**Ryan “Bob” Dean**

**CS 427 – Assignment 1**

**1.**

I ran my shift script on the string for all possible shifts, and picked out the one that was readable:

yahoo is planning on combating spam by requiring email to be authenticated the problem they claim is that there's no way of knowing who the sender really is it seems obvious to me that this wont stop spam at all spammers are already breaking into computers and hijacking legitimate users email systems spammers are already sending mail out of random countries and stolen accounts how exactly will this make things better

**2.**

a.) The values allowed for b are entirely dependent on the values of a. For example. B can be 0 if a is 1. However, b can't be 0 if a is 2, because if p is the range 0-25, ap mod 26 for p = 0 and 13 would both be 0.

b.) 26x, for obvious reasons. An a of 1 would just be a standard Caesar cipher.

c.) The values of a and the total range of characters (in this case, 26) must have no common divisors other than 1. Otherwise, they will have at least one duplicate encoding.

1, 3, 5, 7, 9 ,11, 15, 17, 19, 21, 23, 25 are the unique a values.

**3.**

if

E -> B

T -> U

then

a = 3

b = 13

**4.**

First, I counted the characters. I replaced the 2 most popular characters with E and T, realized this was wrong because there weren't nearly enough T(x)E's (the, then, than, these, etc.), so I tried the first and third most popular. At this point, I started seeing common words, and by replacing letters and making more words, I worked the rest of the message out. Handy words that helped were the first word (the characters for S and E are common, and seems is the only word that makes sense at the start of a sentence), and from there the next word would be have to be “to” or “like”, etc. Eventually I saw a word that looked like “keyboard” and the rest worked itself out from there, with a few snags with the names and such.

Translated text:

SEEMSLIKEHPWIRELESSKEYBOARDSDONTHAVEANYBUILTINAUTHENTICATIONHEREISASTORYABOUTONEPERSONSKEYBOARDTALKINGTOANOTHERPERSONSCOMPUTERTHROUGHWALLSONEHUNDREDANDFIFTYMETERSAWAYWHILEASTAVANGERMANTYPEDAWAYATHISDESKTOPCOMPUTERHISTEXTWASALSOSTREAMINGINONHISNEIGHBORSMACHINEINABUILDINGONEHUNDREDANDFIFTYMETERSAWAYHEWLETTPACKARDHAVENEVERRECEIVEDACOMPLAINTLIKEITPERERIKHELLEGOTAJOLTWHENHISHOMECOMPUTERSUDDENLYSEEMEDTODEVELOPALIFEOFITSOWNABOUTTENPMIWASSITTINGANDWATCHINGTVWHENTHECOMPUTERWHICHWASINSLEEPMODESUDDENLYBEGANTOBUllILOOKEDOVERANDNOTICEDITWASWAKINGUPIALSOSAWAREDLIGHTONTHEEYBOARDSRECEIVERBOXBLINKINGASIFIWASWRITINGSOMETHINGHELLESAIDAGAMEWHICHHECOULDNOTREMEMBERUSINGTHATDAYAPPEAREDONTHESCREENWHENHELLEWENTOVERTOSHUTITOFFTHESCREENDISPLAYEDAMESSAGEASKINGHIMIFHEREALLYWANTEDTODELETETHISFILENOTKNOWINGWHATITMEANTHEANSWEREDNOTOPLAYITSAFETHEMACHINEWASNOTFINISHEDASERIESOFBEEPSANDCLICKSTHATHINTEDATERRORMESSAGESCAMESOQUICKLYTHATHELLEAGAINGOTTHEIMPRESSIONSOMEONEWASWRITINGSOHETURNEDONHISWORDPROCESSORHESAWTEXTTICKINGINLIVEANDCOULDTELLFROMTHEMESSAGETHATITWASHISNEIGHBORPERARILDEVJEBERGALSOHISBOSSATSTAVANGERAFTENBLADWHOWASWRITINGAPHONECALLQUICKLYCONFIRMEDTHATHELLEWASWATCHINGEVJEBERGTYPELIVEIFHPCANTFINDADECENTEXPLANATIONFORTHISIDONTDAREUSETHISKEYBOARDICHANGEDTHESIGNALCHANNELANDNOWPERERIKDOESNTGETITBUTNOWIDONTKNOWWHOMIGHTBEREADINGWHATIWRITEASIWRITEITEVJEBERGSAIDEVJEBERGANDHELLEHADRECEIVEDNEWHPMACHINESFROMTHESAMECOMPANYANDHELLEHADONETIMEEEARLIERNOTICEDAREGISTRATIONFORMAPPEARWITHHISNEIGHBORSINFORMATIONINITHPPRODUCTMANAGERTOREASRELINDBELIEVESTHATONLYACOMBINATIONOFUNUSUALCIRCUMSTANCESCOULDRESULTINTHEKEYBOARDSIGNALTRAVELINGONEHUNDREDANDFITFYMETERSANDTHROUGHONEWOODENANDONECONCRETEWALLWITHTHECONDITIONSANDDISTANCEDESCRIBEDWEHAVENOLOGICALORTECHNICALEXPLANATIONFORHOWTHISISPOSSIBLETHEKEYBOARDSHOULDHAVEATHEORETICALRADIUSOFABOUTTWENTYMETERSASSUMINGACLEARPATHFROMKEYBOARDTORECEIVER

the letters 'z' doesn't seem to show up, even though there are 26 unique characters in the encoding, leading me to believe I made a small mistake somewhere here. I'm guessing “PERERIK HELLE” and “EVJEBERG” are names, and that “STAVANGER” is a typo.

I don't have a key since I translated it on the fly, but I do know I started with h = e (most frequest), o = a (second most frequent), b = t (third most frequent), and q = s (deduction), and so forth.

**5.**

Using a script I found a common set of characters “sphy” that showed up fairly frequently. The occurrences were 638 , 56 , 147 , 161 , 49 , 462 , 560 characters apart, respectively. Most of these are divisible by 7, so that's a good guess as to the key length. From there, I separated the string into 7 substrings, and replaced and shifted characters until something readable came out.

The key is SCHNEIE

The translated text is:

MAGINETHISSITUATIONANENGINEERBUILDSABRIDGEITSTANDSFORADAYANDTHENCOLLAPSESHEBUILDSANOTHERITSTANDSFORTHREEDAYSANDTHENCOLLAPSESTHENHBUILDSATHIRDWHICHSTANDSFORTWOWEEKSBUTCOLLAPSESDURINGTHEFIRSTRAINSTORMSOHEBUILDSAFOURTHITSBEENSTANDINGFORAMONTHANDHASSURVIVEDTWORAINSTORMSDOYOUBELIEVETHISFOURTHBRIDGEISSTRONGSECUREANDSAFEORISITMORELIKELYJUSTANOTHERACCIDENTWAITINGTOHAPPENASBIZARREASITMAYSEEMTHISKINDOFDESIGNPROCESSHAPPENSALLTHETIMEINCRYPTOGRAPHYAFIELDTHATISFULLOFPEOPLEWHOLOVETODESIGNTHEIROWNALGORITHWIANDPROTOCOLSWITHSOMANYASPIRINGCRYPTANALYSTSOUTTHEREHOWEVERTHERESBOUNDTOBEALOTOFWEAKDESIGNSTHEPROBLEMISTHISANYONENOMATTERHOWUNSKILLEDCANDESIGNANALGORITHMTHATHEHIMSELFCANNOTBREAKTHOUGHACOMPETENTCRYPTANALYSTCANBREAKMOSTOFTHISSTUFFAFTERASHORTREVIEWTHERESTOFITSURVIVESANDINMOSTCASESISNEVERLOOKEDATAGAINESPECIALLYOUTSIDETHEMILITARYWORLDBUTJUSTBECAUSEANALGORITHMSURVIVESANINITIALREVIEWISNOREASONTOTRUSTITIHADACLIENTONCEWHODESPERATELYWANTEDTODESIGNHISOWNENCRYPTIONALGORITHMHEHADNOCRYPTOGRAPHICTRAININGNOEXPERIENCEANALYZINGOTHERALGORITHMSHEWASADESIGNERHESAIDNOTANANALYSTSOCOUNTERPANEDIDHISANALYSISFORHIMANDWEBROKEHISALGORITHMINADAYHEFIXEDITANDSENTITBACKANDWEBROKEITINTWODAYSHEFIXEDITANDSENTITBACKAGAINANDWEBROKEITAGAINFINALLYTHEFOURTHVERSIONOFHISALGORITHMRESISTEDOURATTEMPTSATCRYPTANALYSISATLEASTFORFOURTYHOURSBUTTHATDOESNTMEANTHATITSNOTSTILLFLAWEDORTHATITCANTBEBROKENGIVENENOUGHTIMEANDRESOURCESUNFORTUNATELYINTHEWORLDOFCRYPTOGRAPHYDIFFERENTISBADCRYPTOGRAPHYISATITSBESTWHENITISCONSERVATIVEANDTHECONSERVATIVEAPPROACHISTOCHOOSEANALGORITHMTHATHASTHATHASALREADYBEENANALYZEDTHEADMONITIONNOTTOPUTALLYOUREGGSINONEBASKETDOESNOTAPPLYINTHISCASETHESECURITYOFASYSTEMISTHESECURITYOFITSWEAKESTCOMPONENTSINCETHEWEAKESTCOMPONENTBREAKSTHEENTIRESYSTEMINCRYPTOGRAPHYTHEREISSECURITYINFOLLOWINGTHECROWDAHOMEGROWNALGORITHMCANTPOSSIBLYBESUBJECTEDTOTHEHUNDREDSOFTHOUSANDSOFHOURSOFANALYSISTHATDESANDTRIPLEDESHAVEBEENSUBJECTEDTOACOMPANYJUSTCANTMOBILIZETHERESOURCESTHATAREBEINGBROUGHTTOBEARAGAINSTTHEAESCANDIDATESORTHEIPSECINTERNETSECURITYPROTOCOLNOONECANDUPLICATETHECONFIDENCETHATRSAOFFERSAFTRTWENTYYEARSOFCRYPTANALYTICREVIEWASTANDARDSECURITYREVIEWEVENBYCOMPETENTCRYPTOGRAPHERSCANONLYPROVEINSECURITYITCANNEVERPROVESECURITYBYFOLLOWINGTHEPACKYOUCANLEVERAGETHECRYPTANALYTICEXPERTISEOFTHEWORLDWIDECOMMUNITYNOTJUSTAHANDFULOFHOURSOFACONSULTANTSTIMETHISARTICLEORIGINALLYAPPEAREDININFORMATIONSECURITYMAGAZINE