Lisa Maszkiewicz

02/10/2020

Cryptology

Prof. Dave Zaret

Homework #1

Problem 1)

Solution:

**IEEIPYEQKVZJRPDPKAPRPVAIFZPKJBFLPJTBEWFZPIAIPFPPIFZNPIFQTLFZ**

NO ONE WOULD HAVE BELIEVED IN THE LAST YEARS OF THE NINETEENTH CENTURY TH-

**JFFZABYETKVYJBDPAIOYJFNZPVXPPIKLJIVNKEBPKLDLAIFPKKAOPINPBOTP**

-AT THIS WORLD WAS BEING WATCHED KEENLY AND CLOSELY BY INTELLIGENCES GRE-

**JFPTFZJIGJIBIEEIPOJRPJFZEQOZFFEFZPEKVPTYETKVBEWBSJNPJBBEQTNP**

-ATER THAN MANS NO ONE GAVE A THOUGHT TO THE OLDER WORLDS OF SPACE AS SOURCE-

**BEWZQGJIVJIOPTETFZEQOZFEWFZPGEKLFEVABGABBFZPAVPJEWKAWPQSEIF**

-S OF HUMAN DANGER OR THOUGHT OF THEM ONLY TO DISMISS THE IDEA OF LIFE UPON T-

**ZPGJBAGSEBBADKP**

-HEM AS IMPOSSIBLE

My train of thought:

First I wrote in E for each of the P's. Next, I noticed after a couple PP's (which I believed to be EE) there was an I. I was not aware of any vowel that could follow that, so I decided I was likely a consonant, I={t,n,s,h,r}. I next set on figuring out what FZ was likely to be. I eliminated any of the common digrams that did not start with {t,a,o,i,n,s,h,r}, or that started with an E because I believed P=E. That left me with FZ={TH,ST,TO,NT,HA,ND,NG,TI,HI}. I noticed multiple FZP's, which would be \*\*E. The only common trigrams ending in E were ERE (impossible) and THE. So I decided F=T and Z=H. Next I decided to try and determine what E and I were. I noticed one section with the cryptotext: "QOZFFEFZP", which I had so far deduced was likely: "\*\*HTT\*THe". The middle \* being whatever E symbolized, which I had already know is one of the set {a,o,i,n,s,r} (removed known guesses). I thought it likely that the T\* was a two letter word, or at least a vowel, so I={a,o,i}<-(point of error). If a two letter word, only {o} would work. So I hypothesized I=O. This looked very strange in multiple places and I decided I had likely made a wrong turn somewhere. I then realized I meant to deduce E={a,o,i} at 'point of error'. So I meant to hypothesize E=O. I rewrote my text to reflect this and it looked MUCH better. I noticed the ciphertext starts with IEEIPY..., which I have hypothesized thus far is \*OO\*E\*\*... Ealier I stated that I={n,s,r} (again removing letters I have already guessed). I think that the only of those consonants that likely would make sense is I={n}. I am not sure yet. Next I do a frequency analysis on digrams starting with P (aka E). I see that PK, PJ, PI, and PT are the most common. The most common digrams starting with E are ER, ED, ES, EN, EA, ET. I am starting to like I=N even more. So I will do frequency analysis on digrams starting with cipherletter "E" which I believe to be O. Because, the popular digrams starting with O are ON, OU, OR, and then OF. I notice doing this that there are a couple FZEQOZF's, which I already have as THO\*\*HT. EW, EI, ET and EQ are the common digrams starting with E. So I hypothesize Q=U and O=G. I notice the probabilities are not in my favor. 0.03 Q's when usually U's are about 0.028. Anyways, back to my digrams starting with O, EW is by far the most common, however there are not that many W's, 0.02, so not likely N nor R, but could be U or F. But I already guessed Q is U. So let's go with W=F. Now for the ciphertext digrams starting with E, the common ones I have left are EI and ET. And the common digrams starting with O I have left are ON and OR. I really am liking I=N so I'm gonna go for it. This is looking real good. I see something that looks like Nineteenth in the second row and I have made previous observations that A=I would make sense. Also the only O starting digram left is T=R. Let's try and figure out what A is by doing frequency analysis on bigrams ending in N (cipherlettter I). The common bigrams ending in N are IN, AN, ON, and EN. I already know all of them but A so I deduce that J=A. Same technique on digrams that end in T to deduce that B=S probably. Now I'm rewriting the text so it looks nicer and I'm pretty sure L=Y and N=C. Also G=M. From here I was able to guess the letters left.

Problem 2)

Solution:

**ESKAGWJNSESRAVRFEKADWIHWGEKDYLVVLWDOKRGFRDAESKGKLNDWHESKEKGG**

THE DROUGHT HAD LASTED NOW FOR TEN MILLION YEARS AND THE REIGN OF THE TERR-

**LZVKVLQRGAFSRAVWDNFLDXKKDAKASKGKWDESKKTJREWGLDESKXWDELDKDEIS**

-IBLE LIZARDS HAD LONG SINCE ENDED HERE ON THE EQUATOR IN HTE CONTINENT WH-

**LXSIWJVAWDKAROZKUDWIDRFRHGLXRESKZREEVKHWGKBLFEKDXKSRAGKRXSKA**

-ICH WOULD ONE DAY BE KNOWN AS AFRICA THE BATTLE FOR EXISTENCE HAD REACHED

**RDKIXVLYRBWHHKGWXLEORDAESKPLXEWGIRFDWEOKELDFLNSE**

A NEW CLIMAX OF FEROCITY AND THE VICTOR WAS NOT YET IN SIGHT

My train of thought:

Calculating probabilities from the frequencies given, it seems like K is a good bet for E, with probability 0.14. Next I’ll try to find THE by doing frequency analysis on the two letters proceeding the cryptoletter K (=E). ESK wins by a landslide and therefore I know that E=T and S=H. Next I will try to figure out R by first looking for bigrams that end in E, then looking for bigrams that start with E. Common bigrams that end in E are HE, RE, TE and SE. Common bigrams that start with E are ER, ED, ES, EN, EA and ET. Since I already know H and T I’m hoping I can narrow down what R and possible S are. From this I think that {G,D} = {R,S}. I’m next going to look at bigrams ending in letter T. Common bigrams ending in T are ST, AT, NT, ET and IT. These frequency results make me think {D,R}={S,A}, so I will conclude that D=S probably. Their probabilities don’t align exactly (.092 vs S predicted .063) but I feel like the bigram analysis is more sturdy than the probabilities. I have gained a few other predictions from doing these bigram analyses, not confident enough to commit to them, but they are: R=A, N=G, and G=R. Actually, looking back at these bigrams I just analyzed, D=S is most likely true, same G=R. I notice now that in the text there is one portion that now spells out THETERR\*\*\*E. It looks like it says THE TERR\*\*\*E, the only letter that I think can follow TERR is A or I, likely it says TERRIBLE. Which would imply L=I, I will do frequency analysis on bigrams starting with L. Common bigrams starting with I are IN, IS, and IT. Since I believe I know S and T, I should be able to conclude L=I and hopefully also figure out what N may be. Alright, seems like it could match up. I really just don’t know any other letters but A or I that could go there, and my current hypothesis is that R=A so that wouldn’t work. I’m going to go for it. Also, this exposes a S\*I\*HT at the end of the ciphertext, I think N=G. I see B\*TTLE and I already think R=A so I’m going to go ahead and fill that in. Next going to do bigram analysis of bigrams starting with T. About now I’m thinking that I mad a mistake somewhere. The beginning of the ciphertext has ESKAGWJNSE.. Which I believed until now to be THENRO\*GHT. The only letter I can see going where the star is would be U, so J=U. However, the N doesn’t seem to fit there. So maybe A!=N. I’d like to backtrack on that one. Other ones I feel good about is K=E, E=T, S=H, L=I, Z=B, V=L, R=A. The only word that seems to fit there is drought or brought. I feel good about Z=B, so let’s try A=D, the probabilities match a little closer anyways. That is looking much better in multiple places, however now I don’t know how I feel about D=S. It seems more likely to be N…. maybe. I changed that and things are looking even better. I have also discovered a few others that look promising, such as X=C, P=V, I=W, and F=S. From here, I can likely fill in the blanks from just scanning. That one was interesting, I’m very surprised I could figure out the mistakes I made, I guess partially since I made them later on. And some of my structure was good. I was lucky. I would have been very sad to redo the whole thing. Also, when copying the ciphertext on the first line, I cut off ones of the V’s in million, so it spelled milion, and that I struggled with for a while.