PROJECT 1

CRYPTANALYSIS

JEFFREY ADAM FERMON

AND

CHRISTIAN SOTO

ECE571

FUNDAMENTALS OF INFORMATION AND NETWORK SECURITY

SPRING 2018

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

UNIVERSITY OF ARIZONA

**- INTRO -**

Cryptanalysis is the art of deciphering communications and systems, which are secured by cryptography (3). Cryptanalysts are those who hack secret codes and read encrypted messages. They are often called code breakers, or simply put, hackers. In this report, we present our results of a recent cryptanalysis on four different cipher texts. The cipher text files were given, and though the messages were quite long, it ultimately eased the difficulty in cracking the messages. For each cipher text message given, we found the type of encryption used, as well as the key and the plain texts. Interestingly, we could not decrypt one of the cipher texts; a detailed explanation is also highlighted in this report. Lastly, we describe the techniques and functions used to decrypt the messages. Several statistical analysis methods were used and eventually implemented into our code. The cipher-cracking program was written in python.

**- SHIFT CIPHER -**

The Shift cipher is also known as the Caesar cipher. The earliest known, and simplest substation cipher (1). It basically replaces each letter of the alphabet with the letter standing a number of places further down the alphabet. This number is the ‘key’. The equations for a shift cipher encryption and decryptions, as described in Stallings book is as follows:

Some of the pros and cons of using the shift cipher is that it is very easy to use, yet the encrypted text has only 26 possibilities. The key could be obtained through trial and error, a method called the Brute Force Attack. One way to solve the cipher is to use the frequency of the letters in the alphabet (2).

For our analysis, we found that cipher1.txt was encrypted using shift cipher techniques. Our results revealed the key to be ‘13’.

**- SUBSTITUTION CIPHER -**

For a general simple substitution cipher, a random letter is chosen to encrypt each letter of the alphabet. Each letter is used once, therefore, the key always ends up being a string of 26 random letters. The advantage of using this type of substitution cipher is that it produces far more possible keys, 4 x 10^26 keys. The disadvantage however, is that the cipher ends up being easy enough to compare the cipher text to words in a dictionary file implemented in the code, to slowly figure out which cipher letters decrypt to which letters (2). Basically, language characteristics become the problem. As we find out in our section of frequency analysis, the letter ‘e’ is the most commonly used letter in the normal English language. In contrast, letters ‘z’, ‘j’, ‘k’, ‘q’ and ‘x’ are rare. One can then construct tables of single, double and triple letter frequencies, or diagrams,

In a substitution cipher, a plaintext word and its cipher word will always have the same word pattern, no matter which simple substitution key was used to do the encryption. A logical algorithm to use in order to crack a simple substitution starts out with a cipher letter-mapping tool. This is the main tool for modeling the possible letters that each cipher text letter can decrypt to (2). Based on the candidates for each cipher word, when letters are added to the mapping, and then intersecting mapping and removing solved letters from other lists of potential decryption letters, one can narrow down the number of possible keys (2). A python code could then be used to figure out exactly what the original simple substation key was.

In our analysis, we found that cipher2.txt used substitute cipher encryption with key ZMAYTXLPRSBWEFQCIUDGH.

**- VIGENERE CIPHER -**

The Vigenere cipher, is the simplest polyalphabetic substitution cipher (1). It is similar to the Caesar cipher, except with multiple keys. It uses more than one set of substitutions, hence the name “polyalphabetic substitution (2). The cipher uses a letter key, instead of a numeric key. The letter A is denoted with key 0, B with 1, C with 2 and so on up until letter Z which uses numeric key 25. According to Stallings (1), a general equation of the encryption process for this cipher is:

And for the decryption, the process simply works in reverse. The equation is

The key in a Vigenere cipher is a series of letters, such as a single English word. This single word key will be split into multiple sub-keys. The more letters are used in this cipher, the stronger the encrypted message will be, especially against a brute-force attack. In our analysis, we found that cipher3.txt was encrypted using this technique. The key we found was “TUCSON”. Even though the cipher text is quite large, the fact that the key is relatively short; ‘TUCSON’ is a poor choice for a Vigenere key. A key with 6 letters has 308,915,776 possible combinations. This is a large number for a human to crack, but it can easily be done by computer force. To crack the cipher, frequency analysis was used.

**- PERMUTATION CIPHER -**

Permutation cipher, or columnar transposition, instead of replacing letter with other letters, the cipher mixes up the message into an order that makes the plain text unreadable. This cipher is far more secure than a simple shift or substation cipher. In our analysis we found that none of the cipher.txt files were encrypted using this technique. We were able to reach this conclusion because our FrequencyAnalyzer class failed to return a high enough letter frequency similarity score for any of the cipher texts provided. Since the letters in a permutation cipher aren’t replaced, we expect to see a strong correlation between the most and least frequent letters in the cipher to English.

**- ONE-TIME PAD -**

The hardest cipher to break, it is basically impossible to crack such cipher. The scheme of a one-time pad is such that it is unbreakable (1). It produces random output that bears no statistical relationship to the plaintext (1). This cipher is very secure because it uses a truly random key that is in equal length as the original message that is being used. For these two reasons, the one-time pad cipher is basically a Vigenere cipher (2) that uses the key one time only.

After doing our analysis of all four given cipher.txt files, we concluded that cipher4.txt must be encrypted using the one-time pad algorithm.

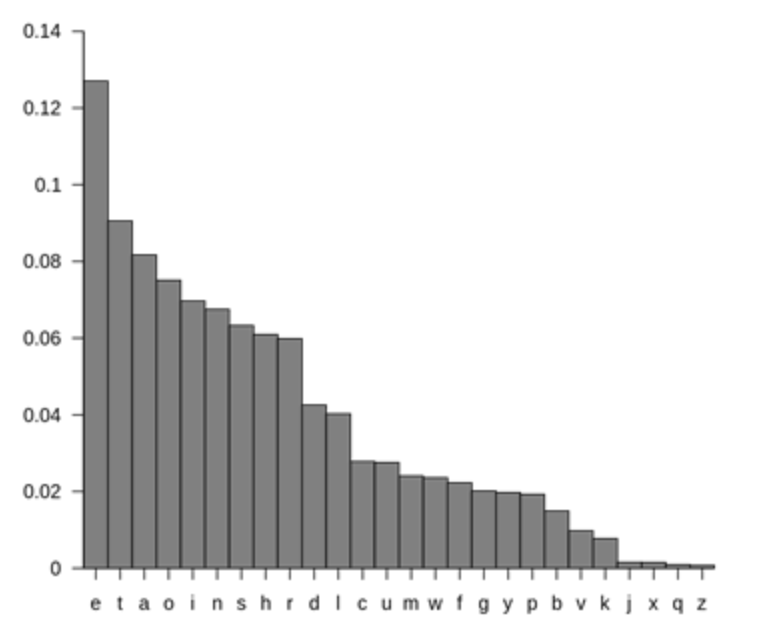
FREQENCY ANALYSIS

For our analysis we created a FrequencyAnalyzer class that calculate various statistics about the cipher texts:

* Single letter frequency
* Bigram frequency
* Trigram frequency
* Single letter frequency percent difference – a one to one comparison of percentage difference of frequency distribution for each letter’s frequency distribution in the ciphertext to it’s rank partner in English (e.g. percentage difference between the frequency of the most frequent letter in the cipher text to the frequency of the most frequent letter in English, and so on for each individual letter)
* Bigram frequency percent difference – The same as single letter frequency percent difference except for bigrams
* Trigram frequency percent difference – The same as single letter frequency percent difference except for trigrams
* Single letter frequency match – a percentage for how closely the frequencies of the 6 most common letters in the cipher text match the frequencies of the 6 most common letters in English (1000% is perfect match)
* Bigram Frequency match - The same as single letter frequency match except for bigrams
* Trigram Frequency match – The same as single letter frequency match except for trigrams
* Cypher Frequency Match To English – a percentage for how closely the 6 most/least common letters in the cipher text match the 6 most/least common letters in English

This class was useful in not only determining the type of cipher, but if a decrypted text was properly decrypted.

Figure 1 Letter frequency of normal English, sorted. (2)



First we used the FrequencyAnalysis class to determine what the most likely type was for each cypher text.

The criteria we used for each cypher was as follows:

* Permutation - A single letter frequency match score over 90%, and a frequency match to English score of the cyphertext over 80%.
* Shift - A single letter frequency match score over 90% of the cyphertext, and a frequency match to English score over 80% for a single brute force decryption of the text.
* Substitution - A single letter frequency match score over 90% of the cypher text, and frequency match to English score of the cyphertext under 80%, and no frequency match to English score over 80% for a single brute force shift decryption of the text.
* Vigenere - A single letter frequency match score under 90%, frequency match to English score over 80% for the most likely decryption of the text (See Vigenere Algorithm section for explanation)
* One-Time Pad – A failure to meet the criteria of all other types.

DECRYPTION ALGORITHMS

Permutation

No texts were found to meet the frequency analysis criteria outlined above so no algorithm was created.

Shift

To determine a decryption for a shift cipher we used a mixture of brute-force and frequency analysis. First all 26 shifts of the text were completed and analyzed for a letter frequency match to English. Any key with a percentage match of the 6 most/least frequent letters in English over 85% was then placed into a list and sorted from greatest to least. The most likely, or highest percentage match key and decryption was then presented as the solution along with a confidence score based on how close frequency score was to English as well as the percentage difference between that score and the next closest is there was another solution over 85%.

Vigenere

The Vigenere cypher was solved by first finding the most likely key length and using that to break the cyphertext into that many individual shift cyphers. This was done by first determining the most common repeating 3-5 letter sequences in the cyphertext, logging the distance between successive occurrences, sorting them from most to least frequent and removing any sequences with less than 3 occurrences. Once sorted, the common divisors of the distances between each individual sequence occurrence were calculated and tallied to give us a frequency distribution for the most common divisors of all repeating sequence distances. The tallies were then sorted from greatest to least and all tallies less than 50% (if a divisor occurred less than half as much as the most common divisor, it was removed from the list)

The list of divisors was then sorted from largest divisor to smallest. After receiving the list of divisors, they are then used as possible key lengths to solve the cypher.

For each key length, the cypher text is broken up into a number of shift ciphers matching the key length (i.e. if the key length is 3 for a cypher text ABCABCABC, then 3 shift ciphers are created containing every 3rd letter: AAA, BBB, and CCC). Now that the result is just a number of shift cyphers, a brute force attack was performed on each cipher and the FrequencyAnalyzer class was then used on each individual shift to determine the single letter frequency match to English. The closest match to English for each cypher was saved as the most likely key. Once all of the most likely keys were found for each cypher, the entire text was decrypted and analyzed for its frequency similarity to English as the other decrypted texts were. If the similarity was over 85%, it was presented as solution and the user was queried for response. If the user responded that the text was not correctly decrypted, the program continued on to the next most likely letters until another decrypted text exceeded the criteria for a possible solution.

Substitution

This cipher required the most user interaction. The FrequencyAnalyzer was used to determine the most frequent letters, bigrams, and trigrams for a cypher text. The application then determined a letter mapping for each letter to its key letter by comparing it to the English frequencies for single letters, bigrams, and trigrams. This was done by mapping each letter to its corresponding decrypted value based on single letter frequencies first (i.e. first most common letter was decrypted as E, second was T and so on). Next the 6 most frequent bigrams and trigrams were analyzed to determine the number of times that each letter appeared mapped to a certain letter. For instance, if the most common bigram in the text was JW, that mapped to the most common bigram in English of HE, so each J received a vote for being the encryption of H and W received a voted for being the encryption of E. By tallying the votes foe the bigram and trigram comparisons and merging them with the single letter frequency mappings, we received an initial mapping of the cypher letters to their decryption. The user was then presented with the mapping and a sample of the text decrypted using the key. The user could then enter input to change the mappings. This process ended up taking a lot of trial and error, but the text was eventually solved.

DECRYPTION RESULTS

CIPHER1

ENCRYPTION: Shift Cipher

CIPHERTEXT: see cipher1.txt

KEY: **13**

PLAINTEXT: (first 5 lines) LET ME BEGIN BY SAYING THANKS TO ALL YOU WHOVE TRAVELED FROM FAR AND WIDE TO BRAVE THE COLD TODAY WE ALL MADE THIS JOURNEY FOR A REASON IT SHUMBLING BUT IN MY HEART I KNOW YOU DIDN’T COME HERE JUST FOR ME YOU CAME HERE BECAUSE YOU BELIEVE IN WHAT THIS COUNTRY CAN BE IN THE FACE OF WAR YOU BELIEVE THERE CAN BE PEACE IN THE FACE OF DESPAIR YOU BELIEVE THERE CAN BE HOPE IN THE FACE OF A POLITICS THAT’S SHUT YOU OUT THAT’S TOLD YOU TO SETTLE THAT’S DIVIDED US FOR TOO LONG YOU BELIEVE WE CAN BE ONE PEOPLE REACHING FOR WHATS POSSIBLE BUILDING THAT MORE PERFECT UNION T…..

CIPHER2

ENCRYPTION: Substitution Cipher

CIPHERTEXT: see cipher2.txt

KEY: **ZMAYTXLPRSBWEFQCIUDGHJKNOV**

PLAINTEXT: “We the people of the United Stat..” (First 26 letters).

WETHEPEOPLEOFTHEUNITEDSTATESINORDERTOFORMAMOREPERFECTUNIONESTABLISHJUSTICEINSUREDOMESTICTRANQUILITYPROVIDEFORTHECOMMONDEFENCEPROMOTETHEGENERALWELFAREANDSECURETHEBLESSINGSOFLIBERTYTOOURSELVESANDOURPOSTERITYDOORDAINANDESTABLISHTHISCONSTITUTIONFORTHEUNITEDSTATESOFAMERICAARTICLEISECTIONALLLEGISLATIVEPOWERSHEREINGRANTEDSHALLBEVESTEDINACONGRESSOFTHEUNITEDSTATESWHICHSHALLCONSISTOFASENATEANDHOUSEOFREPRESENTATIVESSECTIONTHEHOUSEOFREPRESENTATIVESSHALLBECOMPOSEDOFMEMBERSCHOSENEVERYSECONDYEARBYTHEPEOPLEOFTHESEVERALSTATESANDTHEELECTORSINEACHSTATESHALLHAVETHEQUALIFICATIONSREQUISITEFORELECTORSOFTHEMOSTNUMEROUSBRANCHOFTHESTATELEGISLATURENOPERSONSHALLBEAREPRESENTATIVEWHOSHALLNOTHAVEATTAINEDTOTHEAGEOFTWENTYFIVEYEARSANDBEENSEVENYEARSACITIZENOFTHEUNITEDSTATESANDWHOSHALLNOTWHENELECTEDBEANINHABITANTOFTHATSTATEINWHICHHESHALLBECHOSENREPRESENTATIVESANDDIRECTTAXESSHALLBEAPPORTIONEDAMONGTHESEVERALSTATESWHICHMAYBEINCLUDEDWITHINTHISUNIONACCORDINGTOTHEIRRESPECTIVENUMBERSWHICHSHALLBEDETERMINEDBYADDINGTOTHEWHOLENUMBEROFFREEPERSONSINCLUDINGTHOSEBOUNDTOSERVICEFORATERMOFYEARSANDEXCLUDINGINDIANSNOTTAXEDTHREEFIFTHSOFALLOTHERPERSONSTHEACTUALENUMERATIONSHALLBEMADEWITHINTHREEYEARSAFTERTHEFIRSTMEETINGOFTHECONGRESSOFTHEUNITEDSTATESANDWITHINEVERYSUBSEQUENTTERMOFTENYEARSINSUCHMANNERASTHEYSHALLBYLAWDIRECTTHENUMBEROFREPRESENTATIVESSHALLNOTEXCEEDONEFOREVERYTHIRTYTHOUSANDBUTEACHSTATESHALLHAVEATLEASTONEREPRESENTATIVEANDUNTILSUCHENUMERATIONSHALLBEMADETHESTATEOFNEWHAMPSHIRESHALLBEENTITLEDTOCHOOSETHREEMASSACHUSETTSEIGHTRHODEISLANDANDPROVIDENCEPLANTATIONSONECONNECTICUTFIVENEWYORKSIXNEWJERSEYFOURPENNSYLVANIAEIGHTDELAWAREONEMARYLANDSIXVIRGINIATENNORTHCAROLINAFIVESOUTHCAROLINAFIVEANDGEORGIATHREEWHENVACANCIESHAPPENINTHEREPRESENTATIONFROMANYSTATETHEEXECUTIVEAUTHORITYTHEREOFSHALLISSUEWRITSOFELECTIONTOFILLSUCHVACANCIESTHEHOUSEOFREPRESENTATIVESSHALLCHOOSETHEIRSPEAKERANDOTHEROFFICERSANDSHALLHAVETHESOLEPOWEROFIMPEACHMENTSECTIONTHESENATEOFTHEUNITEDSTATESSHALLBECOMPOSEDOFTWOSENATORSFROMEACHSTATECHOSENBYTHELEGISLATURETHEREOFFORSIXYEARSANDEACHSENATORSHALLHAVEONEVOTEIMMEDIATELYAFTERTHEYSHALLBEASSEMBLEDINCONSEQUENCEOFTHEFIRSTELECTIONTHEYSHALLBEDIVIDEDASEQUALLYASMAYBEINTOTHREECLASSESTHESEATSOFTHESENATORSOFTHEFIRSTCLASSSHALLBEVACATEDATTHEEXPIRATIONOFTHESECONDYEAROFTHESECONDCLASSATTHEEXPIRATIONOFTHEFOURTHYEARANDOFTHETHIRDCLASSATTHEEXPIRATIONOFTHESIXTHYEARSOTHATONETHIRDMAYBECHOSENEVERYSECONDYEARANDIFVACANCIESHAPPENBYRESIGNATIONOROTHERWISEDURINGTHERECESSOFTHELEGISLATUREOFANYSTATETHEEXECUTIVETHEREOFMAYMAKETEMPORARYAPPOINTMENTSUNTILTHENEXTMEETINGOFTHELEGISLATUREWHICHSHALLTHENFILLSUCHVACANCIESNOPERSONSHALLBEASENATORWHOSHALLNOTHAVEATTAINEDTOTHEAGEOFTHIRTYYEARSANDBEENNINEYEARSACITIZENOFTHEUNITEDSTATESANDWHOSHALLNOTWHENELECTEDBEANINHABITANTOFTHATSTATEFORWHICHHESHALLBECHOSENTHEVICEPRESIDENTOFTHEUNITEDSTATESSHALLBEPRESIDENTOFTHESENATEBUTSHALLHAVENOVOTEUNLESSTHEYBEEQUALLYDIVIDEDTHESENATESHALLCHOOSETHEIROTHEROFFICERSANDALSOAPRESIDENTPROTEMPOREINTHEABSENCEOFTHEVICEPRESIDENTORWHENHESHALLEXERCISETHEOFFICEOFPRESIDENTOFTHEUNITEDSTATESTHESENATESHALLHAVETHESOLEPOWERTOTRYALLIMPEACHMENTSWHENSITTINGFORTHATPURPOSETHEYSHALLBEONOATHORAFFIRMATIONWHENTHEPRESIDENTOFTHEUNITEDSTATESISTRIEDTHECHIEFJUSTICESHALLPRESIDEANDNOPERSONSHALLBECONVICTEDWITHOUTTHECONCURRENCEOFTWOTHIRDSOFTHEMEMBERSPRESENTJUDGMENTINCASESOFIMPEACHMENTSHALLNOTEXTENDFURTHERTHANTOREMOVALFROMOFFICEANDDISQUALIFICATIONTOHOLDANDENJOYANYOFFICEOFHONORTRUSTORPROFITUNDERTHEUNITEDSTATESBUTTHEPARTYCONVICTEDSHALLNEVERTHELESSBELIABLEANDSUBJECTTOINDICTMENTTRIALJUDGMENTANDPUNISHMENTACCORDINGTOLAWSECTIONTHETIMESPLACESANDMANNEROFHOLDINGELECTIONSFORSENATORSANDREPRESENTATIVESSHALLBEPRESCRIBEDINEACHSTATEBYTHELEGISLATURETHEREOFBUTTHECONGRESSMAYATANYTIMEBYLAWMAKEORALTERSUCHREGULATIONSEXCEPTASTOTHEPLACEOFCHOOSINGSENATORSTHECONGRESSSHALLASSEMBLEATLEASTONCEINEVERYYEARANDSUCHMEETINGSHALLBEONTHEFIRSTMONDAYINDECEMBERUNLESSTHEYSHALLBYLAWAPPOINTADIFFERENTDAYSECTIONEACHHOUSESHALLBETHEJUDGEOFTHEELECTIONSRETURNSANDQUALIFICATIONSOFITSOWNMEMBERSANDAMAJORITYOFEACHSHALLCONSTITUTEAQUORUMTODOBUSINESSBUTASMALLERNUMBERMAYADJOURNFROMDAYTODAYANDMAYBEAUTHORIZEDTOCOMPELTHEATTENDANCEOFABSENTMEMBERSINSUCHMANNERANDUNDERSUCHPENALTIESASEACHHOUSEMAYPROVIDEEACHHOUSEMAYDETERMINETHERULESOFITSPROCEEDINGSPUNISHITSMEMBERSFORDISORDERLYBEHAVIORANDWITHTHECONCURRENCEOFTWOTHIRDSEXPELAMEMBEREACHHOUSESHALLKEEPAJOURNALOFITSPROCEEDINGSANDFROMTIMETOTIMEPUBLISHTHESAMEEXCEPTINGSUCHPARTSASMAYINTHEIRJUDGMENTREQUIRESECRECYANDTHEYEASANDNAYSOFTHEMEMBERSOFEITHERHOUSEONANYQUESTIONSHALLATTHEDESIREOFONEFIFTHOFTHOSEPRESENTBEENTEREDONTHEJOURNALNEITHERHOUSEDURINGTHESESSIONOFCONGRESSSHALLWITHOUTTHECONSENTOFTHEOTHERADJOURNFORMORETHANTHREEDAYSNORTOANYOTHERPLACETHANTHATINWHICHTHETWOHOUSESSHALLBESITTINGSECTIONTHESENATORSANDREPRESENTATIVESSHALLRECEIVEACOMPENSATIONFORTHEIRSERVICESTOBEASCERTAINEDBYLAWANDPAIDOUTOFTHETREASURYOFTHEUNITEDSTATESTHEYSHALLINALLCASESEXCEPTTREASONFELONYANDBREACHOFTHEPEACEBEPRIVILEGEDFROMARRESTDURINGTHEIRATTENDANCEATTHESESSIONOFTHEIRRESPECTIVEHOUSESANDINGOINGTOANDRETURNINGFROMTHESAMEANDFORANYSPEECHORDEBATEINEITHERHOUSETHEYSHALLNOTBEQUESTIONEDINANYOTHERPLACENOSENATORORREPRESENTATIVESHALLDURINGTHETIMEFORWHICHHEWASELECTEDBEAPPOINTEDTOANYCIVILOFFICEUNDERTHEAUTHORITYOFTHEUNITEDSTATESWHICHSHALLHAVEBEENCREATEDORTHEEMOLUMENTSWHEREOFSHALLHAVEBEENINCREASEDDURINGSUCHTIMEANDNOPERSONHOLDINGANYOFFICEUNDERTHEUNITEDSTATESSHALLBEAMEMBEROFEITHERHOUSEDURINGHISCONTINUANCEINOFFICESECTIONALLBILLSFORRAISINGREVENUESHALLORIGINATEINTHEHOUSEOFREPRESENTATIVESBUTTHESENATEMAYPROPOSEORCONCURWITHAMENDMENTSASONOTHERBILLSEVERYBILLWHICHSHALLHAVEPASSEDTHEHOUSEOFREPRESENTATIVESANDTHESENATESHALLBEFOREITBECOMEALAWBEPRESENTEDTOTHEPRESIDENTOFTHEUNITEDSTATESIFHEAPPROVEHESHALLSIGNITBUTIFNOTHESHALLRETURNITWITHHISOBJECTIONSTOTHATHOUSEINWHICHITSHALLHAVEORIGINATEDWHOSHALLENTERTHEOBJECTIONSATLARGEONTHEIRJOURNALANDPROCEEDTORECONSIDERITIFAFTERSUCHRECONSIDERATIONTWOTHIRDSOFTHATHOUSESHALLAGREETOPASSTHEBILLITSHALLBESENTTOGETHERWITHTHEOBJECTIONSTOTHEOTHERHOUSEBYWHICHITSHALLLIKEWISEBERECONSIDEREDANDIFAPPROVEDBYTWOTHIRDSOFTHATHOUSEITSHALLBECOMEALAWBUTINALLSUCHCASESTHEVOTESOFBOTHHOUSESSHALLBEDETERMINEDBYYEASANDNAYSANDTHENAMESOFTHEPERSONSVOTINGFORANDAGAINSTTHEBILLSHALLBEENTEREDONTHEJOURNALOFEACHHOUSERESPECTIVELYIFANYBILLSHALLNOTBERETURNEDBYTHEPRESIDENTWITHINTENDAYSSUNDAYSEXCEPTEDAFTERITSHALLHAVEBEENPRESENTEDTOHIMTHESAMESHALLBEALAWINLIKEMANNERASIFHEHADSIGNEDITUNLESSTHECONGRESSBYTHEIRADJOURNMENTPREVENTITSRETURNINWHICHCASEITSHALLNOTBEALAWEVERYORDERRESOLUTIONORVOTETOWHICHTHECONCURRENCEOFTHESENATEANDHOUSEOFREPRESENTATIVESMAYBENECESSARYEXCEPTONAQUESTIONOFADJOURNMENTSHALLBEPRESENTEDTOTHEPRESIDENTOFTHEUNITEDSTATESANDBEFORETHESAMESHALLTAKEEFFECTSHALLBEAPPROVEDBYHIMORBEINGDISAPPROVEDBYHIMSHALLBEREPASSEDBYTWOTHIRDSOFTHESENATEANDHOUSEOFREPRESENTATIVESACCORDINGTOTHERULESANDLIMITATIONSPRESCRIBEDINTHECASEOFABILLSECTIONTHECONGRESSSHALLHAVEPOWERTOLAYANDCOLLECTTAXESDUTIESIMPOSTSANDEXCISESTOPAYTHEDEBTSANDPROVIDEFORTHECOMMONDEFENCEANDGENERALWELFAREOFTHEUNITEDSTATESBUTALLDUTIESIMPOSTSANDEXCISESSHALLBEUNIFORMTHROUGHOUTTHEUNITEDSTATESTOBORROWMONEYONTHECREDITOFTHEUNITEDSTATESTOREGULATECOMMERCEWITHFOREIGNNATIONSANDAMONGTHESEVERALSTATESANDWITHTHEINDIANTRIBESTOESTABLISHANUNIFORMRULEOFNATURALIZATIONANDUNIFORMLAWSONTHESUBJECTOFBANKRUPTCIESTHROUGHOUTTHEUNITEDSTATESTOCOINMONEYREGULATETHEVALUETHEREOFANDOFFOREIGNCOINANDFIXTHESTANDARDOFWEIGHTSANDMEASURESTOPROVIDEFORTHEPUNISHMENTOFCOUNTERFEITINGTHESECURITIESANDCURRENTCOINOFTHEUNITEDSTATESTOESTABLISHPOSTOFFICESANDPOSTROADSTOPROMOTETHEPROGRESSOFSCIENCEANDUSEFULARTSBYSECURINGFORLIMITEDTIMESTOAUTHORSANDINVENTORSTHEEXCLUSIVERIGHTTOTHEIRRESPECTIVEWRITINGSANDDISCOVERIESTOCONSTITUTETRIBUNALSINFERIORTOTHESUPREMECOURTTODEFINEANDPUNISHPIRACIESANDFELONIESCOMMITTEDONTHEHIGHSEASANDOFFENSESAGAINSTTHELAWOFNATIONSTODECLAREWARGRANTLETTERSOFMARQUEANDREPRISALANDMAKERULESCONCERNINGCAPTURESONLANDANDWATERTORAISEANDSUPPORTARMIESBUTNOAPPROPRIATIONOFMONEYTOTHATUSESHALLBEFORALONGERTERMTHANTWOYEARSTOPROVIDEANDMAINTAINANAVYTOMAKERULESFORTHEGOVERNMENTANDREGULATIONOFTHELANDANDNAVALFORCESTOPROVIDEFORCALLINGFORTHTHEMILITIATOEXECUTETHELAWSOFTHEUNIONSUPPRESSINSURRECTIONSANDREPELINVASIONSTOPROVIDEFORORGANIZINGARMINGANDDISCIPLININGTHEMILITIAANDFORGOVERNINGSUCHPARTOFTHEMASMAYBEEMPLOYEDINTHESERVICEOFTHEUNITEDSTATESRESERVINGTOTHESTATESRESPECTIVELYTHEAPPOINTMENTOFTHEOFFICERSANDTHEAUTHORITYOFTRAININGTHEMILITIAACCORDINGTOTHEDISCIPLINEPRESCRIBEDBYCONGRESSTOEXERCISEEXCLUSIVELEGISLATIONINALLCASESWHATSOEVEROVERSUCHDISTRICTNOTEXCEEDINGTENMILESSQUAREASMAYBYCESSIONOFPARTICULARSTATESANDTHEACCEPTANCEOFCONGRESSBECOMETHESEATOFTHEGOVERNMENTOFTHEUNITEDSTATESANDTOEXERCISELIKEAUTHORITYOVERALLPLACESPURCHASEDBYTHECONSENTOFTHELEGISLATUREOFTHESTATEINWHICHTHESAMESHALLBEFORTHEERECTIONOFFORTSMAGAZINESARSENALSDOCKYARDSANDOTHERNEEDFULBUILDINGSANDTOMAKEALLLAWSWHICHSHALLBENECESSARYANDPROPERFORCARRYINGINTOEXECUTIONTHEFOREGOINGPOWERSANDALLOTHERPOWERSVESTEDBYTHISCONSTITUTIONINTHEGOVERNMENTOFTHEUNITEDSTATESORINANYDEPARTMENTOROFFICERTHEREOFSECTIONTHEMIGRATIONORIMPORTATIONOFSUCHPERSONSASANYOFTHESTATESNOWEXISTINGSHALLTHINKPROPERTOADMITSHALLNOTBEPROHIBITEDBYTHECONGRESSPRIORTOTHEYEARONETHOUSANDEIGHTHUNDREDANDEIGHTBUTATAXORDUTYMAYBEIMPOSEDONSUCHIMPORTATIONNOTEXCEEDINGTENDOLLARSFOREACHPERSONTHEPRIVILEGEOFTHEWRITOFHABEASCORPUSSHALLNOTBESUSPENDEDUNLESSWHENINCASESOFREBELLIONORINVASIONTHEPUBLICSAFETYMAYREQUIREITNOBILLOFATTAINDEROREXPOSTFACTOLAWSHALLBEPASSEDNOCAPITATIONOROTHERDIRECTTAXSHALLBELAIDUNLESSINPROPORTIONTOTHECENSUSORENUMERATIONHEREINBEFOREDIRECTEDTOBETAKENNOTAXORDUTYSHALLBELAIDONARTICLESEXPORTEDFROMANYSTATENOPREFERENCESHALLBEGIVENBYANYREGULATIONOFCOMMERCEORREVENUETOTHEPORTSOFONESTATEOVERTHOSEOFANOTHERNORSHALLVESSELSBOUNDTOORFROMONESTATEBEOBLIGEDTOENTERCLEARORPAYDUTIESINANOTHERNOMONEYSHALLBEDRAWNFROMTHETREASURYBUTINCONSEQUENCEOFAPPROPRIATIONSMADEBYLAWANDAREGULARSTATEMENTANDACCOUNTOFTHERECEIPTSANDEXPENDITURESOFALLPUBLICMONEYSHALLBEPUBLISHEDFROMTIMETOTIMENOTITLEOFNOBILITYSHALLBEGRANTEDBYTHEUNITEDSTATESANDNOPERSONHOLDINGANYOFFICEOFPROFITORTRUSTUNDERTHEMSHALLWITHOUTTHECONSENTOFTHECONGRESSACCEPTOFANYPRESENTEMOLUMENTOFFICEORTITLEOFANYKINDWHATEVERFROMANYKINGPRINCEORFOREIGNSTATESECTIONNOSTATESHALLENTERINTOANYTREATYALLIANCEORCONFEDERATIONGRANTLETTERSOFMARQUEANDREPRISALCOINMONEYEMITBILLSOFCREDITMAKEANYTHINGBUTGOLDANDSILVERCOINATENDERINPAYMENTOFDEBTSPASSANYBILLOFATTAINDEREXPOSTFACTOLAWORLAWIMPAIRINGTHEOBLIGATIONOFCONTRACTSORGRANTANYTITLEOFNOBILITYNOSTATESHALLWITHOUTTHECONSENTOFTHECONGRESSLAYANYIMPOSTSORDUTIESONIMPORTSOREXPORTSEXCEPTWHATMAYBEABSOLUTELYNECESSARYFOREXECUTINGITSINSPECTIONLAWSANDTHENETPRODUCEOFALLDUTIESANDIMPOSTSLAIDBYANYSTATEONIMPORTSOREXPORTSSHALLBEFORTHEUSEOFTHETREASURYOFTHEUNITEDSTATESANDALLSUCHLAWSSHALLBESUBJECTTOTHEREVISIONANDCONTROLOFTHECONGRESSNOSTATESHALLWITHOUTTHECONSENTOFCONGRESSLAYANYDUTYOFTONNAGEKEEPTROOPSORSHIPSOFWARINTIMEOFPEACEENTERINTOANYAGREEMENTORCOMPACTWITHANOTHERSTATEORWITHAFOREIGNPOWERORENGAGEINWARUNLESSACTUALLYINVADEDORINSUCHIMMINENTDANGERASWILLNOTADMITOFDELAYARTICLEIISECTIONTHEEXECUTIVEPOWERSHALLBEVESTEDINAPRESIDENTOFTHEUNITEDSTATESOFAMERICAHESHALLHOLDHISOFFICEDURINGTHETERMOFFOURYEARSANDTOGETHERWITHTHEVICEPRESIDENTCHOSENFORTHESAMETERMBEELECTEDASFOLLOWSEACHSTATESHALLAPPOINTINSUCHMANNERASTHELEGISLATURETHEREOFMAYDIRECTANUMBEROFELECTORSEQUALTOTHEWHOLENUMBEROFSENATORSANDREPRESENTATIVESTOWHICHTHESTATEMAYBEENTITLEDINTHECONGRESSBUTNOSENATORORREPRESENTATIVEORPERSONHOLDINGANOFFICEOFTRUSTORPROFITUNDERTHEUNITEDSTATESSHALLBEAPPOINTEDANELECTORTHEELECTORSSHALLMEETINTHEIRRESPECTIVESTATESANDVOTEBYBALLOTFORTWOPERSONSOFWHOMONEATLEASTSHALLNOTLIEANINHABITANTOFTHESAMESTATEWITHTHEMSELVESANDTHEYSHALLMAKEALISTOFALLTHEPERSONSVOTEDFORANDOFTHENUMBEROFVOTESFOREACHWHICHLISTTHEYSHALLSIGNANDCERTIFYANDTRANSMITSEALEDTOTHESEATOFTHEGOVERNMENTOFTHEUNITEDSTATESDIRECTEDTOTHEPRESIDENTOFTHESENATETHEPRESIDENTOFTHESENATESHALLINTHEPRESENCEOFTHESENATEANDHOUSEOFREPRESENTATIVESOPENALLTHECERTIFICATESANDTHEVOTESSHALLTHENBECOUNTEDTHEPERSONHAVINGTHEGREATESTNUMBEROFVOTESSHALLBETHEPRESIDENTIFSUCHNUMBERBEAMAJORITYOFTHEWHOLENUMBEROFELECTORSAPPOINTEDANDIFTHEREBEMORETHANONEWHOHAVESUCHMAJORITYANDHAVEANEQUALNUMBEROFVOTESTHENTHEHOUSEOFREPRESENTATIVESSHALLIMMEDIATELYCHOOSEBYBALLOTONEOFTHEMFORPRESIDENTANDIFNOPERSONHAVEAMAJORITYTHENFROMTHEFIVEHIGHESTONTHELISTTHESAIDHOUSESHALLINLIKEMANNERCHOOSETHEPRESIDENTBUTINCHOOSINGTHEPRESIDENTTHEVOTESSHALLBETAKENBYSTATESTHEREPRESENTATIONFROMEACHSTATEHAVINGONEVOTEAQUORUMFORTHISPURPOSESHALLCONSISTOFAMEMBERORMEMBERSFROMTWOTHIRDSOFTHESTATESANDAMAJORITYOFALLTHESTATESSHALLBENECESSARYTOACHOICEINEVERYCASEAFTERTHECHOICEOFTHEPRESIDENTTHEPERSONHAVINGTHEGREATESTNUMBEROFVOTESOFTHEELECTORSSHALLBETHEVICEPRESIDENTBUTIFTHERESHOULDREMAINTWOORMOREWHOHAVEEQUALVOTESTHESENATESHALLCHOOSEFROMTHEMBYBALLOTTHEVICEPRESIDENTTHECONGRESSMAYDETERMINETHETIMEOFCHOOSINGTHEELECTORSANDTHEDAYONWHICHTHEYSHALLGIVETHEIRVOTESWHICHDAYSHALLBETHESAMETHROUGHOUTTHEUNITEDSTATESNOPERSONEXCEPTANATURALBORNCITIZENORACITIZENOFTHEUNITEDSTATESATTHETIMEOFTHEADOPTIONOFTHISCONSTITUTIONSHALLBEELIGIBLETOTHEOFFICEOFPRESIDENTNEITHERSHALLANYPERSONBEELIGIBLETOTHATOFFICEWHOSHALLNOTHAVEATTAINEDTOTHEAGEOFTHIRTYFIVEYEARSANDBEENFOURTEENYEARSARESIDENTWITHINTHEUNITEDSTATESINCASEOFTHEREMOVALOFTHEPRESIDENTFROMOFFICEOROFHISDEATHRESIGNATIONORINABILITYTODISCHARGETHEPOWERSANDDUTIESOFTHESAIDOFFICETHESAMESHALLDEVOLVEONTHEVICEPRESIDENTANDTHECONGRESSMAYBYLAWPROVIDEFORTHECASEOFREMOVALDEATHRESIGNATIONORINABILITYBOTHOFTHEPRESIDENTANDVICEPRESIDENTDECLARINGWHATOFFICERSHALLTHENACTASPRESIDENTANDSUCHOFFICERSHALLACTACCORDINGLYUNTILTHEDISABILITYBEREMOVEDORAPRESIDENTSHALLBEELECTEDTHEPRESIDENTSHALLATSTATEDTIMESRECEIVEFORHISSERVICESACOMPENSATIONWHICHSHALLNEITHERBEINCREASEDNORDIMINISHEDDURINGTHEPERIODFORWHICHHESHALLHAVEBEENELECTEDANDHESHALLNOTRECEIVEWITHINTHATPERIODANYOTHEREMOLUMENTFROMTHEUNITEDSTATESORANYOFTHEMBEFOREHEENTERONTHEEXECUTIONOFHISOFFICEHESHALLTAKETHEFOLLOWINGOATHORAFFIRMATIONIDOSOLEMNLYSWEARORAFFIRMTHATIWILLFAITHFULLYEXECUTETHEOFFICEOFPRESIDENTOFTHEUNITEDSTATESANDWILLTOTHEBESTOFMYABILITYPRESERVEPROTECTANDDEFENDTHECONSTITUTIONOFTHEUNITEDSTATESSECTIONTHEPRESIDENTSHALLBECOMMANDERINCHIEFOFTHEARMYANDNAVYOFTHEUNITEDSTATESANDOFTHEMILITIAOFTHESEVERALSTATESWHENCALLEDINTOTHEACTUALSERVICEOFTHEUNITEDSTATESHEMAYREQUIRETHEOPINIONINWRITINGOFTHEPRINCIPALOFFICERINEACHOFTHEEXECUTIVEDEPARTMENTSUPONANYSUBJECTRELATINGTOTHEDUTIESOFTHEIRRESPECTIVEOFFICESANDHESHALLHAVEPOWERTOGRANTREPRIEVESANDPARDONSFOROFFENSESAGAINSTTHEUNITEDSTATESEXCEPTINCASESOFIMPEACHMENTHESHALLHAVEPOWERBYANDWITHTHEADVICEANDCONSENTOFTHESENATETOMAKETREATIESPROVIDEDTWOTHIRDSOFTHESENATORSPRESENTCONCURANDHESHALLNOMINATEANDBYANDWITHTHEADVICEANDCONSENTOFTHESENATESHALLAPPOINTAMBASSADORSOTHERPUBLICMINISTERSANDCONSULSJUDGESOFTHESUPREMECOURTANDALLOTHEROFFICERSOFTHEUNITEDSTATESWHOSEAPPOINTMENTSARENOTHEREINOTHERWISEPROVIDEDFORANDWHICHSHALLBEESTABLISHEDBYLAWBUTTHECONGRESSMAYBYLAWVESTTHEAPPOINTMENTOFSUCHINFERIOROFFICERSASTHEYTHINKPROPERINTHEPRESIDENTALONEINTHECOURTSOFLAWORINTHEHEADSOFDEPARTMENTSTHEPRESIDENTSHALLHAVEPOWERTOFILLUPALLVACANCIESTHATMAYHAPPENDURINGTHERECESSOFTHESENATEBYGRANTINGCOMMISSIONSWHICHSHALLEXPIREATTHEENDOFTHEIRNEXTSESSIONSECTIONHESHALLFROMTIMETOTIMEGIVETOTHECONGRESSINFORMATIONOFTHESTATEOFTHEUNIONANDRECOMMENDTOTHEIRCONSIDERATIONSUCHMEASURESASHESHALLJUDGENECESSARYANDEXPEDIENTHEMAYONEXTRAORDINARYOCCASIONSCONVENEBOTHHOUSESOREITHEROFTHEMANDINCASEOFDISAGREEMENTBETWEENTHEMWITHRESPECTTOTHETIMEOFADJOURNMENTHEMAYADJOURNTHEMTOSUCHTIMEASHESHALLTHINKPROPERHESHALLRECEIVEAMBASSADORSANDOTHERPUBLICMINISTERSHESHALLTAKECARETHATTHELAWSBEFAITHFULLYEXECUTEDANDSHALLCOMMISSIONALLTHEOFFICERSOFTHEUNITEDSTATESSECTIONTHEPRESIDENTVICEPRESIDENTANDALLCIVILOFFICERSOFTHEUNITEDSTATESSHALLBEREMOVEDFROMOFFICEONIMPEACHMENTFORANDCONVICTIONOFTREASONBRIBERYOROTHERHIGHCRIMESANDMISDEMEANORSARTICLEIIISECTIONTHEJUDICIALPOWEROFTHEUNITEDSTATESSHALLBEVESTEDINONESUPREMECOURTANDINSUCHINFERIORCOURTSASTHECONGRESSMAYFROMTIMETOTIMEORDAINANDESTABLISHTHEJUDGESBOTHOFTHESUPREMEANDINFERIORCOURTSSHALLHOLDTHEIROFFICESDURINGGOODBEHAVIORANDSHALLATSTATEDTIMESRECEIVEFORTHEIRSERVICESACOMPENSATIONWHICHSHALLNOTBEDIMINISHEDDURINGTHEIRCONTINUANCEINOFFICESECTIONTHEJUDICIALPOWERSHALLEXTENDTOALLCASESINLAWANDEQUITYARISINGUNDERTHISCONSTITUTIONTHELAWSOFTHEUNITEDSTATESANDTREATIESMADEORWHICHSHALLBEMADEUNDERTHEIRAUTHORITYTOALLCASESAFFECTINGAMBASSADORSOTHERPUBLICMINISTERSANDCONSULSTOALLCASESOFADMIRALTYANDMARITIMEJURISDICTIONTOCONTROVERSIESTOWHICHTHEUNITEDSTATESSHALLBEAPARTYTOCONTROVERSIESBETWEENTWOORMORESTATESBETWEENASTATEANDCITIZENSOFANOTHERSTATEBETWEENCITIZENSOFDIFFERENTSTATESBETWEENCITIZENSOFTHESAMESTATECLAIMINGLANDSUNDERGRANTSOFDIFFERENTSTATESANDBETWEENASTATEORTHECITIZENSTHEREOFANDFOREIGNSTATESCITIZENSORSUBJECTSINALLCASESAFFECTINGAMBASSADORSOTHERPUBLICMINISTERSANDCONSULSANDTHOSEINWHICHASTATESHALLBEPARTYTHESUPREMECOURTSHALLHAVEORIGINALJURISDICTIONINALLTHEOTHERCASESBEFOREMENTIONEDTHESUPREMECOURTSHALLHAVEAPPELLATEJURISDICTIONBOTHASTOLAWANDFACTWITHSUCHEXCEPTIONSANDUNDERSUCHREGULATIONSASTHECONGRESSSHALLMAKETHETRIALOFALLCRIMESEXCEPTINCASESOFIMPEACHMENTSHALLBEBYJURYANDSUCHTRIALSHALLBEHELDINTHESTATEWHERETHESAIDCRIMESSHALLHAVEBEENCOMMITTEDBUTWHENNOTCOMMITTEDWITHINANYSTATETHETRIALSHALLBEATSUCHPLACEORPLACESASTHECONGRESSMAYBYLAWHAVEDIRECTEDSECTIONTREASONAGAINSTTHEUNITEDSTATESSHALLCONSISTONLYINLEVYINGWARAGAINSTTHEMORINADHERINGTOTHEIRENEMIESGIVINGTHEMAIDANDCOMFORTNOPERSONSHALLBECONVICTEDOFTREASONUNLESSONTHETESTIMONYOFTWOWITNESSESTOTHESAMEOVERTACTORONCONFESSIONINOPENCOURTTHECONGRESSSHALLHAVEPOWERTODECLARETHEPUNISHMENTOFTREASONBUTNOATTAINDEROFTREASONSHALLWORKCORRUPTIONOFBLOODORFORFEITUREEXCEPTDURINGTHELIFEOFTHEPERSONATTAINTEDARTICLEIVSECTIONFULLFAITHANDCREDITSHALLBEGIVENINEACHSTATETOTHEPUBLICACTSRECORDSANDJUDICIALPROCEEDINGSOFEVERYOTHERSTATEANDTHECONGRESSMAYBYGENERALLAWSPRESCRIBETHEMANNERINWHICHSUCHACTSRECORDSANDPROCEEDINGSSHALLBEPROVEDANDTHEEFFECTTHEREOFSECTIONTHECITIZENSOFEACHSTATESHALLBEENTITLEDTOALLPRIVILEGESANDIMMUNITIESOFCITIZENSINTHESEVERALSTATESAPERSONCHARGEDINANYSTATEWITHTREASONFELONYOROTHERCRIMEWHOSHALLFLEEFROMJUSTICEANDBEFOUNDINANOTHERSTATESHALLONDEMANDOFTHEEXECUTIVEAUTHORITYOFTHESTATEFROMWHICHHEFLEDBEDELIVEREDUPTOBEREMOVEDTOTHESTATEHAVINGJURISDICTIONOFTHECRIMENOPERSONHELDTOSERVICEORLABOURINONESTATEUNDERTHELAWSTHEREOFESCAPINGINTOANOTHERSHALLINCONSEQUENCEOFANYLAWORREGULATIONTHEREINBEDISCHARGEDFROMSUCHSERVICEORLABOURBUTSHALLBEDELIVEREDUPONCLAIMOFTHEPARTYTOWHOMSUCHSERVICEORLABOURMAYBEDUESECTIONNEWSTATESMAYBEADMITTEDBYTHECONGRESSINTOTHISUNIONBUTNONEWSTATESSHALLBEFORMEDORERECTEDWITHINTHEJURISDICTIONOFANYOTHERSTATENORANYSTATEBEFORMEDBYTHEJUNCTIONOFTWOORMORESTATESORPARTSOFSTATESWITHOUTTHECONSENTOFTHELEGISLATURESOFTHESTATESCONCERNEDASWELLASOFTHECONGRESSTHECONGRESSSHALLHAVEPOWERTODISPOSEOFANDMAKEALLNEEDFULRULESANDREGULATIONSRESPECTINGTHETERRITORYOROTHERPROPERTYBELONGINGTOTHEUNITEDSTATESANDNOTHINGINTHISCONSTITUTIONSHALLBESOCONSTRUEDASTOPREJUDICEANYCLAIMSOFTHEUNITEDSTATESOROFANYPARTICULARSTATESECTIONTHEUNITEDSTATESSHALLGUARANTEETOEVERYSTATEINTHISUNIONAREPUBLICANFORMOFGOVERNMENTANDSHALLPROTECTEACHOFTHEMAGAINSTINVASIONANDONAPPLICATIONOFTHELEGISLATUREOROFTHEEXECUTIVEWHENTHELEGISLATURECANNOTBECONVENEDAGAINSTDOMESTICVIOLENCEARTICLEVTHECONGRESSWHENEVERTWOTHIRDSOFBOTHHOUSESSHALLDEEMITNECESSARYSHALLPROPOSEAMENDMENTSTOTHISCONSTITUTIONORONTHEAPPLICATIONOFTHELEGISLATURESOFTWOTHIRDSOFTHESEVERALSTATESSHALLCALLACONVENTIONFORPROPOSINGAMENDMENTSWHICHINEITHERCASESHALLBEVALIDTOALLINTENTSANDPURPOSESASPARTOFTHISCONSTITUTIONWHENRATIFIEDBYTHELEGISLATURESOFTHREEFOURTHSOFTHESEVERALSTATESORBYCONVENTIONSINTHREEFOURTHSTHEREOFASTHEONEORTHEOTHERMODEOFRATIFICATIONMAYBEPROPOSEDBYTHECONGRESSPROVIDEDTHATNOAMENDMENTWHICHMAYBEMADEPRIORTOTHEYEARONETHOUSANDEIGHTHUNDREDANDEIGHTSHALLINANYMANNERAFFECTTHEFIRSTANDFOURTHCLAUSESINTHENINTHSECTIONOFTHEFIRSTARTICLEANDTHATNOSTATEWITHOUTITSCONSENTSHALLBEDEPRIVEDOFITSEQUALSUFFRAGEINTHESENATEARTICLEVIALLDEBTSCONTRACTEDANDENGAGEMENTSENTEREDINTOBEFORETHEADOPTIONOFTHISCONSTITUTIONSHALLBEASVALIDAGAINSTTHEUNITEDSTATESUNDERTHISCONSTITUTIONASUNDERTHECONFEDERATIONTHISCONSTITUTIONANDTHELAWSOFTHEUNITEDSTATESWHICHSHALLBEMADEINPURSUANCETHEREOFANDALLTREATIESMADEORWHICHSHALLBEMADEUNDERTHEAUTHORITYOFTHEUNITEDSTATESSHALLBETHESUPREMELAWOFTHELANDANDTHEJUDGESINEVERYSTATESHALLBEBOUNDTHEREBYANYTHINGINTHECONSTITUTIONORLAWSOFANYSTATETOTHECONTRARYNOTWITHSTANDINGTHESENATORSANDREPRESENTATIVESBEFOREMENTIONEDANDTHEMEMBERSOFTHESEVERALSTATELEGISLATURESANDALLEXECUTIVEANDJUDICIALOFFICERSBOTHOFTHEUNITEDSTATESANDOFTHESEVERALSTATESSHALLBEBOUNDBYOATHORAFFIRMATIONTOSUPPORTTHISCONSTITUTIONBUTNORELIGIOUSTESTSHALLEVERBEREQUIREDASAQUALIFICATIONTOANYOFFICEORPUBLICTRUSTUNDERTHEUNITEDSTATESARTICLEVIITHERATIFICATIONOFTHECONVENTIONSOFNINESTATESSHALLBESUFFICIENTFORTHEESTABLISHMENTOFTHISCONSTITUTIONBETWEENTHESTATESSORATIFYINGTHESAMEDONEINCONVENTIONBYTHEUNANIMOUSCONSENTOFTHESTATESPRESENTTHESEVENTEENTHDAYOFSEPTEMBERINTHEYEAROFOURLORDONETHOUSANDSEVENHUNDREDANDEIGHTYSEVENANDOFTHEINDEPENDENCEOFTHEUNITEDSTATESOFAMERICATHETWELFTHINWITNESSWHEREOFWEHAVEHEREUNTOSUBSCRIBEDOURNAMESWETH

CIPHER3

ENCRYPTION: Vigenere Cipher

CIPHERTEXT: see cipher3.txt

KEY: **TUCSON**

PLAINTEXT: “call me Ishmael some years ago..” (First 25 letters)

CALLMEISHMAELSOMEYEARSAGONEVERMINDHOWLONGPRECISELYHAVINGLITTLEORNOMONEYINMYPURSEANDNOTHINGPARTICULARTOINTERESTMEONSHOREITHOUGHTIWOULDSAILABOUTALITTLEANDSEETHEWATERYPARTOFTHEWORLDITISAWAYIHAVEOFDRIVINGOFFTHESPLEENANDREGULATINGTHECIRCULATIONWHENEVERIFINDMYSELFGROWINGGRIMABOUTTHEMOUTHWHENEVERITISADAMPDRIZZLYNOVEMBERINMYSOULWHENEVERIFINDMYSELFINVOLUNTARILYPAUSINGBEFORECOFFINWAREHOUSESANDBRINGINGUPTHEREAROFEVERYFUNERALIMEETANDESPECIALLYWHENEVERMYHYPOSGETSUCHANUPPERHANDOFMETHATITREQUIRESASTRONGMORALPRINCIPLETOPREVENTMEFROMDELIBERATELYSTEPPINGINTOTHESTREETANDMETHODICALLYKNOCKINGPEOPLESHATSOFFTHENIACCOUNTITHIGHTIMETOGETTOSEAASSOONASICANTHISISMYSUBSTITUTEFORPISTOLANDBALLWITHAPHILOSOPHICALFLOURISHCATOTHROWSHIMSELFUPONHISSWORDIQUIETLYTAKETOTHESHIPTHEREISNOTHINGSURPRISINGINTHISIFTHEYBUTKNEWITALMOSTALLMENINTHEIRDEGREESOMETIMEOROTHERCHERISHVERYNEARLYTHESAMEFEELINGSTOWARDSTHEOCEANWITHMETHERENOWISYOURINSULARCITYOFTHEMANHATTOESBELTEDROUNDBYWHARVESASINDIANISLESBYCORALREEFSCOMMERCESURROUNDSITWITHHERSURFRIGHTANDLEFTTHESTREETSTAKEYOUWATERWARDITSEXTREMEDOWNTOWNISTHEBATTERYWHERETHATNOBLEMOLEISWASHEDBYWAVESANDCOOLEDBYBREEZESWHICHAFEWHOURSPREVIOUSWEREOUTOFSIGHTOFLANDLOOKATTHECROWDSOFWATERGAZERSTHERECIRCUMAMBULATETHECITYOFADREAMYSABBATHAFTERNOONGOFROMCORLEARSHOOKTOCOENTIESSLIPANDFROMTHENCEBYWHITEHALLNORTHWARDWHATDOYOUSEEPOSTEDLIKESILENTSENTINELSALLAROUNDTHETOWNSTANDTHOUSANDSUPONTHOUSANDSOFMORTALMENFIXEDINOCEANREVERIESSOMELEANINGAGAINSTTHESPILESSOMESEATEDUPONTHEPIERHEADSSOMELOOKINGOVERTHEBULWARKSOFSHIPSFROMCHINASOMEHIGHALOFTINTHERIGGINGASIFSTRIVINGTOGETASTILLBETTERSEAWARDPEEPBUTTHESEAREALLLANDSMENOFWEEKDAYSPENTUPINLATHANDPLASTERTIEDTOCOUNTERSNAILEDTOBENCHESCLINCHEDTODESKSHOWTHENISTHISARETHEGREENFIELDSGONEWHATDOTHEYHEREBUTLOOKHERECOMEMORECROWDSPACINGSTRAIGHTFORTHEWATERANDSEEMINGLYBOUNDFORADIVESTRANGENOTHINGWILLCONTENTTHEMBUTTHEEXTREMESTLIMITOFTHELANDLOITERINGUNDERTHESHADYLEEOFYONDERWAREHOUSESWILLNOTSUFFICENOTHEYMUSTGETJUSTASNIGHTHEWATERASTHEYPOSSIBLYCANWITHOUTFALLINGINANDTHERETHEYSTANDMILESOFTHEMLEAGUESINLANDERSALLTHEYCOMEFROMLANESANDALLEYSSTREETSANDAVENUESNORTHEASTSOUTHANDWESTYETHERETHEYALLUNITETELLMEDOESTHEMAGNETICVIRTUEOFTHENEEDLESOFTHECOMPASSESOFALLTHOSESHIPSATTRACTTHEMTHITHERONCEMORESAYYOUAREINTHECOUNTRYINSOMEHIGHLANDOFLAKESTAKEALMOSTANYPATHYOUPLEASEANDTENTOONEITCARRIESYOUDOWNINADALEANDLEAVESYOUTHEREBYAPOOLINTHESTREAMTHEREISMAGICINITLETTHEMOSTABSENTMINDEDOFMENBEPLUNGEDINHISDEEPESTREVERIESSTANDTHATMANONHISLEGSSETHISFEETAGOINGANDHEWILLINFALLIBLYLEADYOUTOWATERIFWATERTHEREBEINALLTHATREGIONSHOULDYOUEVERBEATHIRSTINTHEGREATAMERICANDESERTTRYTHISEXPERIMENTIFYOURCARAVANHAPPENTOBESUPPLIEDWITHAMETAPHYSICALPROFESSORYESASEVERYONEKNOWSMEDITATIONANDWATERAREWEDDEDFOREVERBUTHEREISANARTISTHEDESIRESTOPAINTYOUTHEDREAMIESTSHADIESTQUIETESTMOSTENCHANTINGBITOFROMANTICLANDSCAPEINALLTHEVALLEYOFTHESACOWHATISTHECHIEFELEMENTHEEMPLOYSTHERESTANDHISTREESEACHWITHAHOLLOWTRUNKASIFAHERMITANDACRUCIFIXWEREWITHINANDHERESLEEPSHISMEADOWANDTHERESLEEPHISCATTLEANDUPFROMYONDERCOTTAGEGOESASLEEPYSMOKEDEEPINTODISTANTWOODLANDSWINDSAMAZYWAYREACHINGTOOVERLAPPINGSPURSOFMOUNTAINSBATHEDINTHEIRHILLSIDEBLUEBUTTHOUGHTHEPICTURELIESTHUSTRANCEDANDTHOUGHTHISPINETREESHAKESDOWNITSSIGHSLIKELEAVESUPONTHISSHEPHERDSHEADYETALLWEREVAINUNLESSTHESHEPHERDSEYEWEREFIXEDUPONTHEMAGICSTREAMBEFOREHIMGOVISITTHEPRAIRIESINJUNEWHENFORSCORESONSCORESOFMILESYOUWADEKNEEDEEPAMONGTIGERLILIESWHATISTHEONECHARMWANTINGWATERTHEREISNOTADROPOFWATERTHEREWERENIAGARABUTACATARACTOFSANDWOULDYOUTRAVELYOURTHOUSANDMILESTOSEEITWHYDIDTHEPOORPOETOFTENNESSEEUPONSUDDENLYRECEIVINGTWOHANDFULSOFSILVERDELIBERATEWHETHERTOBUYHIMACOATWHICHHESADLYNEEDEDORINVESTHISMONEYINAPEDESTRIANTRIPTOROCKAWAYBEACHWHYISALMOSTEVERYROBUSTHEALTHYBOYWITHAROBUSTHEALTHYSOULINHIMATSOMETIMEOROTHERCRAZYTOGOTOSEAWHYUPONYOURFIRSTVOYAGEASAPASSENGERDIDYOUYOURSELFFEELSUCHAMYSTICALVIBRATIONWHENFIRSTTOLDTHATYOUANDYOURSHIPWERENOWOUTOFSIGHTOFLANDWHYDIDTHEOLDPERSIANSHOLDTHESEAHOLYWHYDIDTHEGREEKSGIVEITASEPARATEDEITYANDOWNBROTHEROFJOVESURELYALLTHISISNOTWITHOUTMEANINGANDSTILLDEEPERTHEMEANINGOFTHATSTORYOFNARCISSUSWHOBECAUSEHECOULDNOTGRASPTHETORMENTINGMILDIMAGEHESAWINTHEFOUNTAINPLUNGEDINTOITANDWASDROWNEDBUTTHATSAMEIMAGEWEOURSELVESSEEINALLRIVERSANDOCEANSITISTHEIMAGEOFTHEUNGRASPABLEPHANTOMOFLIFEANDTHISISTHEKEYTOITALLNOWWHENISAYTHATIAMINTHEHABITOFGOINGTOSEAWHENEVERIBEGINTOGROWHAZYABOUTTHEEYESANDBEGINTOBEOVERCONSCIOUSOFMYLUNGSIDONOTMEANTOHAVEITINFERREDTHATIEVERGOTOSEAASAPASSENGERFORTOGOASAPASSENGERYOUMUSTNEEDSHAVEAPURSEANDAPURSEISBUTARAGUNLESSYOUHAVESOMETHINGINITBESIDESPASSENGERSGETSEASICKGROWQUARRELSOMEDONTSLEEPOFNIGHTSDONOTENJOYTHEMSELVESMUCHASAGENERALTHINGNOINEVERGOASAPASSENGERNORTHOUGHIAMSOMETHINGOFASALTDOIEVERGOTOSEAASACOMMODOREORACAPTAINORACOOKIABANDONTHEGLORYANDDISTINCTIONOFSUCHOFFICESTOTHOSEWHOLIKETHEMFORMYPARTIABOMINATEALLHONOURABLERESPECTABLETOILSTRIALSANDTRIBULATIONSOFEVERYKINDWHATSOEVERITISQUITEASMUCHASICANDOTOTAKECAREOFMYSELFWITHOUTTAKINGCAREOFSHIPSBARQUESBRIGSSCHOONERSANDWHATNOTANDASFORGOINGASCOOKTHOUGHICONFESSTHEREISCONSIDERABLEGLORYINTHATACOOKBEINGASORTOFOFFICERONSHIPBOARDYETSOMEHOWINEVERFANCIEDBROILINGFOWLSTHOUGHONCEBROILEDJUDICIOUSLYBUTTEREDANDJUDGMATICALLYSALTEDANDPEPPEREDTHEREISNOONEWHOWILLSPEAKMORERESPECTFULLYNOTTOSAYREVERENTIALLYOFABROILEDFOWLTHANIWILLITISOUTOFTHEIDOLATROUSDOTINGSOFTHEOLDEGYPTIANSUPONBROILEDIBISANDROASTEDRIVERHORSETHATYOUSEETHEMUMMIESOFTHOSECREATURESINTHEIRHUGEBAKEHOUSESTHEPYRAMIDSNOWHENIGOTOSEAIGOASASIMPLESAILORRIGHTBEFORETHEMASTPLUMBDOWNINTOTHEFORECASTLEALOFTTHERETOTHEROYALMASTHEADTRUETHEYRATHERORDERMEABOUTSOMEANDMAKEMEJUMPFROMSPARTOSPARLIKEAGRASSHOPPERINAMAYMEADOWANDATFIRSTTHISSORTOFTHINGISUNPLEASANTENOUGHITTOUCHESONESSENSEOFHONOURPARTICULARLYIFYOUCOMEOFANOLDESTABLISHEDFAMILYINTHELANDTHEVANRENSSELAERSORRANDOLPHSORHARDICANUTESANDMORETHANALLIFJUSTPREVIOUSTOPUTTINGYOURHANDINTOTHETARPOTYOUHAVEBEENLORDINGITASACOUNTRYSCHOOLMASTERMAKINGTHETALLESTBOYSSTANDINAWEOFYOUTHETRANSITIONISAKEENONEIASSUREYOUFROMASCHOOLMASTERTOASAILORANDREQUIRESASTRONGDECOCTIONOFSENECAANDTHESTOICSTOENABLEYOUTOGRINANDBEARITBUTEVENTHISWEARSOFFINTIMEWHATOFITIFSOMEOLDHUNKSOFASEACAPTAINORDERSMETOGETABROOMANDSWEEPDOWNTHEDECKSWHATDOESTHATINDIGNITYAMOUNTTOWEIGHEDIMEANINTHESCALESOFTHENEWTESTAMENTDOYOUTHINKTHEARCHANGELGABRIELTHINKSANYTHINGTHELESSOFMEBECAUSEIPROMPTLYANDRESPECTFULLYOBEYTHATOLDHUNKSINTHATPARTICULARINSTANCEWHOAINTASLAVETELLMETHATWELLTHENHOWEVERTHEOLDSEACAPTAINSMAYORDERMEABOUTHOWEVERTHEYMAYTHUMPANDPUNCHMEABOUTIHAVETHESATISFACTIONOFKNOWINGTHATITISALLRIGHTTHATEVERYBODYELSEISONEWAYOROTHERSERVEDINMUCHTHESAMEWAYEITHERINAPHYSICALORMETAPHYSICALPOINTOFVIEWTHATISANDSOTHEUNIVERSALTHUMPISPASSEDROUNDANDALLHANDSSHOULDRUBEACHOTHERSSHOULDERBLADESANDBECONTENTAGAINIALWAYSGOTOSEAASASAILORBECAUSETHEYMAKEAPOINTOFPAYINGMEFORMYTROUBLEWHEREASTHEYNEVERPAYPASSENGERSASINGLEPENNYTHATIEVERHEARDOFONTHECONTRARYPASSENGERSTHEMSELVESMUSTPAYANDTHEREISALLTHEDIFFERENCEINTHEWORLDBETWEENPAYINGANDBEINGPAIDTHEACTOFPAYINGISPERHAPSTHEMOSTUNCOMFORTABLEINFLICTIONTHATTHETWOORCHARDTHIEVESENTAILEDUPONUSBUTBEINGPAIDWHATWILLCOMPAREWITHITTHEURBANEACTIVITYWITHWHICHAMANRECEIVESMONEYISREALLYMARVELLOUSCONSIDERINGTHATWESOEARNESTLYBELIEVEMONEYTOBETHEROOTOFALLEARTHLYILLSANDTHATONNOACCOUNTCANAMONIEDMANENTERHEAVENAHHOWCHEERFULLYWECONSIGNOURSELVESTOPERDITIONFINALLYIALWAYSGOTOSEAASASAILORBECAUSEOFTHEWHOLESOMEEXERCISEANDPUREAIROFTHEFORECASTLEDECKFORASINTHISWORLDHEADWINDSAREFARMOREPREVALENTTHANWINDSFROMASTERNTHATISIFYOUNEVERVIOLATETHEPYTHAGOREANMAXIMSOFORTHEMOSTPARTTHECOMMODOREONTHEQUARTERDECKGETSHISATMOSPHEREATSECONDHANDFROMTHESAILORSONTHEFORECASTLEHETHINKSHEBREATHESITFIRSTBUTNOTSOINMUCHTHESAMEWAYDOTHECOMMONALTYLEADTHEIRLEADERSINMANYOTHERTHINGSATTHESAMETIMETHATTHELEADERSLITTLESUSPECTITBUTWHEREFOREITWASTHATAFTERHAVINGREPEATEDLYSMELTTHESEAASAMERCHANTSAILORISHOULDNOWTAKEITINTOMYHEADTOGOONAWHALINGVOYAGETHISTHEINVISIBLEPOLICEOFFICEROFTHEFATESWHOHASTHECONSTANTSURVEILLANCEOFMEANDSECRETLYDOGSMEANDINFLUENCESMEINSOMEUNACCOUNTABLEWAYHECANBETTERANSWERTHANANYONEELSEANDDOUBTLESSMYGOINGONTHISWHALINGVOYAGEFORMEDPARTOFTHEGRANDPROGRAMMEOFPROVIDENCETHATWASDRAWNUPALONGTIMEAGOITCAMEINASASORTOFBRIEFINTERLUDEANDSOLOBETWEENMOREEXTENSIVEPERF

CIPHER4

ENCRYPTION: One-Time Pad

CIPHERTEXT: see cipher4.txt

KEY:

PLAINTEXT:

APPENDIX

BIBLIOGRAPHY

1. Stalling’s Book
2. python hacker book/online
3. encyclopedia Brittanica