Homework 1

Casey Bates

13 April 2020

1 Frequency Analysis

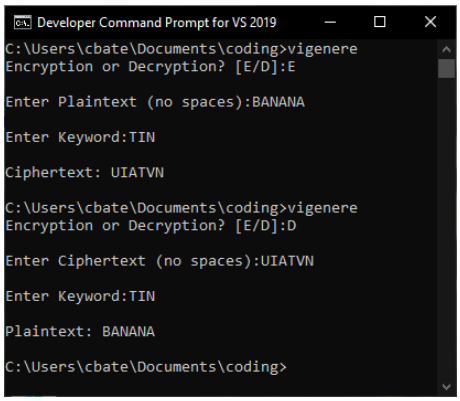
Given (From Lecture): J - e, A - t, Z - h, R - r
Given CT: here there VX F XtrMCO trFUVtVMC MQ XtMrI teTTVCO FX F reXNTt MQ thVX GMXt WeMWTe Fre treGeCUMNX WNKTVP XWeFSerX FCU there VX FTGMXt CM HrVtteC XWeePh

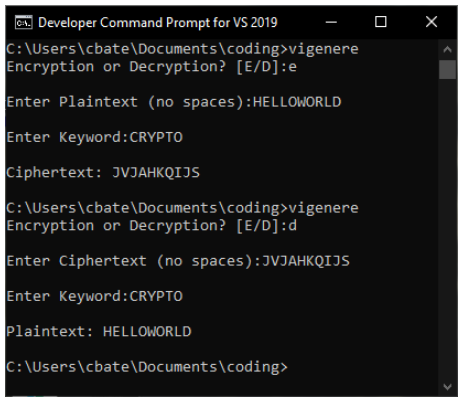
Method:
Tried F - a, since 'a' and 'i' are only single-letter words in the English language.
Tried FCU - and, since 'and' is a common trigram.
Tried CM - no, since 'no' is the only two letter word starting with 'n'.
Now we have the word 'tradVtVon', so V - i.
We have 'iX', so X - s
At this point, most of the words are only missing one or two plaintext letters, so using common sense we are able to figure out the rest of the ciphertext to plaintext assignments.

Plaintext: here there is a strong tradition of story telling as a result of this most people are tremendous public speakers and there is almost no written speech

2 Vigenere Encryption and Decryption

Code for encryption and decryption of the Vigenere cipher is in vigenere.cpp. Example outputs shown below.





3 Kasiski Method

MOST FREQUENT TRIGRAMS
hal (5 appearances): distance 1 = 135, distance 2 = 25, distance 3 = 10, distance 4 = 50
alv (3 appearances): distance 1 = 30, distance 2 = 15
lrk (3 appearances); distance 1 = 45. distance 2 = 190

All distances are multiples of 5, so they keyword is most likely 5 characters.

Code used to create the following histograms can be found in kasiski.cpp.
[5, **8**, **9**, 2, 1, **12**, 5, **10**, 0, 2, 1, 0, 3, 0, **9**, 1, 3, 3, **7**, 2, 1, **8**, **6**, 0, 1, 3]
Possible Shifts: 14 - 'o'
[**7**, **6**, 0, 0, **7**, 3, 5, **9**, 0, 0, **8**, 3, **8**, 0, 3, 4, 0, 3, 0, **9**, 1, 3, 4, **15**, 2, 3]
Possible Shifts: 19 - 't'
[**6**, 1, 3, 5, 0, 2, 1, **7**, 0, 2, 3, **19**, **7**, 0, **6**, 4, 1, 0, 4, 1, **6**, **11**, 0, 0, **6**, **7**]
Possible Shifts: 7 - 'h'
[2, 0, 3, 0, **12**, 1, 1, **8**, **6**, 5, 4, **8**, 5, 0, 0, 5, 4, 5, **7**, 0, 0, **6**, **8**, **10**, 0, 2]
Possible Shifts: 4 - 'e'
[0, 1, 3, 5, 3, 4, 1, 0, **8**, **8**, **12**, 0, 4, 4, 0, 0, 0, **6**, 3, 2, 3, **14**, 4, 2, 4, **11**]
Possible Shifts: 17 - 'r'

Keyword: other
Plaintext: BANCHOFF DISCOVERED HIS FIRST GEOMETRY THEOREM AS A FRESHMAN EVERY FRIDAY MORNING THE WHOLE SCHOOL WOVLD FILE INTO CHVRCH FOR MASS AND OVR HOME ROOM WAS THE FIRST TO ENTER WHILE WAITING FOR THE REST TO COME IN THERE WAS PLENTY OF TIME TO CONTEMPLATE THE SHADOWS ADVANCING ACROSS THE TILES AT THE BASE OF THE ALTAR RAIL WHEN WE FIRST ARRIVED THE NARROW OF THE ALTER RAIL COVERED ONLY A SMALL PORTION OF THE TRIANGVLARTILES AND

BY THE END OF MASS ALMOST THE ENTIRE TRIANGLE WAS IN SHADOW WHEN I ASKED MYSELF DID THE SHADOW COVER HALF THE AREA I HADNT STVDIED ANY FORMAL GEOMETRY YET BVT I FIGVRED