WMU FESA M BXK XL JVXJXFMRAU. CXI NATAD SNXW WVMR CXI'DA ZXNNM ZAR." Hint, ping pong.

(b) Try this one: "KRFC CB VFBK GBK X UBC CGYAY AMRTA? NZ ERCGYT KRA R ITXFVYT RFI R EXYFI". Hint Raaachel.

(c) In case you figure those two out really quickly, here are a few more, which don't have the length of the words to guide you "OGAVS HTVEG CSJNP MJPOH DKPAT AQAAI "

(d) ”BCZOT HTLHB OCVSY HBTVP LHNCV PONHB FVAOF NFSTH HSOBC ZOTLO AAOGH TUOFS CHCAB CZOTL QFVPO NCXL”

(e) ”UIZZR YNPHY IEXEP EGRYR PSRNH NRJLE ZZIKY NTHSU ICACI AHCIS RKEI”

4. Now we are going to have a little game. The instructors are going to distribute some cypher text, and you are going to try and decrypt as many of them as possible working with your table as a team. Some of the messages will be encrypted with a Ceaser Cypher, and other with a different substitution cypher. The table that wins won’t get any prizes, but they will live in eternal glory!

Some useful information:

The most common letters in English are in order: ’e t a o i n s h r d l c u m w f g y p b v k j x q z’

The most common letters that start words are in order: ’t a s h w i o b m f c l d p n e g r y u v j k q z x’

The most common bigrams (two letter combinations) are: ’th he in er an re nd at on nt ha es st en ed to it ou’

The most common trigrams are: ’the and tha ent ing ion tio for nde has nce edt tis oft sth men’

The most common repeated letters are: ’ss ee tt ff ll mm oo’

And finally, here are all of the letters of the English alphabet, in order for quick reference. Below them, is their number in the 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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26