Caesar Cipher

Mark Nakamae

Cal Poly SLO

June 2020

Description

This project involved deciphering ciphertexts encrypted using the caesar cipher algorithm described [here](https://en.wikipedia.org/wiki/Caesar_cipher)**.** This is a simple substitution encryption algorithm that replaces letters based on the specified shift in alphabet dictated by a key letter. This algorithm can be solved through brute force and simple frequency analysis to find the decrypted plaintext.

In this folder, I’ve included my thought process on approaching my solution, as well as the source code I’ve written and sample encrypted files.

**caesar\_1** Encryption Key: 8

SCROOGE TOOK HIS MELANCHOLY DINNER IN HIS USUAL MELANCHOLY TAVERN; AND HAVING READ ALL THE NEWSPAPERS, AND BEGUILED THE REST OF THE EVENING WITH HIS BANKER’S-BOOK, WENT HOME TO BED. HE LIVED IN CHAMBERS WHICH HAD ONCE BELONGED TO HIS DECEASED PARTNER. THEY WERE A GLOOMY SUITE OF ROOMS, IN A LOWERING PILE OF BUILDING UP A YARD, WHERE IT HAD SO LITTLE BUSINESS TO BE, THAT ONE COULD SCARCELY HELP FANCYING IT MUST HAVE RUN THERE WHEN IT WAS A YOUNG HOUSE, PLAYING AT HIDE-AND-SEEK WITH OTHER HOUSES, AND FORGOTTEN THE WAY OUT AGAIN. IT WAS OLD ENOUGH NOW, AND DREARY ENOUGH, FOR NOBODY LIVED IN IT BUT SCROOGE, THE OTHER ROOMS BEING ALL LET OUT AS OFFICES. THE YARD WAS SO DARK THAT EVEN SCROOGE, WHO KNEW ITS EVERY STONE, WAS FAIN TO GROPE WITH HIS HANDS. THE FOG AND FROST SO HUNG ABOUT THE BLACK OLD GATEWAY OF THE HOUSE, THAT IT SEEMED AS IF THE GENIUS OF THE WEATHER SAT IN MOURNFUL MEDITATION ON THE THRESHOLD.

**caesar\_2** Encryption Key 15

ONEOFTHEPHENOMENAWHICHHADPECULIARLYATTRACTEDMYATTENTIONWASTHESTRUCTUREOFTHEHUMANFRAME,AND,INDEED,ANYANIMALENDUEDWITHLIFE.WHENCE,IOFTENASKEDMYSELF,DIDTHEPRINCIPLEOFLIFEPROCEED?ITWASABOLDQUESTION,ANDONEWHICHHASEVERBEENCONSIDEREDASAMYSTERY;YETWITHHOWMANYTHINGSAREWEUPONTHEBRINKOFBECOMINGACQUAINTED,IFCOWARDICEORCARELESSNESSDIDNOTRESTRAINOURINQUIRIES.IREVOLVEDTHESECIRCUMSTANCESINMYMINDANDDETERMINEDTHENCEFORTHTOAPPLYMYSELFMOREPARTICULARLYTOTHOSEBRANCHESOFNATURALPHILOSOPHYWHICHRELATETOPHYSIOLOGY.UNLESSIHADBEENANIMATEDBYANALMOSTSUPERNATURALENTHUSIASM,MYAPPLICATIONTOTHISSTUDYWOULDHAVEBEENIRKSOMEANDALMOSTINTOLERABLE.TOEXAMINETHECAUSESOFLIFE,WEMUSTFIRSTHAVERECOURSETODEATH.IBECAMEACQUAINTEDWITHTHESCIENCEOFANATOMY,BUTTHISWASNOTSUFFICIENT;IMUSTALSOOBSERVETHENATURALDECAYANDCORRUPTIONOFTHEHUMANBODY.INMYEDUCATIONMYFATHERHADTAKENTHEGREATESTPRECAUTIONSTHATMYMINDSHOULDBEIMPRESSEDWITHNOSUPERNATURALHORRORS.IDONOTEVERREMEMBERTOHAVETREMBLEDATATALEOFSUPERSTITIONORTOHAVEFEAREDTHEAPPARITIONOFASPIRIT.DARKNESSHADNOEFFECTUPONMYFANCY,ANDACHURCHYARDWASTOMEMERELYTHERECEPTACLEOFBODIESDEPRIVEDOFLIFE,WHICH,FROMBEINGTHESEATOFBEAUTYANDSTRENGTH,HADBECOMEFOODFORTHEWORM.NOWIWASLEDTOEXAMINETHECAUSEANDPROGRESSOFTHISDECAYANDFORCEDTOSPENDDAYSANDNIGHTSINVAULTSANDCHARNEL-HOUSES.MYATTENTIONWASFIXEDUPONEVERYOBJECTTHEMOSTINSUPPORTABLETOTHEDELICACYOFTHEHUMANFEELINGS.ISAWHOWTHEFINEFORMOFMANWASDEGRADEDANDWASTED;IBEHELDTHECORRUPTIONOFDEATHSUCCEEDTOTHEBLOOMINGCHEEKOFLIFE;ISAWHOWTHEWORMINHERITEDTHEWONDERSOFTHEEYEANDBRAIN.IPAUSED,EXAMININGANDANALYSINGALLTHEMINUTIAEOFCAUSATION,ASEXEMPLIFIEDINTHECHANGEFROMLIFETODEATH,ANDDEATHTOLIFE,UNTILFROMTHEMIDSTOFTHISDARKNESSASUDDENLIGHTBROKEINUPONME—ALIGHTSOBRILLIANTANDWONDROUS,YETSOSIMPLE,THATWHILEIBECAMEDIZZYWITHTHEIMMENSITYOFTHEPROSPECTWHICHITILLUSTRATED,IWASSURPRISEDTHATAMONGSOMANYMENOFGENIUSWHOHADDIRECTEDTHEIRINQUIRIESTOWARDSTHESAMESCIENCE,THATIALONESHOULDBERESERVEDTODISCOVERSOASTONISHINGASECRET.

**caesar\_3** Encryption Key: 20

BUT THIS IS NOT A CLAIM THAT MAN SHOULD STAY ALWAYS YOUTHFUL. SUPPOSING THAT THAT FAMOUS SPANIARD, LANDING UPON FLORIDA'S CORAL STRANDS, HAD FOUND THAT MYTHICAL FOUNTAIN OF YOUTH; WHAT A CALAMITY FOR MANKIND! A WORLD WITHOUT MATURITY OF THOUGHT; WITHOUT MAN'S FULL-GROWN MUSCULAR ABILITY TO CONSTRUCT MIGHTY BUILDINGS, RAILROADS AND SHIPS; A WORLD WITHOUT AUTHORS, DOCTORS, SAVANTS, MUSICIANS; NOTHING BUT YOUTH! I CAN THINK OF BUT A SOLITARY APPROVAL OF SUCH A CONDITION; FOR SUCH A HORROR AS WAR WOULD NOT,—COULD NOT OCCUR; FOR A CHILD IS, NATURALLY, A SMALL BUNCH OF SYMPATHY. I KNOW THAT BOYS WILL "SCRAP;" ALSO THAT "SPATS" WILL OCCUR AMONGST GIRLS; BUT, AT SUCH A MONSTROSITY AS KILLINGS BY BOMBING TOWNS, SINKING SHIPS, OR MASS ANNIHILATION OF MARCHING TROOPS, CHILDHOOD WOULD STAND AGHAST. NOT A TINY BIRD WOULD FALL; NOR WOULD ANY FORM OF GUN NOR FACILITY FOR MANUFACTURING IT, INSULT THAT ALMOST HOLY PURITY OF YOUTHFUL THOUGHT. ANYBODY WHO KNOWS THAT WRACKING SORROW BROUGHT UPON A CHILD BY A DYING PUPPY OR CAT, KNOWS THAT CHILDHOOD CAN SHOW US THAT OUR FIGHTING, OUR POLICY OF "A TOOTH FOR A TOOTH," IS ABOMINABLY WRONG.

**caesar\_4** Encryption Key: 3

ASGADSBYSATTHINKINGTHUS,HISPLANWASRAPIDLYGROWING;AND,INAMONTH,WASACTUALLYSTARTINGTOWORK.HOW?YOU'LLKNOWSHORTLY;BUTFIRST,YOUSHOULDKNOWTHISJOHNGADSBY;AMANOF"AROUNDFIFTY;"AFAMILYMAN,ANDKNOWNTHROUGHOUTBRANTONHILLSFORHISHIGHSTANDARDOFHONORANDALTRUISMONANYKINDOFANOCCASIONFORPUBLICGOOD.ALOYALCHURCHMAN,GADSBYWASAMANWHO,THOUGHADMITTINGTHATANOCCASIONALFAULTINOURDAILYACTSISBOUNDTOOCCUR,HADTAUGHTHISTWOBOYSANDAPAIROFGIRLSTHAT,THOUGHFOLKSDOSLIPFROMWHATSCRIPTURALAUTHORSCALLTHAT"STRAIGHTANDNARROWPATH,"ITWILLNOTPAYTORISKYOUROWNSOULBYSLIPPING,JUSTSOTHATYOUCANLAUGHATYOURABILITYINSTAYINGOUTOFPRISON;FORGADSBY,HAVINGGROWNUPINBRANTONHILLS,COULDPOINTTOMANYSUCHMANORWOMAN.SO,WITHSUCHFIRMCONVICTIONSINHISMIND,THISUPSTANDINGMANWASCONSTANTLYSTRIVINGSOTOACTTHATNOCOMPLAINTFROMMAN,WOMANORCHILDSHOULDBRINGAWORDOFDISAPPROVAL.INHISMIND,WHATAMANMIGHTDOWASTHATMAN'SAFFAIRONLYANDCOULDSTAINNOSOULBUTHISOWN.ANDHISALTRUISMTAUGHTTHATITISNOTDIFFICULTTOFINDMANYWAYSINWHICHTOBRINGJOYTOSUCHASCANNOT,THROUGHPHYSICALDISABILITY,GOOUTTOLOOKFORIT;ANDTHATONLYASMALLBITOFJOY,BROUGHTTOASHUT-ININVALIDWILLCARRYWITHITSUCHAWARMTHASCANFLOWONLYFROMACTSOFHUMANSYMPATHY.

**Code Used for Caesar Cipher Decryption**

Here, I used brute force to solve for the decryption. I tested every possible shift and checked to see which output coherent English words. This was a fairly straightforward decryption, and my program was able to decipher each on the first try.

**import** sys

#print the encoded file but shifted by a specified amount

**def** shift\_chars(shift, line):

alpha = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"

letters = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"

tmp = letters[:shift]

letters = letters[shift:] + tmp

**for** char **in** line:

**if** (char **not** **in** alpha):

**print**(char, end = "")

**else**:

**print**(letters[alpha.find(char)], end = "")

**print**()

#test a specific shift value

**def** test\_shift(shift):

f = open(sys.argv[1], 'r')

**for** line **in** f:

shift\_chars(shift, line.upper())

f.close()

**def** main():

shift = 0

#test every possible shift for the 26 letters

**while**(shift < 26):

**print**(" --- SHIFTED " + str(26 - shift) + " ---")

test\_shift(shift)

shift += 1

**print**()

**if** \_\_name\_\_ == '\_\_main\_\_':

main()