Vigenere Cipher

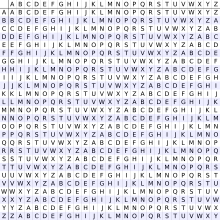
Mark Nakamae

Cal Poly SLO

June 2020

Description

This project involved deciphering ciphertexts encrypted using the Vigenere cipher algorithm described [here](https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher)**.** This is a slightly more complicated substitution encryption algorithm that replaces letters based on a key phrase. Each letter in the key phrase essentially acts as a caesar cipher key shift value in which letters are encoded accordingly:



For example, if a user wants to encrypt the phrase “ATTACKATDAWN” with the password “LEMON”, the user would look at the row with L from LEMON and the column with A from ATTACK. This gives the value of L for the cipher text. Then the user goes to row E, column T for the next letter and so on. When the user reaches the end of the keyphrase, it simply repeats itself and starts at L again. Repeating this process gives a ciphertext of “LXFOPVEFRNHR”.

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.

**vigerene\_1.txt** (key: “LEWIS”)

THE ROOM DISPLAYED A MODEST AND PLEASANT COLOR-SCHEME, AFTER ONE OF THE BEST STANDARD DESIGNS OF THE DECORATOR WHO “DID THE INTERIORS” FOR MOST OF THE SPECULATIVE-BUILDERS’ HOUSES IN ZENITH. THE WALLS WERE GRAY, THE WOODWORK WHITE, THE RUG A SERENE BLUE; AND VERY MUCH LIKE MAHOGANY WAS THE FURNITURE—THE BUREAU WITH ITS GREAT CLEAR MIRROR, MRS. BABBITT’S DRESSING-TABLE WITH TOILET-ARTICLES OF ALMOST SOLID SILVER, THE PLAIN TWIN BEDS, BETWEEN THEM A SMALL TABLE HOLDING A STANDARD ELECTRIC BEDSIDE LAMP, A GLASS FOR WATER, AND A STANDARD BEDSIDE BOOK WITH COLORED ILLUSTRATIONS—WHAT PARTICULAR BOOK IT WAS CANNOT BE ASCERTAINED, SINCE NO ONE HAD EVER OPENED IT. THE MATTRESSES WERE FIRM BUT NOT HARD, TRIUMPHANT MODERN MATTRESSES WHICH HAD COST A GREAT DEAL OF MONEY; THE HOT-WATER RADIATOR WAS OF EXACTLY THE PROPER SCIENTIFIC SURFACE FOR THE CUBIC CONTENTS OF THE ROOM. THE WINDOWS WERE LARGE AND EASILY OPENED, WITH THE BEST CATCHES AND CORDS, AND HOLLAND ROLLER-SHADES GUARANTEED NOT TO CRACK. IT WAS A MASTERPIECE AMONG BEDROOMS, RIGHT OUT OF CHEERFUL MODERN HOUSES FOR MEDIUM INCOMES. ONLY IT HAD NOTHING TO DO WITH THE BABBITTS, NOR WITH ANY ONE ELSE. IF PEOPLE HAD EVER LIVED AND LOVED HERE, READ THRILLERS AT MIDNIGHT AND LAIN IN BEAUTIFUL INDOLENCE ON A SUNDAY MORNING, THERE WERE NO SIGNS OF IT. IT HAD THE AIR OF BEING A VERY GOOD ROOM IN A VERY GOOD HOTEL. ONE EXPECTED THE CHAMBERMAID TO COME IN AND MAKE IT READY FOR PEOPLE WHO WOULD STAY BUT ONE NIGHT, GO WITHOUT LOOKING BACK, AND NEVER THINK OF IT AGAIN.

**vigerne\_2.txt** (key: “CACTACAE”)

ACANTHACEAE

ACHARIACEAE

ACHATOCARPACEAE

ACORACEAE

ACTINIDIACEAE

ADOXACEAE

AEXTOXICACEAE

AIZOACEAE

AKANIACEAE

ALISMATACEAE

ALSEUOSMIACEAE

ALSTROEMERIACEAE

ALTINGIACEAE

ALZATEACEAE

AMARANTHACEAE

AMARYLLIDACEAE

AMBORELLACEAE

ANACARDIACEAE

ANARTHRIACEAE

ANCISTROCLADACEAE

ANISOPHYLLEACEAE

ANNONACEAE

APHANOPETALACEAE

APHLOIACEAE

APIACEAE

APOCYNACEAE

APODANTHACEAE

APONOGETONACEAE

AQUIFOLIACEAE

ARACEAE

ARALIACEAE

ARECACEAE

ARGOPHYLLACEAE

ARISTOLOCHIACEAE

ASPARAGACEAE

ASTELIACEAE

ASTEROPEIACEAE

ATHEROSPERMATACEAE

AUSTROBAILEYACEAE

BALANOPACEAE

BALANOPHORACEAE

BALSAMINACEAE

BARBEUIACEAE

BARBEYACEAE

BASELLACEAE

BATACEAE

BEGONIACEAE

BERBERIDACEAE

BERBERIDOPSIDACEAE

BETULACEAE

BIEBERSTEINIACEAE

BIGNONIACEAE

BIXACEAE

BLANDFORDIACEAE

BONNETIACEAE

BORAGINACEAE

BORYACEAE

BRASSICACEAE

BROMELIACEAE

BRUNELLIACEAE

BRUNIACEAE

BURMANNIACEAE

BURSERACEAE

BUTOMACEAE

BUXACEAE

BYBLIDACEAE

CABOMBACEAE

CACTACEAE

CALCEOLARIACEAE

CALOPHYLLACEAE

CALYCANTHACEAE

CALYCERACEAE

CAMPANULACEAE

CAMPYNEUMATACEAE

CANELLACEAE

CANNABACEAE

CANNACEAE

CAPPARACEAE

CAPRIFOLIACEAE

CARDIOPTERIDACEAE

CARICACEAE

CARLEMANNIACEAE

CARYOCARACEAE

CARYOPHYLLACEAE

CASUARINACEAE

CELASTRACEAE

CENTROLEPIDACEAE

CENTROPLACACEAE

CEPHALOTACEAE

CERATOPHYLLACEAE

CERCIDIPHYLLACEAE

CHLORANTHACEAE

CHRYSOBALANACEAE

CIRCAEASTERACEAE

CISTACEAE

CLEOMACEAE

CLETHRACEAE

CLUSIACEAE

COLCHICACEAE

COLUMELLIACEAE

COMBRETACEAE

COMMELINACEAE

COMPOSITAE

CONNARACEAE

CONVOLVULACEAE

CORIARIACEAE

CORNACEAE

CORSIACEAE

CORYNOCARPACEAE

COSTACEAE

CRASSULACEAE

CROSSOSOMATACEAE

CRYPTERONIACEAE

CTENOLOPHONACEAE

CUCURBITACEAE

CUNONIACEAE

CURTISIACEAE

CYCLANTHACEAE

CYMODOCEACEAE

CYNOMORIACEAE

CYPERACEAE

CYRILLACEAE

CYTINACEAE

DAPHNIPHYLLACEAE

DASYPOGONACEAE

DATISCACEAE

DEGENERIACEAE

DIAPENSIACEAE

DICHAPETALACEAE

DIDIEREACEAE

DILLENIACEAE

DIONCOPHYLLACEAE

DIOSCOREACEAE

DIPENTODONTACEAE

DIPTEROCARPACEAE

DIRACHMACEAE

DORYANTHACEAE

DROSERACEAE

DROSOPHYLLACEAE

EBENACEAE

ECDEIOCOLEACEAE

ELAEAGNACEAE

ELAEOCARPACEAE

ELATINACEAE

EMBLINGIACEAE

ERICACEAE

ERIOCAULACEAE

ERYTHROXYLACEAE

ESCALLONIACEAE

EUCOMMIACEAE

EUPHORBIACEAE

EUPHRONIACEAE

EUPOMATIACEAE

EUPTELEACEAE

FAGACEAE

FLAGELLARIACEAE

FOUQUIERIACEAE

FRANKENIACEAE

GARRYACEAE

GEISSOLOMATACEAE

GELSEMIACEAE

GENTIANACEAE

GERANIACEAE

GESNERIACEAE

GISEKIACEAE

GOMORTEGACEAE

GOODENIACEAE

GOUPIACEAE

GRISELINIACEAE

GROSSULARIACEAE

GRUBBIACEAE

GUNNERACEAE

GYROSTEMONACEAE

HAEMODORACEAE

HALOPHYTACEAE

HALORAGACEAE

HAMAMELIDACEAE

HANGUANACEAE

HAPTANTHACEAE

HELICONIACEAE

HELWINGIACEAE

HERNANDIACEAE

HIMANTANDRACEAE

HUACEAE

HUMIRIACEAE

HYDATELLACEAE

HYDNORACEAE

HYDRANGEACEAE

HYDROCHARITACEAE

HYDROLEACEAE

HYDROSTACHYACEAE

HYPERICACEAE

HYPOXIDACEAE

ICACINACEAE

IRIDACEAE

IRVINGIACEAE

ITEACEAE

IXIOLIRIACEAE

IXONANTHACEAE

JOINVILLEACEAE

JUGLANDACEAE

JUNCACEAE

JUNCAGINACEAE

KIRKIACEAE

KOEBERLINIACEAE

KRAMERIACEAE

LACISTEMATACEAE

LACTORIDACEAE

LAMIACEAE

LANARIACEAE

LARDIZABALACEAE

LAURACEAE

LECYTHIDACEAE

LEGUMINOSAE

LENTIBULARIACEAE

LEPIDOBOTRYACEAE

LILIACEAE

LIMEACEAE

LIMNANTHACEAE

LINACEAE

LINDERNIACEAE

LOASACEAE

LOGANIACEAE

LOPHIOCARPACEAE

LORANTHACEAE

LOWIACEAE

LYTHRACEAE

MAGNOLIACEAE

MALPIGHIACEAE

MALVACEAE

MARANTACEAE

MARCGRAVIACEAE

MARTYNIACEAE

MAYACACEAE

MELANTHIACEAE

MELASTOMATACEAE

MELIACEAE

MELIANTHACEAE

MENISPERMACEAE

MENYANTHACEAE

METTENIUSACEAE

MISODENDRACEAE

MITRASTEMONACEAE

MOLLUGINACEAE

MONIMIACEAE

MONTIACEAE

MONTINIACEAE

MORACEAE

MORINGACEAE

MUNTINGIACEAE

MUSACEAE

MYODOCARPACEAE

MYRICACEAE

MYRISTICACEAE

MYROTHAMNACEAE

MYRTACEAE

NARTHECIACEAE

NELUMBONACEAE

NEPENTHACEAE

NEURADACEAE

NITRARIACEAE

NOTHOFAGACEAE

NYCTAGINACEAE

NYMPHAEACEAE

OCHNACEAE

OLACACEAE

OLEACEAE

ONAGRACEAE

ONCOTHECACEAE

OPILIACEAE

ORCHIDACEAE

OROBANCHACEAE

OXALIDACEAE

PAEONIACEAE

PANDACEAE

PANDANACEAE

PAPAVERACEAE

PARACRYPHIACEAE

PASSIFLORACEAE

PAULOWNIACEAE

PEDALIACEAE

PENAEACEAE

PENTADIPLANDRACEAE

PENTAPHRAGMATACEAE

PENTAPHYLACACEAE

PENTHORACEAE

PERACEAE

PERIDISCACEAE

PETERMANNIACEAE

PETROSAVIACEAE

PHILESIACEAE

PHILYDRACEAE

PHRYMACEAE

PHYLLANTHACEAE

PHYLLONOMACEAE

PHYSENACEAE

PHYTOLACCACEAE

PICRAMNIACEAE

PICRODENDRACEAE

PIPERACEAE

PITTOSPORACEAE

PLANTAGINACEAE

PLATANACEAE

PLOCOSPERMATACEAE

PLUMBAGINACEAE

POACEAE

PODOSTEMACEAE

POLEMONIACEAE

POLYGALACEAE

POLYGONACEAE

PONTEDERIACEAE

PORTULACACEAE

POSIDONIACEAE

POTAMOGETONACEAE

PRIMULACEAE

PROTEACEAE

PUTRANJIVACEAE

QUILLAJACEAE

RAFFLESIACEAE

RANUNCULACEAE

RAPATEACEAE

RESEDACEAE

RESTIONACEAE

RHABDODENDRACEAE

RHAMNACEAE

RHIPOGONACEAE

RHIZOPHORACEAE

RORIDULACEAE

ROSACEAE

ROUSSEACEAE

RUBIACEAE

RUPPIACEAE

RUTACEAE

SABIACEAE

SALICACEAE

SALVADORACEAE

SANTALACEAE

SAPINDACEAE

SAPOTACEAE

SARCOBATACEAE

SARCOLAENACEAE

SARRACENIACEAE

SAURURACEAE

SAXIFRAGACEAE

SCHEUCHZERIACEAE

SCHISANDRACEAE

SCHLEGELIACEAE

SCHOEPFIACEAE

SCROPHULARIACEAE

SETCHELLANTHACEAE

SIMAROUBACEAE

SIMMONDSIACEAE

SIPARUNACEAE

SLADENIACEAE

SMILACACEAE

SOLANACEAE

SPHAEROSEPALACEAE

SPHENOCLEACEAE

STACHYURACEAE

STAPHYLEACEAE

STEGNOSPERMATACEAE

STEMONACEAE

STEMONURACEAE

STILBACEAE

STRASBURGERIACEAE

STRELITZIACEAE

STYLIDIACEAE

STYRACACEAE

SURIANACEAE

SYMPLOCACEAE

TALINACEAE

TAMARICACEAE

TAPISCIACEAE

TECOPHILAEACEAE

TETRACHONDRACEAE

TETRAMELACEAE

TETRAMERISTACEAE

THEACEAE

THOMANDERSIACEAE

THURNIACEAE

THYMELAEACEAE

TICODENDRACEAE

TOFIELDIACEAE

TORRICELLIACEAE

TOVARIACEAE

TRIGONIACEAE

TRIURIDACEAE

TROCHODENDRACEAE

TROPAEOLACEAE

TYPHACEAE

ULMACEAE

URTICACEAE

VAHLIACEAE

VELLOZIACEAE

VERBENACEAE

VIOLACEAE

VITACEAE

VIVIANIACEAE

VOCHYSIACEAE

WINTERACEAE

XANTHORRHOEACEAE

XERONEMATACEAE

XYRIDACEAE

ZINGIBERACEAE

ZOSTERACEAE

ZYGOPHYLLACEAE

**vigerne\_3.txt** (key: “SNARKSAREREAL”)

THEBELLMAN’SSPEECH

THEBELLMANHIMSELFTHEYALLPRAISEDTOTHESKIES—

SUCHACARRIAGE,SUCHEASEANDSUCHGRACE!

SUCHSOLEMNITY,TOO!ONECOULDSEEHEWASWISE,

THEMOMENTONELOOKEDINHISFACE!

HEHADBOUGHTALARGEMAPREPRESENTINGTHESEA,

WITHOUTTHELEASTVESTIGEOFLAND:

ANDTHECREWWEREMUCHPLEASEDWHENTHEYFOUNDITTOBE

AMAPTHEYCOULDALLUNDERSTAND.

“WHAT’STHEGOODOFMERCATOR’SNORTHPOLESANDEQUATORS,

TROPICS,ZONES,ANDMERIDIANLINES?”

SOTHEBELLMANWOULDCRY:ANDTHECREWWOULDREPLY

“THEYAREMERELYCONVENTIONALSIGNS!

“OTHERMAPSARESUCHSHAPES,WITHTHEIRISLANDSANDCAPES!

BUTWE’VEGOTOURBRAVECAPTAINTOTHANK:”

(SOTHECREWWOULDPROTEST)“THATHE’SBOUGHTUSTHEBEST—

APERFECTANDABSOLUTEBLANK!”

THISWASCHARMING,NODOUBT;BUTTHEYSHORTLYFOUNDOUT

THATTHECAPTAINTHEYTRUSTEDSOWELL

HADONLYONENOTIONFORCROSSINGTHEOCEAN,

ANDTHATWASTOTINGLEHISBELL.

HEWASTHOUGHTFULANDGRAVE—BUTTHEORDERSHEGAVE

WEREENOUGHTOBEWILDERACREW.

WHENHECRIED“STEERTOSTARBOARD,BUTKEEPHERHEADLARBOARD!”

WHATONEARTHWASTHEHELMSMANTODO?

THENTHEBOWSPRITGOTMIXEDWITHTHERUDDERSOMETIMES:

ATHING,ASTHEBELLMANREMARKED,

THATFREQUENTLYHAPPENSINTROPICALCLIMES,

WHENAVESSELIS,SOTOSPEAK,“SNARKED.”

BUTTHEPRINCIPALFAILINGOCCURREDINTHESAILING,

ANDTHEBELLMAN,PERPLEXEDANDDISTRESSED,

SAIDHEHADHOPED,ATLEAST,WHENTHEWINDBLEWDUEEAST,

THATTHESHIPWOULDNOTTRAVELDUEWEST!

BUTTHEDANGERWASPAST—THEYHADLANDEDATLAST,

WITHTHEIRBOXES,PORTMANTEAUS,ANDBAGS:

YETATFIRSTSIGHTTHECREWWERENOTPLEASEDWITHTHEVIEW,

WHICHCONSISTEDOFCHASMSANDCRAGS.

THEBELLMANPERCEIVEDTHATTHEIRSPIRITSWERELOW,

ANDREPEATEDINMUSICALTONE

SOMEJOKESHEHADKEPTFORASEASONOFWOE—

BUTTHECREWWOULDDONOTHINGBUTGROAN.

HESERVEDOUTSOMEGROGWITHALIBERALHAND,

ANDBADETHEMSITDOWNONTHEBEACH:

ANDTHEYCOULDNOTBUTOWNTHATTHEIRCAPTAINLOOKEDGRAND,

ASHESTOODANDDELIVEREDHISSPEECH.

“FRIENDS,ROMANS,ANDCOUNTRYMEN,LENDMEYOUREARS!”

(THEYWEREALLOFTHEMFONDOFQUOTATIONS:

SOTHEYDRANKTOHISHEALTH,ANDTHEYGAVEHIMTHREECHEERS,

WHILEHESERVEDOUTADDITIONALRATIONS).

“WEHAVESAILEDMANYMONTHS,WEHAVESAILEDMANYWEEKS,

(FOURWEEKSTOTHEMONTHYOUMAYMARK),

BUTNEVERASYET(‘TISYOURCAPTAINWHOSPEAKS)

HAVEWECAUGHTTHELEASTGLIMPSEOFASNARK!

“WEHAVESAILEDMANYWEEKS,WEHAVESAILEDMANYDAYS,

(SEVENDAYSTOTHEWEEKIALLOW),

BUTASNARK,ONTHEWHICHWEMIGHTLOVINGLYGAZE,

WEHAVENEVERBEHELDTILLNOW!

“COME,LISTEN,MYMEN,WHILEITELLYOUAGAIN

THEFIVEUNMISTAKABLEMARKS

BYWHICHYOUMAYKNOW,WHERESOEVERYOUGO,

THEWARRANTEDGENUINESNARKS.

“LETUSTAKETHEMINORDER.THEFIRSTISTHETASTE,

WHICHISMEAGREANDHOLLOW,BUTCRISP:

LIKEACOATTHATISRATHERTOOTIGHTINTHEWAIST,

WITHAFLAVOUROFWILL-O’-THE-WISP.

“ITSHABITOFGETTINGUPLATEYOU’LLAGREE

THATITCARRIESTOOFAR,WHENISAY

THATITFREQUENTLYBREAKFASTSATFIVE-O’CLOCKTEA,

ANDDINESONTHEFOLLOWINGDAY.

“THETHIRDISITSSLOWNESSINTAKINGAJEST.

SHOULDYOUHAPPENTOVENTUREONONE,

ITWILLSIGHLIKEATHINGTHATISDEEPLYDISTRESSED:

ANDITALWAYSLOOKSGRAVEATAPUN.

“THEFOURTHISITSFONDNESSFORBATHING-MACHINES,

WHICHISCONSTANTLYCARRIESABOUT,

ANDBELIEVESTHATTHEYADDTOTHEBEAUTYOFSCENES—

ASENTIMENTOPENTODOUBT.

“THEFIFTHISAMBITION.ITNEXTWILLBERIGHT

TODESCRIBEEACHPARTICULARBATCH:

DISTINGUISHINGTHOSETHATHAVEFEATHERS,ANDBITE,

ANDTHOSETHATHAVEWHISKERS,ANDSCRATCH.

“FOR,ALTHOUGHCOMMONSNARKSDONOMANNEROFHARM,

YET,IFEELITMYDUTYTOSAY,

SOMEAREBOOJUMS—”THEBELLMANBROKEOFFINALARM,

FORTHEBAKERHADFAINTEDAWAY.

**Code Used for Vigenere Decryption**

I first started by separating the characters into groups based on how long the given key length was. For example, a key length of 5 had 5 different groups of characters. One group would have the characters located at 0, 5, 10, 15, etc. After splitting up the groups, I calculated the frequency of each character in each group. I would then do matrix multiplication between the actual character frequency, and the expected character frequency, which I found from Wikipedia.

After completing this multiplication, I would then shift the array of actual frequencies so the first item would now be the last item. I then did the same matrix multiplication, summed the results of this multiplication, and kept track of which shift had the largest sum. The shift with the largest sum represented the letter most likely used to encode this group.

I performed this multiplication for each separate group, and found the letter most likely for each position in the key word. I then tested this keyword by decrypting the original text file, which output the correct plain text file for each file.

A particularly useful video explaining this process further: <https://www.youtube.com/watch?v=LaWp_Kq0cKs&t=884s>

I made the font smaller so the code would maintain its formatting.

**import** sys

**import** itertools

#generate a list of strings built from the input encoded file. the groups are built

#based on each chars position in the file

**def** get\_groups(num\_groups):

alpha = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"

lower = "abcdefghijklmnopqrstuvwxyz"

groups = ["" **for** x **in** range(num\_groups)]

**for** group **in** range(num\_groups):

count = 0

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

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

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

**if** (char **in** alpha **or** char **in** lower):

**if** (count == group):

groups[group] += char.upper()

count += 1

**if** (count == num\_groups):

count = 0

f.close()

**return** groups

#given a key, find the corresponding decoded character

**def** find\_char(key\_char, char):

alpha = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"

letters = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"

tmp = letters[:alpha.find(key\_char)]

letters = letters[alpha.find(key\_char):] + tmp

**return**(alpha[letters.find(char)])

#given a key, print the decoded message from the input text file

**def** print\_decoded(key):

alpha = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"

decoded = ""

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

i = 0

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

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

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

decoded += char

**else**:

decoded += find\_char(key[i], char.upper())

i += 1

**if** (i >= len(key)):

i = 0

f.close()

**print**(decoded)

**def** main():

alpha = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"

expect = [8.12, 1.49, 2.71, 4.32, 12.02, 2.30, 2.03, 5.92, 7.31, 0.10, 0.69, 3.98, 2.61,\

6.95, 7.68, 1.82, 0.11, 6.02, 6.28, 9.10, 2.88, 1.11, 2.09, 0.17, 2.11, 0.07]

valid\_keys = []

guess = ""

keylen = 0

**if**("vigerene\_easy\_encrypted.txt" **in** sys.argv[1]):

keylen = 5

**elif**("vigerne\_medium\_encrypt.txt" **in** sys.argv[1]):

keylen = 9

**elif**("vigerene\_hard\_encrypt.txt" **in** sys.argv[1]):

keylen = 13

test = ""

test\_name = ""

actual = [[[0.0 **for** x **in** range(26)] **for** y **in** range(26)] **for** z **in** range(keylen)]

#separate input text into groups of letters based on their positions

groups = get\_groups(keylen)

#generate an array containing the frequency of each character in the groups

**for** group\_num **in** range(keylen):

letters = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"

**for** shift\_val **in** range(0, 26):

**for** char **in** groups[group\_num]:

actual[group\_num][shift\_val][letters.find(char)] += 100.0 / len(groups[group\_num])

letters = letters[1:] + letters[0]

#find the most probable key value

**for** group\_num **in** range(keylen):

largest = 0

largest\_idx = 0

**for** shift\_val **in** range(26):

#key with largest probability value is most likely the correct key

probability = 0

**for** idx **in** range(26):

probability += actual[group\_num][shift\_val][idx] \* expect[idx]

**if**(probability > largest):

largest = probability

largest\_idx = shift\_val

#add letter to the test key

test\_name += alpha[largest\_idx - 1]

test += alpha[largest\_idx]

#test the key

**print**("------------ " + test\_name + " ------------")

print\_decoded(test)

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

main()