Cryptanalyst Write-Up

|  |  |
| --- | --- |
| Encrypted | Decrypted |
| EUA IGT LUUR GRR ZNK VKUVRK YUSK UL ZNK ZOSK GTJ YUSK UL ZNK VKUVRK GRR ZNK ZOSK HAZ EUA IGTTUZ LUUR GRR ZNK VKUVRK GRR UL ZNK ZOSK | YOU CAN FOOL ALL THE PEOPLE SOME OF THE TIME AND SOME OF THE PEOPLE ALL THE TIME BUT YOU CANNOT FOOL ALL  THE PEOPLE ALL OF THE TIME |
| B SMVE M HPEMJ RSMR LKE HMY RSBQ KMRBLK WBGG PBQE UN GBVE LUR RSE RPUE JEMKBKC LI BRQ TPEEH WE SLGH RSEQE RPURSQ RL AE QEGI EVBHEKR RSMR MGG JEK MPE TPEMREH EOUMG | I HAVE A DREAM THAT ONE DAY THIS NATION WILL RISE UP LIVE OUT THE TRUE MEANING OF ITS CREED WE HOLD THESE TRUTHS TO BE SELF EVIDENT THAT ALL MEN ARE CREATED EQUAL |
| KMS FW IO BLQQWX KILYJZKMF KFA MWV XUKV OWHY ZWHMVYO ZKM SW BWY OWH KFA XUKV OWH ZKM SW BWY OWHY ZWHMVYO | AND SO MY FELLOW AMERICANS ASK NOT WHAT YOUR COUNTRY CAN DO FOR YOU ASK WHAT YOU CAN DO FOR YOUR COUNTRY |
| DQG JRG VDLG OHW WKHUH EH OLJKW DQG WKHUH ZDV OLJKW | AND GOD SAID LET THERE BE LIGHT AND THERE WAS LIGHT |
| THULWOPIIWAKNIBEKWOALOVD ENEITDTAWEHMIREONWWNKHOD LARIETLNLYDTIOSHTUOETAHS LRIKEEGYSXHXTXXXAXXXRXXX | TWINKLETWINKLELITTLESTAR  HOWIWONDERWHATYOUAREXXXX  UPABOVETHEWORLDSOHIGHXXX  LIKEADIAMONDINTHESKYXXXX |

This was easily the most fun I have had with any assignment in my time at Cal Lutheran. I have spent 24 of the last 48 hours programming and every second was worth the payoff of decrypting the final quote. I will address the quotes in the order of ease of decryption. The first quote was thankfully easy. When dealing with a Caesar cipher, Navid and I realized that there are only 26 possible alphabets that could decrypt the text, each of which can be identified by a number representing the offset of that alphabet from the standard English alphabet. I generated all 26 alphabets and applied them to the encrypted text. Then I ran each solution through a list of the 10000 most common words and generated an accuracy percentage. I returned only the solutions which had an accuracy above a threshold I specified, one of which was the quote.

A computer screen shot of text

Description automatically generated

I used an almost identical technique to decrypt Quote 4. It was still a Caesar cipher, just with no spaces, meaning accuracy checking would be difficult. We realized that we would only have to check 26 solutions still, so I reused my previous code without the accuracy checking and just looked through the solutions.

A screenshot of a computer screen

Description automatically generated

Quote 5 was a new technique, but not a difficult one. When looking through the slides on columnar transposition, we realized that the solution was X rows and Y columns where the product of X and Y is the length of the decrypted text. This meant I only had to write a tool to generate sample outputs using X and Y where X and Y were factors of the text length. 96 has only so many factor pairs, so I just printed out every result and looked at them.

A screenshot of a computer program

Description automatically generated

Quotes 2 and 3 were by far the hardest. I elected to ignore that Quote 2 was technically a different method of encryption than Quote 3 because any method I derived that worked on Quote 3 would also work on quote 2. The tool I created had two functions, generating possible alphabets and applying them and running through the dictionary, both of which required an external file I made. This file stored every letter from the encrypted text and every letter that it could be. For example, the word KILYJZKMF. There are only so many 9 letter words where all 9 letters, except for 1 and 7, are unique. By looking at those words, we can start to narrow down the possibilities from every letter potentially being every letter to something smaller. Doing this repeatedly eventually yields few enough possibilities that we can generate all possible alphabets, apply them, and threshold base on accuracy.

 