Cryptanalysis of Ciphertexts

Azer Hojlas

January 26, 2023

Introduction

The fully decoded plaintexts for both ciphertext 1 and 2 are included in this PDF. The written codes used to decode the texts are also included as well as the key for ciphertext 2.

Ciphertext 1 analysis and process

After an initial frequency analysis of letters, digrams and trigrams that seemed to repeat, I assumed that I was dealing with a simple substitution cipher. The only simple ciphers covered in class were Caesar and random substitution. I started out by successfully implementing a Caesar decoder but failed to get a meaningful result (all shifts in the range of 1 to 38 produced gibberish).

That left me with a random substitution cipher. For this part I used no code, I simply pasted the ciphertext into a popular frequency analysis website (dcode) and got to work. I was lucky that the blank space character ”_” mapped to itself, otherwise it would have taken a lot longer to solve for the different characters. I started out by assuming that the most frequent letter (besides ”_” or blank space) was a substitute for ”E”. Then, finding the substitution for the word ”the” was not difficult, as it is the most popular three letter word in the English language and most frequent trigram in the ciphertext (or variations thereof). After finding the substitutions for ”blank space”, ”T”, ”H”, and ”E”, I set about identifying the substitutes for ”A” and ”I”, the two most popular English one-letter words, which had corresponding statistical matches in the text. After that, finding the rest of the substitutions for each letter of the alphabet was not difficult, as it only required some guessing along with circa an hour of trial and error.

The following table was used when converting the ciphertext into plaintext

```
def ciphertext_1_mapper():
ciphertext = import_text("Ciphertext_1.txt")
decode_table = {
    "W": "A",
    "J": "B",
    "6": "C",
    "V": "D",
    "I": "E",
    "5": "F",
    "U": "G",
    "H": "H",
    "4": "I",
    "T": "J",
    "G": "K",
    "3": "L",
    "S": "M",
    "F": "N",
    "2": "O",
    "R": "P",
        "E": "Q",
        "1": "R",
        "Q": "S",
        "D": "T",
        "O": "U",
        "P": "V",
        "C": "W",
        "#": "X",
        "0": "Y",
        "B": "Z",
        "N": "\n",
        "_": " "
    }
```

The following is the plaintext I got when decoding the ciphertext according to the table above:

NOT ALL SICK MEN ARE UTTERLY WRETCHED SOME ARE BLESSED WITH SONS SOME WITH FRIENDS SOME WITH RICHES SOME WITH WORTHY WORKS THE HALT CAN MANAGE A HORSE THE HANDLESS A FLOCK THE DEAF BE A DOUGHTY FIGHTER TO BE BLIND IS BETTER THAN TO BURN ON A PYRE THERE IS NOTHING THE DEAD CAN DO IT IS ALWAYS BETTER TO BE ALIVE THE LIVING CAN KEEP A COW FIRE I SAW WARMING A WEALTHY MAN WITH A COLD CORPSE AT HIS DOOR A SON IS A BLESSING THOUGH BORN LATE TO A FATHER NO LONGER ALIVE STONES WOULD SELDOM STAND BY THE HIGHWAY IF SONS DID NOT SET THEM THERE HE WELCOMES THE NIGHT WHO HAS ENOUGH PROVISIONS SHORT ARE THE SAILS OF A SHIP DANGEROUS THE DARK IN AUTUMN THE WIND MAY VEER WITHIN FIVE DAYS AND MANY TIMES IN A MONTH THE HALF WIT DOES NOT KNOW THAT GOLD MAKES APES OF MANY MEN ONE IS RICH ONE IS POOR THERE IS NO BLAME IN THAT CATTLE DIE KINDRED DIE EVERY MAN IS MORTAL BUT THE GOOD NAME NEVER DIES OF ONE WHO HAS DONE WELL CATTLE DIE KINDRED DIE EVERY MAN IS MORTAL BUT I KNOW ONE THING THAT NEVER DIES THE GLORY OF THE GREAT DEAD FIELDS AND FLOCKS HAD FITJUNGS SONS WHO NOW CARRY BEGGING BOWLS WEALTH MAY VANISH IN THE WINK OF AN EYE GOLD IS THE FALSEST OF FRIENDS IN THE FOOL WHO ACQUIRES CATTLE AND LANDS OR WINS A WOMANS LOVE HIS WISDOM WANES WITH HIS WAXING PRIDE HE SINKS FROM SENSE TO CONCEIT NOW IS ANSWERED WHAT YOU ASK OF THE RUNES GRAVEN BY THE GODS MADE BY THE ALL FATHER SENT BY THE POWERFUL SAGE LT IS BEST FOR MAN TO REMAIN SILENT FOR THESE THINGS GIVE THANKS AT NIGHTFALL THE DAY GONE A GUTTERED TORCH A SWORD TESTED THE TROTH OF A MAID ICE CROSSED ALE DRUNK HEW WOOD IN WINDTIME IN FINE WEATHER SAIL TELL IN THE NIGHTTIME TALES TO HOUSEGIRLS FOR TOO MANY EYES ARE OPEN BY DAY FROM A SHIP EXPECT SPEED FROM A SHIELD COVER KEENNESS FROM A SWORD BUT A KISS FROM A GIRL DRINK ALE BY THE HEARTH OVER ICE GLIDE BUY A STAINED SWORD BUY A STARVING MARE TO FATTEN AT HOME AND FATTEN THE WATCHDOG TRUST NOT AN ACRE EARLY SOWN NOR PRAISE A SON TOO SOON WEATHER RULES THE ACRE WIT THE SON BOTH ARE EXPOSED TO PERIL A SNAPPING BOW A BURNING FLAME A GRINNING WOLF A GRUNTING BOAR A RAUCOUS CROW A ROOTLESS TREE A BREAKING WAVE A BOILING KETTLE A FLYING ARROW AN EBBING TIDE A COILED ADDER THE ICE OF A NIGHT A BRIDES BED TALK A BROAD SWORD A BEARS PLAY A PRINCE S CHILDREN A WITCH S WELCOME THE WIT OF A SLAVE A SICK CALF A CORPSE STILL FRESH A BROTHERS KILLER ENCOUNTERED UPON THE HIGHWAY A HOUSE HALFBURNED A RACING STALLION WHO HAS WRENCHED A LEG ARE NEVER SAFE LET NO MAN TRUST THEM NO MAN SHOULD TRUST A MAIDENS WORDS NOR WHAT A WOMAN SPEAKS SPUN ON A WHEEL WERE WOMENS HEARTS IN THEIR BREASTS WAS IMPLANTED CAPRICE TO LOVE A WOMAN WHOSE WAYS ARE FALSE IS LIKE SLEDDING OVER SLIPPERY ICE WITH UNSHOD HORSES OUT OF CONTROL BADLY TRAINED TWOYEAROLDS OR DRIFTING RUDDERLESS ON A ROUGH SEA OR CATCHING A REINDEER WITH A CRIPPLED HAND ON A THAWING HILLSIDE THINK NOT TO DO IT NAKED I MAY SPEAK NOW FOR

I KNOW BOTH MEN ARE TREACHEROUS TOO FAIREST WE SPEAK WHEN FALSEST WE THINK MANY A MAID IS DECEIVED GALLANTLY SHALL HE SPEAK AND GIFTS BRING WHO WISHES FOR WOMANS LOVE PRAISE THE FEATURES OF THE FAIR GIRL WHO COURTS WELL WILL CONQUER NEVER REPROACH ANOTHER FOR HIS LOVE IT HAPPENS OFTEN ENOUGH THAT BEAUTY ENSNARES WITH DESIRE THE WISE WHILE THE FOOLISH REMAIN UNMOVED NEVER REPROACH THE PLIGHT OF ANOTHER FOR IT HAPPENS TO MANY MEN STRONG DESIRE MAY STUPEFY HEROES DULL THE WITS OF THE WISE THE MIND ALONE KNOWS WHAT IS NEAR THE HEART EACH IS HIS OWN JUDGE THE WORST SICKNESS FOR A WISE MAN IS TO CRAVE WHAT HE CANNOT ENJOY SO I LEARNED WHEN I SAT IN THE REEDS HOPING TO HAVE MY DESIRE LOVELY WAS THE FLESH OF THAT FAIR GIRL BUT NOTHING I HOPED FOR HAPPENED I SAW ON A BED BILLINGS DAUGHTER SUN WHITE ASLEEP NO GREATER DELIGHT I LONGED FOR THEN THAN TO LIE IN HER LOVELY ARMS COME ODHINN AFTER NIGHTFALL IF YOU WISH FOR A MEETING WITH ME ALL WOULD BE LOST IF ANYONE SAW US AND LEARNED THAT WE WERE LOVERS AFIRE WITH LONGING I LEFT HER THEN DECEIVED BY HER SOFT WORDS I THOUGHT MY WOOING HAD WON THE MAID THAT I WOULD HAVE MY WAY AFTER NIGHTFALL I HURRIED BACK BUT THE WARRIORS WERE ALL AWAKE LIGHTS WERE BURNING BLAZING TORCHES SO FALSE PROVED THE PATH TOWARDS DAYBREAK BACK I CAME THE GUARDS WERE SOUND ASLEEP I FOUND THEN THAT THE FAIR WOMAN HAD TIED A BITCH TO HER BED MANY A GIRL WHEN ONE GETS TO KNOW HER PROVES TO BE FICKLE AND FALSE THAT TREACHEROUS MAIDEN TAUGHT ME A LESSON THE CRAFTY WOMAN COVERED ME WITH SHAME THAT WAS ALL I GOT FROM HER LET A MAN WITH HIS GUESTS BE GLAD AND MERRY MODEST A MAN SHOULD BE BUT TALK WELL IF HE INTENDS TO BE WISE AND EXPECTS PRAISE FROM MEN FIMBUL FAMBI IS THE FOOL CALLED UNABLE TO OPEN HIS MOUTH FRUITLESS MY ERRAND HAD I BEEN SILENT WHEN I CAME TO SUTTUNGS COURTS WITH SPIRITED WORDS I SPOKE TO MY PROFIT IN THE HALL OF THE AGED GIANT RATI HAD GNAWED A NARROW PASSAGE CHEWED A CHANNEL THROUGH STONE A PATH AROUND THE ROADS OF GIANTS I WAS LIKE TO LOSE MY HEAD GUNNLOD SAT ME IN THE GOLDEN SEAT POURED ME PRECIOUS MEAD ILL REWARD SHE HAD FROM ME FOR THAT FOR HER PROUD AND PASSIONATE HEART HER BROODING FOREBODING SPIRIT WHAT I WON FROM HER I HAVE WELL USED I HAVE WAXED IN WISDOM SINCE I CAME BACK BRINGING TO ASGARD ODRERIR THE SACRED DRAUGHT HARDLY WOULD I HAVE COME HOME ALIVE FROM THE GARTH OF THE GRIM TROLL HAD GUNNLOD NOT HELPED ME THE GOOD WOMAN WHO WRAPPED HER ARMS AROUND ME THE FOLLOWING DAY THE FROST GIANTS CAME WALKED INTO HARS HALL TO ASK FOR HARS ADVICE HAD BOLVERK THEY ASKED COME BACK TO HIS FRIENDS OR HAD HE BEEN SLAIN BY SUTTUNG ODHINN THEY SAID SWORE AN OATH ON HIS RING WHO FROM NOW ON WILL TRUST HIM BY FRAUD AT THE FEAST HE BEFUDDLED SUTTUNG AND BROUGHT GRIEF TO GUNNLOD IT IS TIME TO SING IN THE SEAT OF THE WISE OF WHAT AT URDS WELL I SAW IN SILENCE SAW AND THOUGHT ON LONG I LISTENED TO MEN RUNES HEARD SPOKEN COUNSELS REVEALED AT HARS HALL IN HARS HALL THERE I HEARD THIS LODDFAFNIR LISTEN TO MY COUNSEL YOU WILL FARE WELL IF YOU FOLLOW IT IT WILL HELP YOU MUCH IF YOU HEED IT NEVER RISE AT NIGHT UNLESS YOU NEED TO SPY OR TO EASE YOURSELF IN THE OUTHOUSE SHUN A WOMAN WISE IN MAGIC HER BED AND HER EMBRACES IF SHE CAST A SPELL YOU WILL CARE NO LONGER TO MEET AND SPEAK WITH MEN DESIRE NO FOOD DESIRE NO PLEASURE IN SORROW FALL ASLEEP NEVER SEDUCE ANOTHERS WIFE NEVER MAKE HER YOUR MISTRESS IF YOU MUST JOURNEY TO MOUNTAINS AND FIRTHS TAKE FOOD AND FODDER WITH YOU NEVER OPEN YOUR HEART TO AN EVIL MAN WHEN FORTUNE DOES NOT FAVOUR YOU FROM AN EVIL MAN IF YOU MAKE HIM YOUR FRIEND YOU WILL GET EVIL FOR GOOD I SAW A WARRIOR WOUNDED FATALLY BY THE WORDS OF AN EVIL WOMAN HER CUNNING TONGUE CAUSED HIS DEATH THOUGH WHAT SHE ALLEGED WAS A LIE IF YOU KNOW A FRIEND YOU CAN FULLY TRUST GO OFTEN TO HIS HOUSE GRASS AND BRAMBLES GROW QUICKLY UPON THE UNTRODDEN TRACK WITH A GOOD MAN IT IS GOOD TO TALK MAKE HIM YOUR FAST FRIEND BUT WASTE NO WORDS ON A WITLESS OAF

NOR SIT WITH A SENSELESS APE CHERISH THOSE NEAR YOU NEVER BE THE FIRST TO BREAK WITH A FRIEND CARE EATS HIM WHO CAN NO LONGER OPEN HIS HEART TO ANOTHER AN EVIL MAN IF YOU MAKE HIM YOUR FRIEND WILL GIVE YOU EVIL FOR GOOD A GOOD MAN IF YOU MAKE HIM YOUR FRIEND WILL PRAISE YOU IN EVERY PLACE AFFECTION IS MUTUAL WHEN MEN CAN OPEN ALL THEIR HEART TO EACH OTHER HE WHOSE WORDS ARE ALWAYS FAIR IS UNTRUE AND NOT TO BE TRUSTED BANDY NO SPEECH WITH A BAD MAN OFTEN THE BETTER IS BEATEN IN A WORD FIGHT BY THE WORSE BE NOT A COBBLER NOR A CARVER OF SHAFTS EXCEPT IT BE FOR YOURSELF IF A SHOE FIT ILL OR A SHAFT BE CROOKED THE MAKER GETS CURSES AND KICKS IF AWARE THAT ANOTHER IS WICKED SAY SO MAKE NO TRUCE OR TREATY WITH FOES NEVER SHARE IN THE SHAMEFULLY GOTTEN BUT ALLOW YOURSELF WHAT IS LAWFUL NEVER LIFT YOUR EYES AND LOOK UP IN BATTLE LEST THE HEROES ENCHANT YOU WHO CAN CHANGE WARRIORS SUDDENLY INTO HOGS WITH A GOOD WOMAN IF YOU WISH TO ENJOY HER WORDS AND HER GOOD WILL PLEDGE HER FAIRLY AND BE FAITHFUL TO IT ENJOY THE GOOD YOU ARE GIVEN BE NOT OVER WARY BUT WARY ENOUGH FIRST OF THE FOAMING ALE SECOND OF A WOMAN WED TO ANOTHER THIRD OF THE TRICKS OF THIEVES MOCK NOT THE TRAVELLER MET ON THE ROAD NOR MALICIOUSLY LAUGH AT THE GUEST SCOFF NOT AT GUESTS NOR TO THE GATE CHASE THEM BUT RELIEVE THE LONELY AND WRETCHED THE SITTERS IN THE HALL SELDOM KNOW THE KIN OF THE NEWCOMER THE BEST MAN IS MARRED BY FAULTS THE WORST IS NOT WITHOUT WORTH NEVER LAUGH AT THE OLD WHEN THEY OFFER COUNSEL OFTEN THEIR WORDS ARE WISE FROM SHRIVELLED SKIN FROM SCRAGGY THINGS THAT HAND AMONG THE HIDES AND MOVE AMID THE GUTS CLEAR WORDS OFTEN COME HEAVY THE BEAM ABOVE THE DOOR HANG A HORSESHOE ON IT AGAINST ILLLUCK LEST IT SHOULD SUDDENLY CRASH AND CRUSH YOUR GUESTS MEDICINES EXIST AGAINST MANY EVILS EARTH AGAINST DRUNKENNESS HEATHER AGAINST WORMS OAK AGAINST COSTIVENESS CORN AGAINST SORCERY SPURRED RYE AGAINST RUPTURE RUNES AGAINST BALES THE MOON AGAINST FEUDS FIRE AGAINST SICKNESS EARTH MAKES HARMLESS THE FLOODS WOUNDED I HUNG ON A WINDSWEPT GALLOWS FOR NINE LONG NIGHTS PIERCED BY A SPEAR PLEDGED TO ODHINN OFFERED MYSELF TO MYSELF THE WISEST KNOW NOT FROM WHENCE SPRING THE ROOTS OF THAT ANCIENT ROOD THEY GAVE ME NO BREAD THEY GAVE ME NO MEAD I LOOKED DOWN WITH A LOUD CRY I TOOK UP RUNES FROM THAT TREE I FELL NINE LAYS OF POWER I LEARNED FROM THE FAMOUS BOLTHOR BESTLA S FATHER HE POURED ME A DRAUGHT OF PRECIOUS MEAD MIXED WITH MAGIC ODRERIR WAXED AND THROVE WELL WORD FROM WORD GAVE WORDS TO ME DEED FROM DEED GAVE DEEDS TO ME RUNES YOU WILL FIND AND READABLE STAVES VERY STRONG STAVES VERY STOUT STAVES STAVES THAT BOLTHOR STAINED MADE BY MIGHTY POWERS GRAVEN BY THE PROPHETIC GOD FOR THE GODS BY ODHINN FOR THE ELVES BY DAIN BY DVALIN TOO FOR THE DWARVES BY ASVID FOR THE HATEFUL GIANTS AND SOME I CARVED MYSELF THUND BEFORE MAN WAS MADE SCRATCHED THEM WHO ROSE FIRST FELL THEREAFTER KNOW HOW TO CUT THEM KNOW HOW TO READ THEM KNOW HOW TO STAIN THEM KNOW HOW TO PROVE THEM KNOW HOW TO EVOKE THEM KNOW HOW TO SCORE THEM KNOW HOW TO SEND THEM KNOW HOW TO SEND THEM BETTER NOT TO ASK THAN TO OVERPLEDGE AS A GIFT THAT DEMANDS A GIFT BETTER NOT TO SEND THAN TO SLAY TOO MANY THE FIRST CHARM I KNOW IS UNKNOWN TO RULERS OR ANY OF HUMAN KIND HELP IT IS NAMED FOR HELP IT CAN GIVE IN HOURS OF SORROW AND ANGUISH I KNOW A SECOND THAT THE SONS OF MEN MUST LEARN WHO WISH TO BE LEECHES I KNOW A THIRD IN THE THICK OF BATTLE IF MY NEED BE GREAT ENOUGH IT WILL BLUNT THE EDGES OF ENEMY SWORDS THEIR WEAPONS WILL MAKE NO WOUNDS I KNOW A FOURTH IT WILL FREE ME QUICKLY IF FOES SHOULD BIND ME FAST WITH STRONG CHAINS A CHANT THAT MAKES FETTERS SPRING FROM THE FEET BONDS BURST FROM THE H

The following code was used in my unsuccessful attempt at breaking what I believed was a Ceasar cipher

```
def letter_shifter(letter, steps):
    alphabet = "0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ_#"
    index = alphabet.find(letter)
    newLetterIndex = (index + steps) % len(alphabet)
    return alphabet[newLetterIndex]

def caesar_decryptor(ciphertext_filepath, step):
    newText = ""
    ciphertext = import_text(ciphertext_filepath)
    for i in range(len(ciphertext)):
        newText += letter_shifter(ciphertext[i], step)
    return newText
```

Ciphertext 2 analysis and process

Ciphertext 2 was a bit more difficult and time consuming to solve. The only other solvable ciphers covered in class were ”Vigenere” and ”Hill”, and Hill is to my knowledge difficult to crack without the use of a known piece of plaintext known beforehand, i.e using a known plaintext attack. Thus, I was left with Vigenere and went about solving it. My initial efforts were lazy in that i did not look for a practical algorithm to solve the cipher. After implementing code for encoding and decoding text with an arbitrary key, I simply took to brute forcing every permutation of an n-sized key and checking the output against an English dictionary to see if it would produce any matches. Unfortunately, this only worked for keys up to size 5 (38^5 different alphabet permutations, the alphabet being of size 38), after which it became impossible to brute-force larger keys due to the amount of time it took. The brute force algorithm ran in roughly $O(38^n)$ time. Later on, using a proper Vigenere-solving algorithm, I found that the probable key-size was roughly 12. Thus, brute-forcing said key would have taken roughly 13 million years to find based on the earlier runtimes of my python script. I clearly needed to switch tactics.

First, I needed to figure out the key-length. This I could do by employing Kasiski examination by hand. I was far too involved after my initial failure however so I decided to do it properly with code. First, I started by writing code that outputs the index of coincidence (henceforth IOC) for any given text written in the assignment designated alphabet. Then I proceeded by dividing the cipher text into groupings of key size n (each n:th letter goes into a new string that is examined). Then for every n, these groupings produce the average IOC for every n-grouping. The n (and multiples thereof) with the highest IOC or IOC closes to the average English language IOC of 0,066 is presumed to be the correct key-length. The idea behind this is if a correct key-length has been guessed, then each grouping of text will have been encrypted by the same sub-key. Thus, this grouping, like for the caesar cipher, does not upset letter frequencies and should match letter frequencies and the IOC of the English language. Then it is simply a case of figuring out which letter out of 38 possible produces a decoded text that matches the English language. This was achieved by a very simple function that assignes a score based on if the three most frequent letters in the outputted text are blank space ”_”, ”E” and ”A”, as is the case with the English language. This is repeated for all sub-keys until the entire key has been produced. Lastly, the ciphertext is decrypted with said key, which produces human readable plaintext.

The key for my specific ciphertext was the following:

$$IYCS6M1GWAUM$$

The output, or plaintext, when decrypting the cipihertext with said key and replacing ”_” and ”#” with blank space and line breaks is the following:

0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ HOW HAPPY I AM THAT I AM GONE MY DEAR FRIEND WHAT A THING IS THE HEART OF MAN TO LEAVE YOU FROM WHOM I HAVE BEEN INSEPARABLE WHOM I LOVE SO DEARLY AND YET TO FEEL HAPPY I

KNOW YOU WILL FORGIVE ME HAVE NOT OTHER ATTACHMENTS BEEN SPECIALLY APPOINTED BY FATE TO TORMENT A HEAD LIKE MINE POOR LEONORA AND YET I WAS NOT TO BLAME WAS IT MY FAULT THAT WHILST THE PECULIAR CHARMS OF HER SISTER AFFORDED ME AN AGREEABLE ENTERTAINMENT A PASSION FOR ME WAS ENGENDERED IN HER FEEBLE HEART AND YET AM I WHOLLY BLAMELESS DID I NOT ENCOURAGE HER EMOTIONS DID I NOT FEEL CHARMED AT THOSE TRULY GENUINE EXPRESSIONS OF NATURE WHICH THOUGH BUT LITTLE MIRTHFUL IN REALITY SO OFTEN AMUSED US DID I NOT BUT OH WHAT IS MAN THAT HE DARES SO TO ACCUSE HIMSELF MY DEAR FRIEND I PROMISE YOU I WILL IMPROVE I WILL NO LONGER AS HAS EVER BEEN MY HABIT CONTINUE TO RUMINATE ON EVERY PETTY VEXATION WHICH FORTUNE MAY DISPENSE I WILL ENJOY THE PRESENT AND THE PAST SHALL BE FOR ME THE PAST NO DOUBT YOU ARE RIGHT MY BEST OF FRIENDS THERE WOULD BE FAR LESS SUFFERING AMONGST MANKIND IF MEN AND GOD KNOWS WHY THEY ARE SO FASHIONED DID NOT EMPLOY THEIR IMAGINATIONS SO ASSIDUOUSLY IN RECALLING THE MEMORY OF PAST SORROW INSTEAD OF BEARING THEIR PRESENT LOT WITH EQUANIMITY BE KIND ENOUGH TO INFORM MY MOTHER THAT I SHALL ATTEND TO HER BUSINESS TO THE BEST OF MY ABILITY AND SHALL GIVE HER THE EARLIEST INFORMATION ABOUT IT I HAVE SEEN MY AUNT AND FIND THAT SHE IS VERY FAR FROM BEING THE DISAGREEABLE PERSON OUR FRIENDS ALLEGE HER TO BE SHE IS A LIVELY CHEERFUL WOMAN WITH THE BEST OF HEARTS I EXPLAINED TO HER MY MOTHERS WRONGS WITH REGARD TO THAT PART OF HER PORTION WHICH HAS BEEN WITHHELD FROM HER SHE TOLD ME THE MOTIVES AND REASONS OF HER OWN CONDUCT AND THE TERMS ON WHICH SHE IS WILLING TO GIVE UP THE WHOLE AND TO DO MORE THAN WE HAVE ASKED IN SHORT I CANNOT WRITE FURTHER UPON THIS SUBJECT AT PRESENT ONLY ASSURE MY MOTHER THAT ALL WILL GO ON WELL AND I HAVE AGAIN OBSERVED MY DEAR FRIEND IN THIS TRIFLING AFFAIR THAT MISUNDERSTANDINGS AND NEGLECT OCCASION MORE MISCHIEF IN THE WORLD THAN EVEN MALICE AND WICKEDNESS AT ALL EVENTS THE TWO LATTER ARE OF LESS FREQUENT OCCURRENCE IN OTHER RESPECTS I AM VERY WELL OFF HERE SOLITUDE IN THIS TERRESTRIAL PARADISE IS A GENIAL BALM TO MY MIND AND THE YOUNG SPRING CHEERS WITH ITS BOUNTEOUS PROMISES MY OFTENTIMES MISGIVING HEART EVERY TREE EVERY BUSH IS FULL OF FLOWERS AND ONE MIGHT WISH HIMSELF TRANSFORMED INTO A BUTTERFLY TO FLOAT ABOUT IN THIS OCEAN OF PERFUME AND FIND HIS WHOLE EXISTENCE IN IT THE TOWN ITSELF IS DISAGREEABLE BUT THEN ALL AROUND YOU FIND AN INEXPRESSIBLE BEAUTY OF NATURE THIS INDUCED THE LATE COUNT M TO LAY OUT A GARDEN ON ONE OF THE SLOPING HILLS WHICH HERE INTERSECT EACH OTHER WITH THE MOST CHARMING VARIETY AND FORM THE MOST LOVELY VALLEYS THE GARDEN IS SIMPLE AND IT IS EASY TO PERCEIVE EVEN UPON YOUR FIRST ENTRANCE THAT THE PLAN WAS NOT DESIGNED BY A SCIENTIFIC GARDENER BUT BY A MAN WHO WISHED TO GIVE HIMSELF UP HERE TO THE ENJOYMENT OF HIS OWN SENSITIVE HEART MANY A TEAR HAVE I ALREADY SHED TO THE MEMORY OF ITS DEPARTED MASTER IN A SUMMER HOUSE WHICH IS NOW REDUCED TO RUINS BUT WAS HIS FAVOURITE RESORT AND NOW IS MINE I SHALL SOON BE MASTER OF THE PLACE THE GARDENER HAS BECOME ATTACHED TO ME WITHIN THE LAST FEW DAYS AND HE WILL LOSE NOTHING THEREBY MAY 10 A WONDERFUL SERENITY HAS TAKEN POSSESSION OF MY ENTIRE SOUL LIKE THESE SWEET MORNINGS OF SPRING WHICH I ENJOY WITH MY WHOLE HEART I AM ALONE AND FEEL THE CHARM OF EXISTENCE IN THIS SPOT WHICH WAS CREATED FOR THE BLISS OF SOULS LIKE MINE I AM SO HAPPY MY DEAR FRIEND SO ABSORBED IN THE EXQUISITE SENSE OF MERE TRANQUIL EXISTENCE THAT I NEGLECT MY TALENTS I SHOULD BE INCAPABLE OF DRAWING A SINGLE STROKE AT THE PRESENT MOMENT AND YET I FEEL THAT I NEVER WAS A GREATER ARTIST THAN NOW WHEN WHILE THE LOVELY VALLEY TEEMS WITH VAPOUR AROUND ME AND THE MERIDIAN SUN STRIKES THE UPPER SURFACE OF THE IMPENETRABLE FOLIAGE OF MY TREES AND BUT A FEW STRAY GLEAMS STEAL INTO THE INNER SANCTUARY I THROW MYSELF DOWN AMONG THE TALL GRASS BY THE TRICKLING STREAM AND AS I LIE CLOSE TO THE EARTH A THOUSAND UNKNOWN PLANTS ARE NOTICED BY

ME WHEN I HEAR THE BUZZ OF THE LITTLE WORLD AMONG THE STALKS AND GROW FAMILIAR WITH THE COUNTLESS INDESCRIBABLE FORMS OF THE INSECTS AND FLIES THEN I FEEL THE PRESENCE OF THE ALMIGHTY WHO FORMED US IN HIS OWN IMAGE AND THE BREATH OF THAT UNIVERSAL LOVE WHICH BEARS AND SUSTAINS US AS IT FLOATS AROUND US IN AN ETERNITY OF BLISS AND THEN MY FRIEND WHEN DARKNESS OVERSPREADS MY EYES AND HEAVEN AND EARTH SEEM TO DWELL IN MY SOUL AND ABSORB ITS POWER LIKE THE FORM OF A BELOVED MISTRESS THEN I OFTEN THINK WITH LONGING OH WOULD I COULD DESCRIBE THESE CONCEPTIONS COULD IMPRESS UPON PAPER ALL THAT IS LIVING SO FULL AND WARM WITHIN ME THAT IT MIGHT BE THE MIRROR OF MY SOUL AS MY SOUL IS THE MIRROR OF THE INFINITE GOD O MY FRIEND BUT IT IS TOO MUCH FOR MY STRENGTH I SINK UNDER THE WEIGHT OF THE SPLENDOUR OF THESE VISIONS MAY 12 I KNOW NOT WHETHER SOME DECEITFUL SPIRITS HAUNT THIS SPOT OR WHETHER IT BE THE WARM CELESTIAL FANCY IN MY OWN HEART WHICH MAKES EVERYTHING AROUND ME SEEM LIKE PARADISE IN FRONT OF THE HOUSE IS A FOUNTAIN A FOUNTAIN TO WHICH I AM BOUND BY A CHARM LIKE MELUSINA AND HER SISTERS DESCENDING A GENTLE SLOPE YOU COME TO AN ARCH WHERE SOME TWENTY STEPS LOWER DOWN WATER OF THE CLEAREST CRYSTAL GUSHES FROM THE MARBLE ROCK THE NARROW WALL WHICH ENCLOSES IT ABOVE THE TALL TREES WHICH ENCIRCLE THE SPOT AND THE COOLNESS OF THE PLACE ITSELF EVERYTHING IMPARTS A PLEASANT BUT SUBLIME IMPRESSION NOT A DAY PASSES ON WHICH I DO NOT SPEND AN HOUR THERE THE YOUNG MAIDENS COME FROM THE TOWN TO FETCH WATER INNOCENT AND NECESSARY EMPLOYMENT AND FORMERLY THE OCCUPATION OF THE DAUGHTERS OF KINGS AS I TAKE MY REST THERE THE IDEA OF THE OLD PATRIARCHAL LIFE IS AWAKENED AROUND ME I SEE THEM OUR OLD ANCESTORS HOW THEY FORMED THEIR FRIENDSHIPS AND CONTRACTED ALLIANCES AT THE FOUNTAIN SIDE AND I FEEL HOW FOUNTAINS AND STREAMS WERE GUARDED BY BENEFICENT SPIRITS HE WHO IS A STRANGER TO THESE SENSATIONS HAS NEVER REALLY ENJOYED COOL REPOSE AT THE SIDE OF A FOUNTAIN AFTER THE FATIGUE OF A WEARY SUMMER DAY MAY 13 YOU ASK IF YOU SHALL SEND ME BOOKS MY DEAR FRIEND I BESEECH YOU FOR THE LOVE OF GOD RELIEVE ME FROM SUCH A YOKE I NEED NO MORE TO BE GUIDED AGITATED HEATED MY HEART FERMENTS SUFFICIENTLY OF ITSELF I WANT STRAINS TO LULL ME AND I FIND THEM TO PERFECTION IN MY HOMER OFTEN DO I STRIVE TO ALLAY THE BURNING FEVER OF MY BLOOD AND YOU HAVE NEVER WITNESSED ANYTHING SO UNSTEADY SO UNCERTAIN AS MY HEART BUT NEED I CONFESS THIS TO YOU MY DEAR FRIEND WHO HAVE SO OFTEN ENDURED THE ANGUISH OF WITNESSING MY SUDDEN TRANSITIONS FROM SORROW TO IMMODERATE JOY AND FROM SWEET MELANCHOLY TO VIOLENT PASSIONS I TREAT MY POOR HEART LIKE A SICK CHILD AND GRATIFY ITS EVERY FANCY DO NOT MENTION THIS AGAIN THERE ARE PEOPLE WHO WOULD CENSURE ME FOR IT MAY 15 THE COMMON PEOPLE OF THE PLACE KNOW ME ALREADY AND LOVE ME PARTICULARLY THE CHILDREN WHEN AT FIRST I ASSOCIATED WITH THEM AND INQUIRED IN A FRIENDLY TONE ABOUT THEIR VARIOUS TRIFLES SOME FANCIED THAT I WISHED TO RIDICULE THEM AND TURNED FROM ME IN EXCEEDING ILL HUMOUR I DID NOT ALLOW THAT CIRCUMSTANCE TO GRIEVE ME I ONLY FELT MOST KEENLY WHAT I HAVE OFTEN BEFORE OBSERVED PERSONS WHO CAN CLAIM A CERTAIN RANK KEEP THEMSELVES COLDLY ALOOF FROM THE COMMON PEOPLE AS THOUGH THEY FEARED TO LOSE THEIR IMPORTANCE BY THE CONTACT WHILST WANTON IDLERS AND SUCH AS ARE PRONE TO BAD JOKING AFFECT TO DESCEND TO THEIR LEVEL ONLY TO MAKE THE POOR PEOPLE FEEL THEIR IMPERTINENCE ALL THE MORE KEENLY I KNOW VERY WELL THAT WE ARE NOT ALL EQUAL NOR CAN BE SO BUT IT IS MY OPINION THAT HE WHO AVOIDS THE COMMON PEOPLE IN ORDER NOT TO LOSE THEIR RESPECT IS AS MUCH TO BLAME AS A COWARD WHO HIDES HIMSELF FROM HIS ENEMY BECAUSE HE FEARS DEFEAT THE OTHER DAY I WENT TO THE FOUNTAIN AND FOUND A YOUNG SERVANT GIRL WHO HAD SET HER PITCHER ON THE LOWEST STEP AND LOOKED AROUND TO SEE IF ONE OF HER COMPANIONS WAS APPROACHING TO PLACE IT ON HER HEAD I RAN DOWN AND LOOKED AT HER SHALL I HELP YOU PRETTY LASS SAID I SHE BLUSHED

DEEPLY OH SIR SHE EXCLAIMED NO CEREMONY I REPLIED SHE ADJUSTED HER HEAD GEAR AND I HELPED HER SHE THANKED ME AND ASCENDED THE STEPS MAY 17 I HAVE MADE ALL SORTS OF ACQUAINTANCES BUT HAVE AS YET FOUND NO SOCIETY I KNOW NOT WHAT ATTRACTION I POSSESS FOR THE PEOPLE SO MANY OF THEM LIKE ME AND ATTACH THEMSELVES TO ME AND THEN I FEEL SORRY WHEN THE ROAD WE PURSUE TOGETHER GOES ONLY A SHORT DISTANCE IF YOU INQUIRE WHAT THE PEOPLE ARE LIKE HERE I MUST ANSWER THE SAME AS EVERYWHERE THE HUMAN RACE IS BUT A MONOTONOUS AFFAIR MOST OF THEM LABOUR THE GREATER PART OF THEIR TIME FOR MERE SUBSISTENCE AND THE SCANTY PORTION OF FREEDOM WHICH REMAINS TO THEM SO TROUBLES THEM THAT THEY USE EVERY EXERTION TO GET RID OF IT OH THE DESTINY OF MAN BUT THEY ARE A RIGHT GOOD SORT OF PEOPLE IF I OCCASIONALLY FORGET MYSELF AND TAKE PART IN THE INNOCENT PLEASURES WHICH ARE NOT YET FORBIDDEN TO THE PEASANTRY AND ENJOY MYSELF FOR INSTANCE WITH GENUINE FREEDOM AND SINCERITY ROUND A WELL COVERED TABLE OR ARRANGE AN EXCURSION OR A DANCE OPPORTUNELY AND SO FORTH ALL THIS PRODUCES A GOOD EFFECT UPON MY DISPOSITION ONLY I MUST FORGET THAT THERE LIE DORMANT WITHIN ME SO MANY OTHER QUALITIES WHICH MOULDER USELESSLY AND WHICH I AM OBLIGED TO KEEP CAREFULLY CONCEALED AH THIS THOUGHT AFFECTS MY SPIRITS FEARFULLY AND YET TO BE MISUNDERSTOOD IS THE FATE OF THE LIKE OF US ALAS THAT THE FRIEND OF MY YOUTH IS GONE ALAS THAT I EVER KNEW HER I MIGHT SAY TO MYSELF YOU ARE A DREAMER TO SEEK WHAT IS NOT TO BE FOUND HERE BELOW BUT SHE HAS BEEN MINE I HAVE POSSESSED THAT HEART THAT NOBLE SOUL IN WHOSE PRESENCE I SEEMED TO BE MORE THAN I REALLY WAS BECAUSE I WAS ALL THAT I COULD BE GOOD HEAVENS DID THEN A SINGLE POWER OF MY SOUL REMAIN UNEXERCISED IN HER PRESENCE COULD I NOT DISPLAY TO ITS FULL EXTENT THAT MYSTERIOUS FEELING WITH WHICH MY HEART EMBRACES NATURE WAS NOT OUR INTERCOURSE A PERPETUAL WEB OF THE FINEST EMOTIONS OF THE KEENEST WIT THE VARIETIES OF WHICH EVEN IN THEIR VERY ECCENTRICITY BORE THE STAMP OF GENIUS ALAS THE FEW YEARS BY WHICH SHE WAS MY SENIOR BROUGHT HER TO THE GRAVE BEFORE ME NEVER CAN I FORGET HER FIRM MIND OR HER HEAVENLY PATIENCE A FEW DAYS AGO I MET A CERTAIN YOUNG V A FRANK OPEN FELLOW WITH A MOST PLEASING COUNTENANCE HE HAS JUST LEFT THE UNIVERSITY DOES NOT DEEM HIMSELF OVERWISE BUT BELIEVES HE KNOWS MORE THAN OTHER P

The following is the code I developed to break the cipher:

```
    # Author: Azer Hojlas
# Date: 2023-01-26
# Functionality: Encode and decode text using key; find IOC of text and period (keylength) of ciphert
#                for keys with key size n < 6; statistical analysis for keys > 6
#
# Usage: Run file and simply input filename or path, the code will take care of the rest

from itertools import permutations
import enchant
import time
import re
from collections import Counter
from operator import itemgetter

# Global variables
check_if_english = enchant.Dict("en_US")
alphabet = "0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ_#"
english_index_of_coincidence = 0.0660

# Counts the index of coincidence of a text
```

```
def index_of_coincidence(text):
    counter = Counter(text)
    total = sum(counter.values())
    sum_for_each = 0
    for i in alphabet:
        sum_for_each = sum_for_each + counter[i]*(counter[i] - 1)
    return (sum_for_each / (total*(total - 1)))

# Builds a list with strings built with every nth letter of a string, iteratively
def slice_into_groupings(text, n):
    return [text[i::n] for i in range(n)]

# Divides ciphertext into groupings, the n-size numbered grouping with the highest ioc is the key-siz
def period_finder(text):
    list_of_strings = []
    for i in range(1, len(alphabet)):
        list_of_strings.append(slice_into_groupings(text, i))

    dict_of_IOCs = {}

    for list in list_of_strings:
        sum_average = 0
        for string in list:
            ioc = index_of_coincidence(string)
            sum_average = sum_average + ioc
        dict_of_IOCs[len(list)] = sum_average / len(list)

    return dict_of_IOCs

# Find the key given frequency analysis of the groupings based on key length
def key_finder(ciphertext, n):
    list_of_strings = slice_into_groupings(ciphertext, n)
    key = []
    for text in list_of_strings:
        letter_scores = []
        for letter in alphabet:
            decoded = decode(text, letter)
            decoded_score = is_english(decoded)
            letter_scores.append([letter, decoded_score])
        letter_scores_sorted = sorted(letter_scores, key=itemgetter(1))
        key.append(letter_scores_sorted[-1][0])
    return listToString(key)

# Give a score based on the frequency of common english letters
def is_english(text):
    score = 0
    counted = Counter(sorted(text)).most_common()
    if (counted[0][0] == ’_’ or counted[0][0] == ’E’):
        score = score + 1
    if (counted[1][0] == ’_’ or counted[1][0] == ’E’):
        score = score + 1
    if (counted[2][0] == ’_’ or counted[2][0] == ’E’ or counted[2][0] == ’A’):
        score = score + 1
    return score
```

```
# imports a text file
def import_text(file_path):
    with open(file_path, ’r’) as file:
        text = file.read()
    return text

# Converts list to string
def listToString(s):
    str1 = ""
    for ele in s:
        str1 += ele
    return str1

# Takes the key and repeats it until it matches the length of the ciphertext
def key_matcher(text, key):
    key = list(key)
    for i in range(len(text) - len(key)):
        key.append(key[i % len(key)])
    return("" . join(key))

# Takes plaintext and key and creates a vigenere ciphertext
def encode(plaintext, key):
    key_elongated = key_matcher(plaintext, key)
    cipher_text = []
    for i in range(len(plaintext)):
        index = (alphabet.find(plaintext[i]) + alphabet.find(key_elongated[i])) % len(alphabet)
        letter = alphabet[index]
        cipher_text.append(letter)
    return("" . join(cipher_text))

# Takes ciphertext and key and decodes into plaintext
def decode(ciphertext, key):
    key_elongated = key_matcher(ciphertext, key)
    cipher_text = []
    for i in range(len(ciphertext)):
        index = (alphabet.find(ciphertext[i]) - alphabet.find(key_elongated[i])) % len(alphabet)
        letter = alphabet[index]
        cipher_text.append(letter)
    return("" . join(cipher_text))

# Finds all key permutations given a key size n. Used for brute force
def key_generator(n_gram):
    return tuple_to_string_list(list(permutations(alphabet, n_gram)))

# Converts tuple to string
def tuple_to_string_list(tuple_list):
    remade = []
    for i in tuple_list:
        remade.append("" . join(i))
    return remade

# Declared checker as a global variable, which saves a lot of time. Checks for the amount of english
def amount_english_words(text):
    splitted = re.split(r’_|#’, text)
    correct_words = 0
    for word in splitted:
        if (len(word) < 2):
            continue
        if (check_if_english.check(word) == True):
            correct_words = correct_words + 1
    return correct_words

# Brute force guesses keys until correct one is found, each text is checked if written in english. Fe
def brute_force(ciphertext, cutoff, n_keys):
    shortened = ciphertext[:cutoff]
    keys = key_generator(n_keys)
    lookup = {}
    for key in keys:
        plaintext = decode(shortened, key)
        lookup[key] = amount_english_words(plaintext)
    descending = sorted(lookup.items(), key = lambda x: x[1], reverse = True)
    print("\n")
    print(decode(shortened, descending[0][0]))
    print("\n")
    print("Second closest key with corresponding correct amount of words: " + str(descending[1]))
    print("Closest key with corresponding correct amount of words: " + str(descending[0]))
    print("\n")

# Can be used for any key size
def statistical_analysis(ciphertext):
    ciphertext_cleaned = re.split(r’_|#’, ciphertext)
    key_sizes = []
    table = period_finder(ciphertext)
    for length in table:
        if (table[length] > english_index_of_coincidence):
            key_sizes.append(length)
    for n in key_sizes:
        key = key_finder(ciphertext, n)
        decoded = decode(ciphertext, key)
        if ((amount_english_words(decoded) / len(ciphertext_cleaned)) > 0.8):
            print(decoded, "\n\n", "key length: ", n, "\n\n", "Key: ", key)
            break
        else:
            print("key not found")


def main():

    start_time = time.time()
    ciphertext = import_text(input("Please input filepath or filename of ciphertext: "))
    statistical_analysis(ciphertext)
    print("\n Runtime: %s seconds \n" % (time.time() - start_time))


if __name__ == "__main__":
    main()
```