Use your preferred tools and crack the following ciphers:

1. **WottwfahvohWwadzsasbhsrhvsqcrspmamgsztkwhvcihqcdmwbuobslhsfbozdfcxsqhtfcahvswbhsfbshcftfcaamqczzsouisgobrWhchozzmybckhvohamgipawggwcbkwzzuchvfciuvodzouwofwgaqvsqyWtwhwgdfcjsbhvohhvsqcrswgqcdwsrtfcaobmdzoqshvwggipawggwcbkwzzpsqcbgwrsfsrogotowzsrgipawggwcb**

First, simple checks to know cipher type:

- Alphabet: English lowercase alphabet (26 letters) with exception of uppercase ‘W’,
- No white spaces, numbers or special characters,

So, it is most likely a substitution cipher, so it is suitable to try simple (low-complexity analysis) types of substitution ciphers like Caesar cipher, monoalphabetic substitution cipher, then trying more complex types like Vigenère cipher, etc.

First try: Caesar (shift) cipher:

I have implemented an algorithm (using Python) to try to solve Caesar ciphers, which can be found on my GitHub repo following this link: https://git.io/JOgdK - which consists of the following steps:

1) Load the cipher and make it all lowercase.
2) Create a list of the alphabet sorted by their frequency in English texts.
3) Get a list of the alphabet sorted by their frequency in the cipher.
4) Compare the output lists of (2) and (3) and find the element-wise ‘ASCII difference’ between the two lists.
5) Pop the most frequent difference in the output list of (4) and assign it to the key variable.
6) Try to solve the cipher (unshift) with that key.
7) If cipher solved, then finish; else, jump to step (4).

Which from the first try, at step (5), gave the difference of 14 as the most frequent, which is the key that solved the cipher, resulting the following output:

```
iaffirmthatiimplementedthecodebymyselfwithoutcopyinganexternalprojectfromthei
nternetorfrommycolleaguesanditotallyknowthatmysubmissionwillgothroughaplagiar
ismcheckifitisproventhatthecodeiscopiedfromanyplacethissubmissionwillbeconsid
eredasafailedsubmission
```

When formatted properly:

```
I affirm that I implemented the code by myself without copying an external
project from the internet or from my colleagues and I totally know that my
submission will go through a plagiarism check if it is proven that the code
is copied from any place this submission will be considered as a failed
submission.
```

2. **SW50aGlzcHJvamVjdCx5b3VoYXZldG9pbXBsZW1lbnRvbmVvZnRoZXByb2plY3RpZGVhc2Rpc2N1c3NlZGJlbG93dXNpbmdUaXZhLUNzaW11bGF0b3JvbktlaWxhbmR5b3V3aWxsYWxzb2hhdmV0b3dyaXRlYXRob3JvdWdoZGVzY3JpcHRpb25vZnlvdXJjaG9zZW5wcm9qZWN0VGhlcHJvamVjdGlzaW1wbGVtZW50ZWRvbmFuaW5kaXZpZHVhbGJhc2lz**

First, simple checks to know cipher type:

- Alphabet: English alphabet (both lowercase and uppercase) and digits.
- No white spaces or special characters,

So, it is most likely a base64 cipher.

First try: Base64 cipher:

I have implemented a simple program (using Python) to decrypt Base64 ciphers using the Python `base64` library, which can be found on my GitHub repo following this link: https://git.io/JOgxM

When given this cipher, resulted the following output:

```
Inthisproject,youhavetoimplementoneoftheprojectideasdiscussedbelowusingTiva-C
simulatoronKeilandyouwillalsohavetowriteathoroughdescriptionofyourchosenproje
ctTheprojectisimplementedonanindividualbasis
```

When formatted properly:

```
In this project, you have to implement one of the project ideas discussed
below using Tiva-C simulator on Keil and you will also have to write
a thorough description of your chosen project The project is implemented on
an individual basis.
```

3. **FTQ IADP "ODKBFASDMBTK" UE PQDUHQP RDAY FTQ SDQQW WDKBFAE, YQMZUZS TUPPQZ. FTQ ADUSUZ AR ODKBFASDMBTK UE GEGMXXK PMFQP RDAY MNAGF 2000 N.O., IUFT FTQ QSKBFUMZ BDMOFUOQ AR TUQDASXKBTUOE. FTQEQ OAZEUEFQP AR OAYBXQJ BUOFASDMYE, FTQ RGXX YQMZUZS AR ITUOT IME AZXK WZAIZ FA MZ QXUFQ RQI. FTQ RUDEF WZAIZ GEQ AR M YAPQDZ OUBTQD IME NK VGXUGE OMQEMD (100 N.O. FA 44 N.O.), ITA PUP ZAF FDGEF TUE YQEEQZSQDE ITQZ OAYYGZUOMFUZS IUFT TUE SAHQDZADE MZP ARRUOQDE. RAD FTUE DQMEAZ, TQ ODQMFQP M EKEFQY UZ ITUOT QMOT OTMDMOFQD UZ TUE YQEEMSQE IME DQBXMOQP NK M OTMDMOFQD FTDQQ BAEUFUAZE MTQMP AR UF UZ FTQ DAYMZ MXBTMNQF. UZ DQOQZF FUYQE, ODKBFASDMBTK TME FGDZQP UZFA M NMFFXQSDAGZP AR EAYQ AR FTQ IADXP'E NQEF YMFTQYMFUOUMZE MZP OAYBGFQD EOUQZFUEFE. FTQ MNUXUFK FA EQOGDQXK EFADQ MZP FDMZERQD EQZEUFUHQ UZRADYMFUAZ TME BDAHQP M ODUFUOMX RMOFAD UZ EGOOQEE UZ IMD MZP NGEUZQEE. NQOMGEQ SAHQDZYQZFE PA ZAF IUET OQDFMUZ QZFUFUQE UZ MZP AGF AR FTQUD OAGZFDUQE FA TMHQ MOOQEE FA IMKE FA DQOQUHQ MZP EQZP TUPPQZ UZRADYMFUAZ FTMF YMK NQ M FTDQMF FA ZMFUAZMX UZFQDQEFE, ODKBFASDMBTK TME NQQZ EGNVQOF FA HMDUAGE DQEFDUOFUAZE UZ YMZK OAGZFDUQE, DMZSUZS RDAY XUYUFMFUAZE AR FTQ GEMSQ MZP QJBADF AR EARFIMDQ FA FTQ BGNXUO PUEEQYUZMFUAZ AR YMFTQYMFUOMX OAZOQBFE FTMF OAGXP NQ GEQP FA PQHQXAB ODKBFAEKEFQYE. TAIQHQD, FTQ UZFQDZQF TME MXXAIQP FTQ EBDQMP AR BAIQDRGX BDASDMYE MZP, YADQ UYBADFMZFXK, FTQ GZPQDXKUZS FQOTZUCGQE AR ODKBFASDMBTK, EA FTMF FAPMK YMZK AR FTQ YAEF MPHMZOQP ODKBFAEKEFQYE MZP UPQME MDQ ZAI UZ FTQ BGNXUO PAYMUZ**

First, simple checks to know cipher type:

- Alphabet: English uppercase alphabet (26 letters).
- There are numbers, white spaces and special characters (parentheses, square brackets and quotations) which seem just in place (not part of the encoded cipher) so we will skip them in decryption process.

So, just like the first cipher in the assignment, it is most likely a substitution cipher, so it is suitable to try using the same algorithm to try solving it as Caesar cipher then moving to other types of ciphers like monoalphabetic substitution cipher, Vigenère cipher, etc.

The algorithm can be found on my GitHub repo following this link: https://git.io/JOgdK containing this cipher in an unactive (unrun) cell. Running the cell would load the cipher into the program and convert it into a lowercase string since the cipher is all uppercase and the case would not make a big difference in such case.

First try: Caesar (shift) cipher:

Running the algorithm on this cipher gave the difference of 12 as the most frequent, which is the key that solved the cipher, resulting the following output:

```
the word "cryptography" is derived from the greek kryptos, meaning hidden. the origin of cryptography is usually dated from about 2000 b.c., with the egyptian practice of hieroglyphics. these consisted of complex pictograms, the full meaning of which was only known to an elite few. the first known use of a modern cipher was by julius caesar (100 b.c. to 44 b.c.), who did not trust his messengers when communicating with his governors and officers. for this reason, he created a system in which each character in his messages was replaced by a character three positions ahead of it in the roman alphabet. in recent times, cryptography has turned into a battleground of some of the world\'s best mathematicians and computer scientists. the ability to securely store and transfer sensitive information has proved a critical factor in success in war and business. because governments do not wish certain entities in and out of their countries to have access to ways to receive and send hidden information that may be a threat to national interests, cryptography has been subject to various restrictions in many countries, ranging from limitations of the usage and export of software to the public dissemination of mathematical concepts that could be used to develop cryptosystems. however, the internet has allowed the spread of powerful programs and, more importantly, the underlying techniques of cryptography, so that today many of the most advanced cryptosystems and ideas are now in the public domain
```

4. **VoyfmWchasfpgozsfpsgvtgljsutouhozmbvjssgkywhasbimPywhpgvhihocf,Q.Y.Fvkzpbu.Avsucjlzgjvfvbwjzsavsswjlgcmomvibnkwgofk,VoyfmWchasf,hbrowgmfwlbrzVsyawvbsNfouusyobkFcuKshgzlm,oszcmkvvaoysgairlbhzohOcudofagGjvcvzcmKwaqvjfomhourKpnoyrff.HvlaopbgacffofjqcuqsybgOofym'gzhfbuussonowughScfkJcsrstcfa,orhfydwnhfrdvcpbhlbrzhcisqvaspaavfhhz,ccsfavfvkhoskpnoyruvjsybwuupvrmrbcdbozhvlAwuwgafmvtAhuwjobkgiixinohlozskwgofkgourAbuussg(ucbtoupqosdsvdzl).Gwuqsavsyszloglctavsmwfzhbvjss,VoyfmWchasfhbravsWvwscgvdvlf'gZhcus,cu26Xius1997,hospvcyzvocstvibkwatsbzsdvdisofphm,wcgphwcsfljwlkg,hbrjcatsfjwosgijqszgkvfzkkwks.Hosmoojlohafojhskokprshrishobrwlbqlogdszsogfciuusyfshrsygouroyscmhsuqcugwksflrqvfblfgacblgcmacksfumcbbuhrishzphsyohbfs.**
[2]HgcmTsifihfm2018,avsiccrgvhjszczkacyshoob500twzswcuqcwwszkcyzrdwrl,aorwbnhvlahosplghzszswbnpcvyglfwlgwuvwzhcym,ourvhjsissuhfhbgsohlrwuhclwuohmsobnionsg.
[3]Avssogatcbfpvcyzqcugsjihpjssmglhflqcyrghghosthghlghzszswbnpcvygpbvpghvfm,dwhohvltwuozpbgaoztsbagsszwuufviuozmlzscsbtwzswcuqcwwszwbavsBbwasrZhoasgdwhowbaksuhm-mciyvcbfgvtwagflzshgs.

First, simple checks to know cipher type:

- Alphabet: English alphabet (26 letters) all lowercase except for few, which seem like they are made uppercase for punctuation so the case may be neglected.
- No white spaces.
- There are numbers and special characters (parentheses, square brackets, minus signs, dots and commas) which seem just in place (not part of the encoded cipher) so we will skip them in decryption process.

So, it is most likely a substitution cipher, so it is suitable to try simple (low-complexity analysis) types of substitution ciphers like Caesar cipher, monoalphabetic substitution cipher, then trying more complex types like Vigenère cipher, etc.

First try: Caesar (shift) cipher: failed to get any reasonable output.

Used the same algorithm developed before, and for all the possible 26 keys, there were no reasonable output, but when using the suggested key 14 (letter ‘o’) to decrypt the message, the output seemed to be closer to a plain text, that output is as the following:

```
hakryiotmerbsalerbeshfsxvegfagtalynhveeswkitmenuybkitbshtutaor,c.k.rhwlbng.mh
egovxlsvhrhnivlemheeivxsoyayhunzwisarw,hakryiotmer,tndaisyrixndlhekmihnezragg
ekanwrogwetslxy,aeloywhhmakesmudxntlataogparmssvhohloywimchvraytagdwbzakdrr.t
hxmabnsmorrarvcogceknsaarky'sltrnggeeazaigsteorwvoedeform,adtrkpiztrdphobntxn
dltouechmebmmhrttl,ooermhrhwtaewbzakdghvekniggbhdydnopnalthxmigismryhfmtgivan
wsuujuzatxalewisarwsagdmnggees(gonfagbcaepehplx).sigcemhekelxasxofmheyirltnhv
ee,hakryiotmertndmheihieoshphxr'sltoge,og26juge1997,taebhoklhaoefhunwimfenlep
hpuearbty,iosbtioerxvixws,tndvomferviaesuvcelswhrlwwiwe.taeyaavxatmravtewawbd
etduetandixncxaspeleasrouggekretdeksagdakeoytegcogsiwerxdchrnxrsmonxsoymowerg
yonngtduetlbtekatnre.[2]tsoyfeurutry2018,mheuoodshtvelolwmoketaan500fileiogco
iielwokldpidx,madinzthxmtaebxstleleinzbohksxrixsighiltoky,agdhtveueegtrtnseat
xdigtoxigatyeanzuazes.[3]mheeasmfonrbhoklcogsevutbveeysxtrxcokdststaeftstxstl
eleinzbohksbnhbsthry,pitathxfigalbnsmalfenmseeliggrhugalyxleoenfileiogcoiieli
nmhennimedltamespitainmwegty-youkhonrshfimsrxletse.
```

It can be clearly noticed that a substring like “hakry” may be expressing “harry”, and a substring like “juge” may be expressing “June”, and another substring like “feurutry” may be expressing “February”.

From the observed pattern, it can be deduced that for each three consecutive letters, two of them are decrypted properly and one is decrypted poorly.

That suggests that the cipher is a Vigenère cipher with key length of 3 and the first two letters in the key are ‘oo’.

Second try: Vigenère cipher:

I have implemented an algorithm (using Python) to try to solve Vigenère ciphers given the key size as an input, which can be found on my GitHub repo following this link: https://git.io/JO2TZ - and it is very similar to the Caesar cipher algorithm except that it slices the input cipher (character by character) to number of parts equal to the key size, then running the same shift guessing algorithm for each part resulting a possible key.

At the first try, the algorithm suggested the key ‘oor’ -which matches the guess that was made above about the first two letters of the key being ‘oo’- that gave the following output:

```
hahryfotjerysaieryesefsuvedfadtaiynevebswhitjenrybhityshqutxor,z.k.rewlyng.jh
edovulsshrenislejhebivusovayeunwwipart,hahryfotjer,qndxisvriundihehmienewradg
ehantrodweqsluy,ablovwhemahesjuduntiatxogmarjssshoelovwijchsravtaddwyzahdro.t
humaynsjoroarscodcehnsxarhy'sitrkggbeawaidstbortvobdecorj,adqrkmizqrdmhoyntun
ditorecemeymmertql,olerjhrewtxewyzahdgevehnidgbedyanomnaithumidisjryefmqgisan
tsurjuwatualbwipartsaddmkggbes(doncagycabpeeplu).sidcejheheluasuofjheviritnev
eb,hahryfotjerqndjhefhibosephur'sitode,od26jude1997,txebeokihalefeuntimceniep
epubaryty,fosytileruviuws,qndsomcersiabsusceiswerltwite.txeyxavuatjrastetawyd
eqdubtakdiuncuasmelbasooudgehreqdehsaddaheovtedcodsiterudcernursjonusovmoterd
yokngqdubtlytehatkre.[2]qsovferruqry2018,jherooashqveioltmohetxan500cilbiodco
fieiwohldmidu,maainwthumtxebustielbinwboeksuriusidhiitohy,addhqvereedtrqnsbat
udidtouigxtybanwuawes.[3]jhebasjfokrbeokicodsesutyvebysutrucohdsqstxefqstusti
elbinwboeksynhystery,mitxthufidalynsjalcenjseblidgreugxlyulelencilbiodcofieii
njheknijeditajesmitxinjwedty-vouhhokrsefijsruleqse.
```

Which is still a non-reasonable output, but being nearly sure that the first two letters are ‘oo’ gave a small key space to search in, looping for the all 26 lowercase letters to be the third letter in the key ‘oo_‘ and manually observing the results since they are limited to 26 paragraphs.

There is also another solution which is more analytic: to try to figure out the third letter in the key by getting the difference in ASCII value between the expected letters and the corresponding letters in the encrypted cipher.

Both solutions are affordable and both lead to guessing the third letter as ‘h’, thus the suggested key is ‘ooh’.

Decrypting the cypher with it gave the following output:

```
harrypotterisaseriesofsevenfantasynovelswrittenbybritishauthor,j.k.rowling.th
enovelschroniclethelivesofayoungwizard,harrypotter,andhisfriendshermionegrang
erandronweasley,allofwhomarestudentsathogwartsschoolofwitchcraftandwizardry.t
hemainstoryarcconcernsharry'sstruggleagainstlordvoldemort,adarkwizardwhointen
dstobecomeimmortal,overthrowthewizardgoverningbodyknownastheministryofmagican
dsubjugateallwizardsandmuggles(nonmagicalpeople).sincethereleaseofthefirstnov
el,harrypotterandthephilosopher'sstone,on26june1997,thebookshavefoundimmensep
opularity,positivereviews,andcommercialsuccessworldwide.theyhaveattractedawid
eadultaudienceaswellasyoungerreadersandareoftenconsideredcornerstonesofmodern
youngadultliterature.[2]asoffebruary2018,thebookshavesoldmorethan500millionco
piesworldwide,makingthemthebestsellingbookseriesinhistory,andhavebeentranslat
edintoeightylanguages.[3]thelastfourbooksconsecutivelysetrecordsasthefastests
ellingbooksinhistory,withthefinalinstalmentsellingroughlyelevenmillioncopiesi
ntheunitedstateswithintwenty-fourhoursofitsrelease.
```

When formatted properly:

harry potter is a series of seven fantasy novels written by british author, j.k.rowling. the novels chronicle the lives of a young wizard, harry potter, and his friends hermione granger and ron weasley, all of whom are students at Hogwarts school of witchcraft and wizardry. the main story arc concerns harry's struggle against lord voldemort, a dark wizard who intends to become immortal, over throw the wizard governing body known as the ministry of magic and subjugate all wizards and muggles (non-magical people). since the release of the first novel, harry potter and the philosopher's stone, on 26 june 1997, the book shave found immense popularity, positive reviews, and commercial success worldwide. they have attracted a wide adult audience as well as younger readers and are often considered cornerstones of modern young adult literature.

[2] as of February 2018, the book shaves old more than 500 million copies worldwide, making them the bestselling book series in history, and have been translated into eighty languages.

[3] the last four books consecutively set records as the fastest selling books in history, with the final instalment selling roughly eleven million copies in the united states within twenty-four hours of its release.