HOMEWORK-1

Şeyma ÇALIŞKAN

Intern at GSTL

AUTOKEY CHIPHER- Working Principle

The Autokey cipher is a polyalphabetic substitution cipher that shares similarities with the **Vigenère cipher**, but with a crucial difference: instead of using a repeating keyword, it extends the key by appending the **plaintext itself** to the initial keyword.

Encryption Process:

1. The encryption begins with a predefined **keyword**.
2. This keyword is followed by the **plaintext** itself to form a full-length key.
3. Encryption is performed character by character using the Vigenère table:

$$C_i = (P_i + K_i) \mod 26$$

Decryption Process:

- In decryption, the key is reconstructed progressively: it begins with the known keyword and then uses **each newly decrypted character** to rebuild the rest of the key.
- The initial characters are decrypted using the keyword, and subsequent decrypted characters are appended to the key to continue the decryption process.

This method addresses the repetition problem present in classical Vigenère ciphers and makes the cipher more resistant to certain cryptanalytic attacks. However, once the initial part of the key (i.e., the keyword) is discovered, the rest of the key can be derived from the recovered plaintext, making the cipher vulnerable under certain conditions.

The Autokey cipher uses the following tableau (the 'tabula recta') to encipher the plaintext:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

1) In the first task, a ciphertext-only attack is carried out on the autokey cipher. Since the key in the autokey cipher is non-repeating, traditional cryptanalytic techniques such as the Kasiski examination and the Index of Coincidence are not suitable. Instead, statistical language models based on English n-gram frequencies are utilized to infer both the encryption key and the corresponding plaintext. The English trigram and quadgram frequency tables used in scoring are provided in the Crypto Corner website.

The decryption process begins by generating a random three-letter candidate key. The ciphertext is decrypted using this key, and the resulting plaintext is evaluated by a fitness function that calculates a score based on the occurrence of valid English trigrams or quadgrams. A higher score suggests a greater likelihood that the resulting plaintext is linguistically meaningful. This process is repeated 150 times with different candidate keys in order to explore a broader solution space and identify the most probable plaintext. All scores are stored in an array, and the key that yields the plaintext with the highest fitness score is selected and displayed.

As neither the original key length nor the plaintext is known in a ciphertext-only scenario, the algorithm is designed to iterate over different key lengths and apply the same scoring mechanism to each candidate decryption.

Upon execution of the algorithm on the given ciphertext, a coherent and meaningful English plaintext was recovered. The corresponding encryption key was identified as **"OLIVER"**, and the final output was printed to the terminal.

Subsequently, a known-plaintext attack—where both the ciphertext and the corresponding plaintext are known—was also attempted to recover the key. However, since Section A has already successfully completed the task, this additional step was deemed unnecessary.

The terminal output is shown below:

```
-20516.2029177954 autokey, klen 6 :"OLIVER", TREATSOFTHEPLACEWHEREOLIVERTWISTWASBORNANDOFTHECIRCUMSTANCESATTENDINGHISBIRTHAMONGOTHER
PUBLICBUILDINGSINACERTAINTOWNWHICHFORMANYREASONSITWILLBEPRUDENTTOREFRAINFROMMENTIONINGANDTOWHICHIWILLASSIGNNOFICTITIOUSNAMETHEREISON
EANCIENTLYCOMMONTOMOSTTOWNSGREATORSMALLTOWITAWORKHOUSEANDINTHISWORKHOUSEWASBORNONADAYANDDATEWHICHINEEDNOTTROUBLEMYSELFTOREPEATINASMU
CHASITCANBEOFNOPOSSIBLECONSEQUENCETOTHEREADERINTHISSTAGEOFTHEBUSINESSATALLEVENTSTHEITEMOFMORTALITYWHOSENAMEISPREFIXEDTOTHEHEADOFTHIS
CHAPTERFORALONGTIMEAFTERITWASUSHEREDINTOTHISWORLDOFSORROWANDTROUBLEBYTHEPARISHSURGEONITREMAINEDAMATTEROFCONSIDERABLEDOUBTWHETHERTHEC
HILDWOULDSURVIVETOBEARANYNAMEATALLINWHICHCASEITISSOMEWHATMORETHANPROBABLETHATTHESEMEMOIRSWOULDNEVERHAVEAPPEAREDORIFTHEYHADTHATBEINGC
OMPRISEDWITHINACOUPLEOFPAGESTHEYWOULDHAVEPOSSESSEDTHEINESTIMABLEMERITOFBEINGTHEMOSTCONCISEANDFAITHFULSPECIMENOFBIOGRAPHYEXTANTINTHEL
ITERATUREOFANYAGEORCOUNTRYALTHOUGHIAMNOTDISPOSEDTOMAINTAINTHATTHEBEINGBORNINAWORKHOUSEISINITSELFTHEMOSTFORTUNATEANDENVIABLECIRCUMSTA
NCETHATCANPOSSIBLYBEFALLAHUMANBEINGIDOMEANTOSAYTHATINTHISPARTICULARINSTANCEITWASTHEBESTTHINGFOROLIVERTWISTTHATCOULDBYPOSSIBILITYHAVE
OCCURREDTHEFACTISTHATTHEREWASCONSIDERABLEDIFFICULTYININDUCINGOLIVERTOTAKEUPONHIMSELFTHEOFFICEOFRESPIRATIONATROUBLESOMEPRACTICEBUTONE
WHICHCUSTOMHASRENDEREDNECESSARYTOOUREASYEXISTENCEANDFORSOMETIMEHELAYGASPINGONALITTLEFLOCKMATTRESSRATHERUNEQUALLYPOISEDBETWEENTHISWOR
LDANDTHENEXTTHEBALANCEBEINGDECIDEDLYINFAVOUROFTHELATTERNOWIFDURINGTHISBRIEFPERIODOLIVERHADBEENSURROUNDEDBYCAREFULGRANDMOTHERSANXIOUS
AUNTSEXPERIENCEDNURSESANDDOCTORSOFPROFOUNDWISDOMHEWOULDMOSTINEVITABLYANDINDUBITABLYHAVEBEENKILLEDINNOTIMETHEREBEINGNOBODYBYHOWEVERBU
TAPAUPEROLDWOMANWHOWASRENDEREDRATHERMISTYBYANUNWONTEDALLOWANCEOFBEERANDAPARISHSURGEONWHODIDSUCHMATTERSBYCONTRACTOLIVERANDNATUREFOUGH
TOUTTHEPOINTBETWEENTHEMTHERESULTWASTHATAFTERAFEWSTRUGGLESOLIVERBREATHEDSNEEZEDANDPROCEEDEDTOADVERTISETOTHEINMATESOFTHEWORKHOUSETHEFA
CTOFANEWBURDENHAVINGBEENIMPOSEDUPONTHEPARISHBYSETTINGUPASLOUDACRYASCOULDREASONABLYHAVEBEENEXPECTEDFROMAMALEINFANTWHOHADNOTBEENPOSSES
SEDOFTHATVERYUSEFULAPPENDAGEAVOICEFORAMUCHLONGERSPACEOFTIMETHANTHREEMINUTESANDAQUARTERASOLIVERGAVETHISFIRSTPROOFOFTHEFREEANDPROPERAC
TIONOFHISLUNGSTHEPATCHWORKCOVERLETWHICHWASCARELESSLYFLUNGOVERTHEIRONBEDSTEADRUSTLEDTHEPALEFACEOFAYOUNGWOMANWASRAISEDFEEBLYFROMTHEPIL
LOWANDAFAINTVOICEIMPERFECTLYARTICULATEDTHEWORDSLETMESEETHECHILDANDDIETHESURGEONHADBEENSITTINGWITHHISFACETURNEDTOWARDSTHEFIREGIVINGTH
EPALMSOFHISHANDSAWARMANDARUBALTERNATELYASTHEYOUNGWOMANSPOKEHEROSEANDADVANCINGTOTHEBEDSHEADSAIDWITHMOREKINDNESSTHANMIGHTHAVEBEENEXPEC
TEDOFHIMOHYOUMUSTNOTTALKABOUTDYINGYETLORBLESSHERDEARHEARTNOINTERPOSEDTHENURSEHASTILYDEPOSITINGINHERPOCKETAGREENGLASSBOTTLETHECONTENT
SOFWHICHSHEHADBEENTASTINGINACORNERWITHEVIDENTSATISFACTIONLORBLESSHERDEARHEARTWHENSHEHASLIVEDASLONGASIHAVESIRANDHADTHIRTEENCHILDRENOF
HEROWNANDALLONEMDEADEXCEPTTWOANDTHEMINTHEWURKUSWITHMESHELLKNOWBETTERTHANTOTAKEONINTHATWAYBLESSHERDEARHEARTTHINKWHATITISTOBEAMOTHERTH
ERESADEARYOUNGLAMBDOAPPARENTLYTHISCONSOLATORYPERSPECTIVEOFAMOTHERSPROSPECTSFAILEDINPRODUCINGITSDUEEFFECTTHEPATIENTSHOOKHERHEADANDSTR
ETCHEDOUTHERHANDTOWARDSTHECHILDTHESURGEONDEPOSITEDITINHERARMSSHEIMPRINTEDHERCOLDWHITELIPSPASSIONATELYONITSFOREHEADPASSEDHERHANDSOVER
HERFACEGAZEDWILDLYROUNDSHUDDEREDFELLBACKANDDIEDTHEYCHAFEDHERBREASTHANDSANDTEMPLESBUTTHEBLOODHADSTOPPEDFOREVERTHEYTALKEDOFHOPEANDCOMF
ORTTHEYHADBEENSTRANGERSTOOLONGITSALLOVERMRSTHINGUMMYSAIDTHESURGEONATLASTAHPOORDEARSOITISSAIDTHENURSEPICKINGUPTHECORKOFTHEGREENBOTTLE
WHICHHADFALLENOUTONTHEPILLOWASSHESTOOPEDTOTAKEUPTHECHILDPOORDEARYOUNEEDNTMINDSENDINGUPTOMEIFTHECHILDCRIESNURSESAIDTHESURGEONPUTTINGO
NHISGLOVESWITHGREATDELIBERATIONITSVERYLIKELYITWILLBETROUBLESOMEGIVEITALITTLEGRUELIFITISHEPUTONHISHATANDPAUSINGBYTHEBEDSIDEONHISWAYTO
THEDOORADDEDSHEWASAGOODLOOKINGGIRLTOOWHEREDIDSHECOMEFROMSHEWASBROUGHTHERELASTNIGHTREPLIEDTHEOLDWOMANBYTHEOVERSEERSORDERSHEWASFOUNDLY
INGINTHESTREETSHEHADWALKEDSOMEDISTANCEFORHERSHOESWEREWORNTOPIECESBUTWHERESHECAMEFROMORWHERESHEWASGOINGTONOBODYKNOWSTHESURGEONLEANEDO
VERTHEBODYANDRAISEDTHELEFTHANDTHEOLDSTORYHESAIDSHAKINGHISHEADNOWEDDINGRINGISEEAHGOODNIGHTTHEMEDICALGENTLEMANWALKEDAWAYTODINNERANDTHE
NURSEHAVINGONCEMOREAPPLIEDHERSELFTOTHEGREENBOTTLESATDOWNONALOWCHAIRBEFORETHEFIREANDPROCEEDEDTODRESSTHEINFANTWHATANEXCELLENTEXAMPLEOF
THEPOWEROFDRESSYOUNGOLIVERTWISTWASWRAPPEDINTHEBLANKETWHICHHADHITHERTOFORMEDHISONLYCOVERINGHEMIGHTHAVEBEENTHECHILDOFANOBLEMANORABEGGA
RITWOULDHAVEBEENHARDFORTHEHAUGHTIESTSTRANGERTOHAVEASSIGNEDHIMHISPROPERSTATIONINSOCIETYBUTNOWTHATHEWASENVELOPEDINTHEOLDCALICOROBESWHI
CHHADGROWNYELLOWINTHESAMESERVICEHEWASBADGEDANDTICKETEDANDFELLINTOHISPLACEATONCEAPARISHCHILDTHEORPHANOFAWORKHOUSETHEHUMBLEHALFSTARVED
DRUDGETOBECUFFEDANDBUFFETEDTHROUGHTHEWORLDDESPISEDBYALLANDPITIEDBYNONEOLIVERCRIEDLUSTILYIFHECOULDHAVEKNOWNTHATHEWASANORPHANLEFTTOTHE
TENDERMERCIESOFCHURCHWARDENSANDOVERSEERSPERHAPSHEWOULDHAVECRIEDTHELOUDER
```

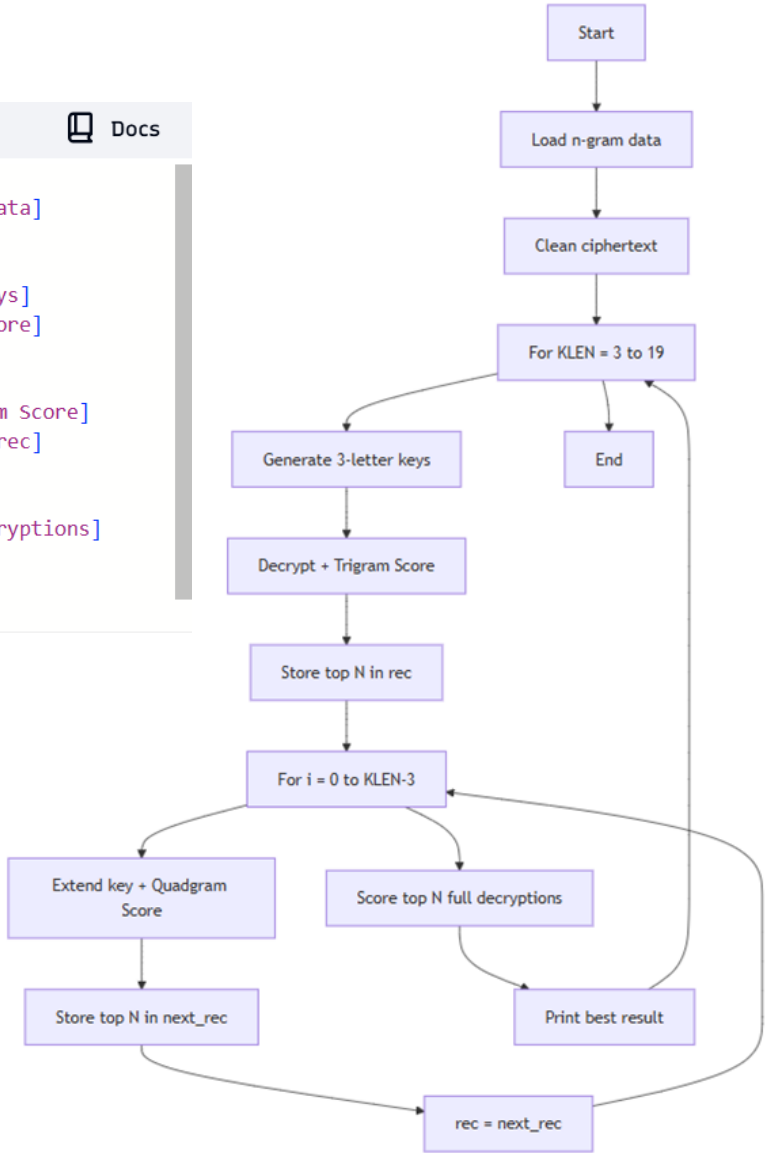
For known-plaintext the output is the key:

```
PS C:\Users\seyma\OneDrive\Desktop\Ödev> python k1.py
OLIVER
```

You can find the pseudo-code and diagram of my algorithm below:

Code Config Docs

```
graph TD
    A[Start] --> B[Load n-gram data]
    B --> C[Clean ciphertext]
    C --> D[For KLEN = 3 to 19]
    D --> E[Generate 3-letter keys]
    E --> F[Decrypt + Trigram Score]
    F --> G[Store top N in rec]
    G --> H[For i = 0 to KLEN-3]
    H --> I[Extend key + Quadgram Score]
    I --> J[Store top N in next_rec]
    J --> K[rec = next_rec]
    K --> H
    H --> L[Score top N full decryptions]
    L --> M[Print best result]
    M --> D
    D --> N[End]
```



2) In the second part of the study, a product cipher is formed by applying the S1 substitution system twice, effectively computing the composition S1 × S1. A second layer of encryption is then introduced using a randomly selected key. For this encryption step, the keyword **"SECRET"** is used. The resulting ciphertext along with the applied key is provided in the Appendices for reference.

To analyze this new ciphertext, the script developed in the first section is executed again. However, due to the fact that the plaintext at this stage is no longer a meaningful English message but rather an intermediate encrypted output, the algorithm fails to produce the correct decryption result. This is expected, as the script was designed to evaluate candidate plaintexts based on **English trigram and quadgram statistics**, and not ciphertext-like intermediate data.

Since the second layer of ciphertext does not resemble natural language, the scoring mechanism cannot reliably distinguish correct plaintext candidates. Consequently, the script returns the most statistically likely key and plaintext based on its internal scoring, though these results do not correspond to the actual encryption parameters used.

In order to recover the keyword **"SECRET"**, the inverse of the encryption function was applied. You can see the corresponding output below:

$$K_i = (C_i - P_i) \mod 26$$

P = Plaintext[i]
C = Ciphertext[i]
K = The Key (it should be "SECRET")

This process is repeated for a number of times equal to the key length, because in the Autokey cipher:

- Only the first *key_length* characters of the keystream come from the actual keyword,
- The remaining characters are derived from the plaintext itself.

The key and plaintext with the highest fitness score obtained from this unsuccessful attempt are presented below:

```
-39181.48905335451 autokey, klen 6 :"OMPJLT", LUZDQJDEKZEHDXITTWLZTKOPDNIPAQJFALVJKCWIYEYETZYFAOIJJUXZCOXKXLTOKVEOMDCVNNKIISJERRCTXKRDBUOUGIVJADXWTAPYVH
RJFFVXQFLVRMIQHKXGNCQLSNTSFDWUMOSGQBELDXBNKIGQHAZKXORRPFICEKRWERZISIXYOTJHZXNELPPVUSVQVQAOQQEOIZUWADIBNSJHEJXMPNEDXVQEEJAYECFHYZHDPQHGKEPQUKVSFONGBBDIXZ
GOVALLTUAATOMOICBRGXKPOVAJXJWGUYIOAGROIBVFFJETHAZONJLJODPIFJHUSMDGBNEPIETLZEMWNXZRBAFBURYPAEASNAGCAWONXEUPGBMATPCPEKHOOTLCJKHUMBVFNGRFBOSVDJGSFJWOGFTGBE
USYITJHAAMWTAXWWRFAWKXGAIUPFRRHZCFSIHPIPDHNPSWXKNEVRMRDHAUBLOMBKTWJNQAPAIYFTSJJLTOKLCNLUGQKKULQEQUMBPEYSHAVOKINXBFXIMPGCFTZBCNPMJBWTHSYKQWBPZMRACBUPXHYZ
BISOINVKTQNFXGZZZUBGTPESMVLJWEBGBVGLOHJMPMTKOVVPUAPPWTSEGIDTAOZISXMYSVSOTVZLOHKAZMAJULBEAXATJXCOGMOSXADSQFRRZHCKATMAIJTNOIEGNDAIWCRDEZIXKBLARMNSPTYXNRRC
GVMRLGAWIDXSZDVOEKWHCNPAHGNTOBYYIXJXAWHKWLDTMUJWGPOPFEULWXKICGJWLAKFFPYWFGNJGSDOUAOLHENJOLEEHVYDTCDJQEWJSDJGQGVABBCEWASQWTTGHFRKZBNIVTNASHGPJKLHFCFLMFUH
ZSHTLCEERMLJRYZXUMRURIJXGPIEQRBWHOEJUQTOBONXZGWTUIAUWTVWJCPZYTWAOUDEVURTHBMBQFVWIGRXCDOVPJXXLSYGDOOSVEUSEAALFJTWMHKETSHZZOYHRBUILGDAAMIRTYEVMQYTEXPQHINY
LEKOBTNIKIZLDNFOWJEZITLTSCDYIMLUNOIOJEIQTIHLETZGPLBFXIJUFTECXPQWNMDRWUJFBXTPKMDMWTWJFYLQJGHAOQUZXNBCNEUUDVFVBAHAQDCZTHNDNIMYZPTJQUIKMVFNJMYMLELZJMFRKGXP
PHTXYOMNTNGTPPURMGXYKBRDMXPQDSONIBKFGLEPOZFNBDGDDVEENHWQZJMWOYXTQIGCJUNTSEEPHDZJGSPIKTKBJGJSIAJFIZITDMAHVFUBMCTIGBULWCDKOHXWQVLSUOOWRVISEGKMVKMGIGBEZLGJ
MULGDADNZBTBUHXSPQRARKLONQEMKNCLCZLQRYMHRDDXLHXGRADTGTJBSNBPLZYYYNVAKPFIFJHIDWKSLWETXAESFZXKONVSZIERBFRLBGJTCQTIDNTIXKKHNYJJZOZULTJGIGVOUUYNFOTTWCAFADYO
IZEGKJENDNVIZIHHMLLURTYOPVYKKAOSDNKNBPWHQDAGOVTALSBPHSARQMBYLMJEFVKVDUJPQROSVSKIQDLWBIZFUCOSQBOMCCLASNQCVKHCUGBTCLFONQKCXKKFGYJJWUVGWTMYQRRBQWYTUEJRCBOF
IKYFMMQHVYLVUHKDBRKNKHJFTXEPYPJODMHMEKMUDCCHDFOTNDWPYDPPYAWOUHQUPAJFYJSEFDUWKXCAHLBLWKFCPFRDKUGGUYJRFHEVAVICXJEYCOWWRBKRRDUZBISOINJYQPJIVBUCHLENCGRTYVWW
YAREDJRRCGOGLTBEGCRZZORSLFMIJHBPKIFYNNMHAZKGEAEIKCQYEMAKENICAAMPWFZDYTJBCEDRVSPVEJMJBOBJLKZNEYJMJVQLZPIFYHSNEKKHODENZEKRUSAIRHKXTPAETIMAEIOJAAMGPEWOOYTN
KOWRFOFVFNAYWPDJDQCIQUYJAIIRIDLQOEEDNEGXKSREKMORSQCBZTTJHGLAAACMBATUYUHNJQPBQRZOIHDJMLUNADYMYTARIQMYTQTURYSWWFGKHVKAUFRMAHROWDAIAPNVOTAASPLVCRYRLWNBXNNL
VRYBBHXBUWTVPMVJPIMXWNBOUPIUVZEYLLWNEQSPPISAUUMVBTXDLZFMYFBEEIKLBMEWJMAUONRETENMYLSXUWFSTKDTUEPFTPHCCSOXWFAREOIKWRYHGPQSAWUSXGCAFVTLOGPYSVSSQZWERZFACGLJ
YHGLLEMCJYEDJCLCYYCEMRQSCTZNOLIXNIMDWPKBDCZDELLMAHQAAWKELRIRWNRQUJYOTAYSPEZDWDBWCWIEGXUKRAAWMJKOKMOALDBDAWMSJDMIGZOZKMXBZWBPLNININWDEUFFJARHZUARCIADDSCA
TTMMYUXKAXXDAHXMUDVVVTFXIRNXFZNSHCKEHYITZXNOKVGBSBQOAOAMEVANNLLVREEJTVZSXEORCHQNNNMKBHXWMWLKWAQSLPWFMIBGXVBLCLSSRFIPJAZDWWSETVTMWCNQSCAWHEZCYQUJBOZRNIYI
MJGTCPVZKZEOEJUNZPLOYTAUNVZVWZVWVKTGGVEWHZSLHUWKEFYFGBUATOBAZRWTXRZVIKRIVZOAMNWWKWNHQMAQQBEJUZMBTHCPKGCXPPPSUTIVCTINZVDXALJXEHOOFNRUHTYFTKEHSLPISLTOTCYS
IIFERECJPKTMGWBGCZEODOYWGLPURFIRYMPJIOUYWCOMCXHDCKDTHQHLKTBENHBFPSOPCRVQJSNIIMYPBXRAJUYYOKZINSPIXRSRZOLXJHAKLTODRBAGPNNSNWXFZXMDKSHLWZCAGBIFIEOILIBHVQHL
BLCLUFNKUJCZLGYODSOVXSFZYUSZLWTHIWCGXINXVXPXPYRUDMHKZDJMKQVULDFOFKDRCEBHESBGSDTMLLTKUUPLTFYMDSEZIBRVYWZEJZVDEOWXSKAWOGYNKVXCBUGBLIUTCDIRGPCXEMUZPIVXIFRI
FBXAYVUGKZZCUIIIBLTTOCLNEILCSVPFZOSWZKUTQMEWXOZCNFMFASLLHRQVFZRVRVAYJZDGTXZFEVRFKKLGYXKWBLRMYPDMUFUOEXQBGKFBHZVKHWWPNERVOSXWLKALHMZFVFHKUVSAHDNGGFSVHEKD
ULXTGIRCEJPSSCSLONKNCSKNJQLWHYTDOZXRMHPYAHLZQPVTDARMADFGRACCUXHESIVWKABYPIEWPUOFIXHVPMFASNEYLZAWTEXJVMDCDFGWRSPFWMGDRRIWSIHLYXOFDFUGDGBXMPWDEILHPNWHKTLW
KKSVTSAGCSGEPBNDEOOHDEXAYRHCGCWGDMCQOLJYVMEWYNUZRLFGTPKWLPIQJGXRUEAYEBKJLRMTUNLYPPBKRQHISJNVDBWEFTAAVKNSSARJAWOBGJNPBNMOODSQEEHWNFPYVLDRKUYTCNTUWFJOFKNZ
HASMRRIYTITAKOXVSPJYSTQIFSBIDBDOAKNLHBIOIAVNPZWPNQVYKVNNIDJFFFHXBKBHEFOBRAYORNGKFMJTQMMJNVCAJGXVWXNVZSSLTOPIRUPZWOLFQUAOCJKWRTUNMWAPBUSPYEZTOVSMNOSPGLZI
LGVWSHXUBMZITXGEGOGHTDUOVIBKJKHDSWWUHHESBRYREWENVOTQBUMTJMOUGPVKFIVERKGEOFNEAYCJGTPVFMZEWNVUDTFYZECJTXMRMCTPWKZFNUAKBXKLQFUEAZMFEWQDMVFDLRKFIGYDKUTOCPIN
DARKIYOBOTCJOFFDCPYSMHDNHOPSJTWEXPPCOHKKERAHVMIKUSOVQWNYSYEMDBXYHCXYLSFJLKAQVNPPSUIIHEPBAWXTUADYGUCKYSLTVFREYHPCEFKPTCKOWWTYCDJOUMHZAEFOPSSIOUJXQHMAXDOZ
ARKNFJHVQEATHGEHYYFWKTQKWDYWDOLHEMZOKFBZSKLEENFXDZHYCXZXYEGWUANYUROKYEOPTODUEYPOFGEDHOEIDMZIZIOBUAQKQDPSEERVIRTDBBAGHEFXXXXNYRVYDRSLONSNNRWIMHXETSFOZUVZ
EMYDCAEYRHQVVQFOAGUQHLSQTTTSBRXOSODTMTLKMYLGPCTJTSOGZQQYCBGNYYHVUDZFUOKKUVIMRPJMTSPOORXXGPINSPWWNXEPSMDODLMPELXNHFSVCQKDIVAUHTYFWZJCIVQMVCSJJTFRMQWWPKNA
VMBXYTILGAKMMUOPCZMOIEMSMOKVMSCQQIGXEGQGMDNLFBMNEHVAKQLCNPFNYVWZHQOLDSIEMXXMKMNFPVTSLCBDLQDVEQYIJEMDSNPPPKOPFSYJAQCGZZYJFGNOCZQHDYAPUTSWWBEPSHMFPWMWGVZR
ECUZCMPSJSIKWWRMHWCNILQRIEWSYOJCTRKCCXHUPDULAIEMZSVPSNSDSOEVASFZOVDWMRFNXXPWUEXMEZCXYCHUSAABLUALJKRKOJFQGGAMKTMGEPIEMHFZANMORKSMTHOTCHVTYEZRDANMREMSDMNZ
XWBMBNOFSWUNZOJPSJEZBUFLTDTPDAKMGAPYGZRMUPJAYTUNUXPNNBBETUOQJLEZSSBLCDRTXKSKFOEWZSSAMFSIFDHYDLZJVCYHDKRNINKRZNDRSFYUEHCABTOQUAFLHCIGWULIVVRAHISWXEARDHGN
HJPOPATHNKJHKOIQZWJGRLBKIMUMFQHUTOQPORKBIEKLUSUOMVLALGMFDKUANYMXEEYXUUIZFJESLAJUUMXZHGKLIPATJQQHKOFHGMBRCYTYDRLHWDCRRYPIGHGOWJFOFKKSTNQUDSECFGIICWMPEVAD
NXUKAUWFCHTAVDHSABIDWUQBSTIXPEJEIMLWAXLBXMCZYCZUKIRYZIAJSPLMSOJNSRLZYDWOFLXDDJCFHXXYTRILZXADI
```

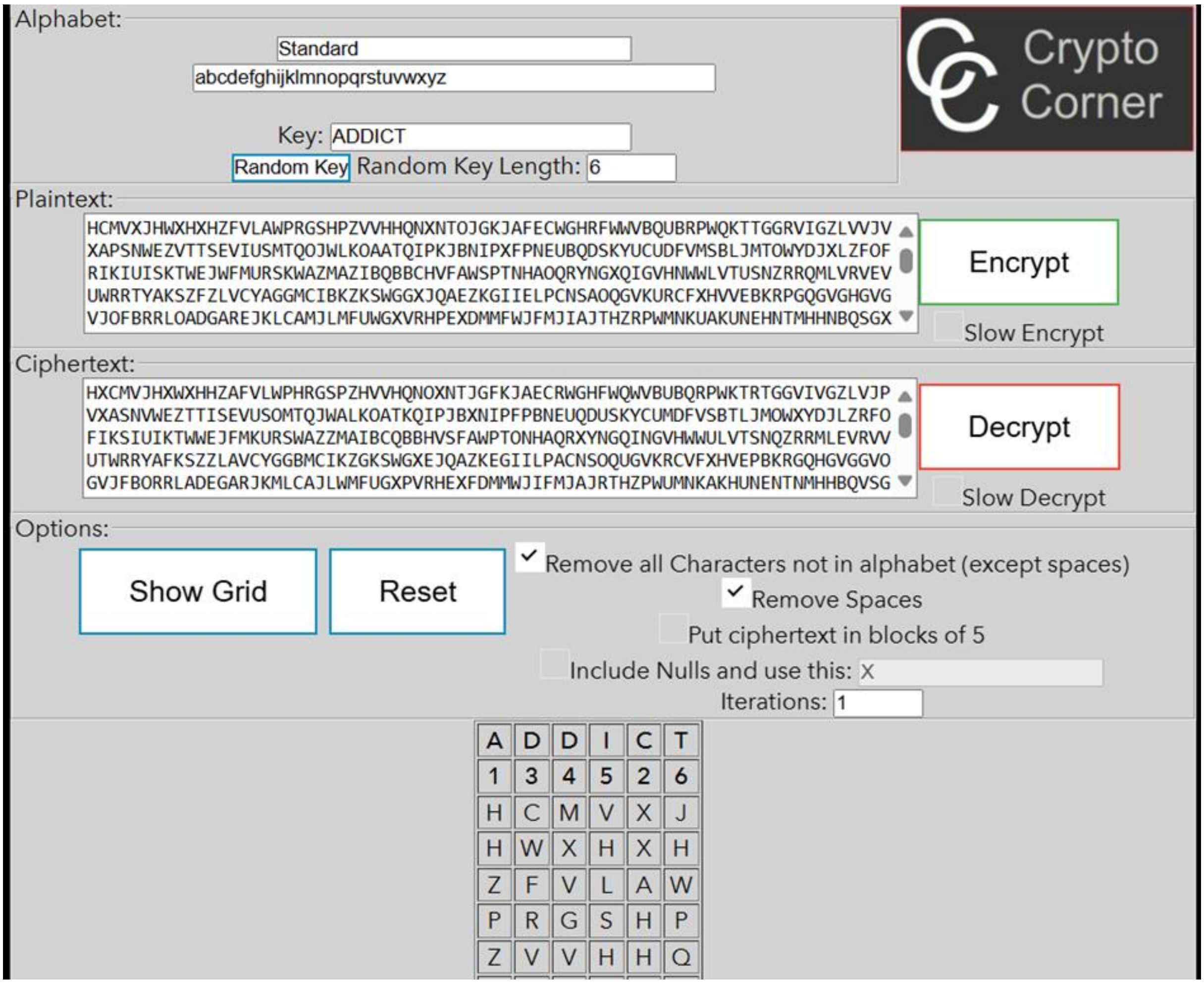
Assuming that the given ciphertext and the key length are known, the key has been successfully recovered using the constructed S2 system. The terminal output of the script used in this process is shown below:

```
PS C:\Users\seyma\OneDrive\desktop> python secretbul.py
Recovered key (should be SECRET): SECRET
```

3) In the last problem, a product cipher is formed by integrating the S1 cipher with a permutation cipher, and then cryptanalysis is conducted on it. The key "ADDICT" is randomly chosen to encrypt the message using the permutation cipher. The encrypted text is available in the Appendices. When the script was run on this encrypted output, it couldn’t uncover the original text or the key, as it relies on English trigrams and quadgrams for analysis. The permutation cipher shuffles the letters’ positions, which disrupts the n-grams and makes them undetectable. Thus, this method cannot successfully decode the encrypted text.

For this reason, the permutation cipher needs to be unraveled first. Techniques like anagramming, dictionary-based attacks, and hill climbing can be used to analyze the permutation cipher. Still, these approaches fall short since the initial ciphertext contains scrambled characters that don’t create recognizable words [3]. Such strategies work best when dealing with unencrypted plaintext.

We used the Crypto Corner site to create the permutation cipher:



This site generates a permutation based on the word "ADDICT."
In other words, what is being done here is a monoalphabetic substitution cipher.
Each letter is mapped to another letter, but this mapping is derived from "ADDICT.

References

1) **http://practicalcryptography.com/ciphers/polyalphabetic-substitution-category/autokey/**

2) **http://practicalcryptography.com/cryptanalysis/letter-frequencies-various-languages/english-letter-frequencies/**

3) **http://practicalcryptography.com/cryptanalysis/stochastic-searching/cryptanalysis-columnar-transposition-cipher/**

4) Mills, David L. *The Autokey Security Architecture, Protocol and Algorithms*. Technical Report 06-1-1, University of Delaware, January 2006.