APPLIED CRYPTOGRAPHY

Lab 1 : Classical Ciphers

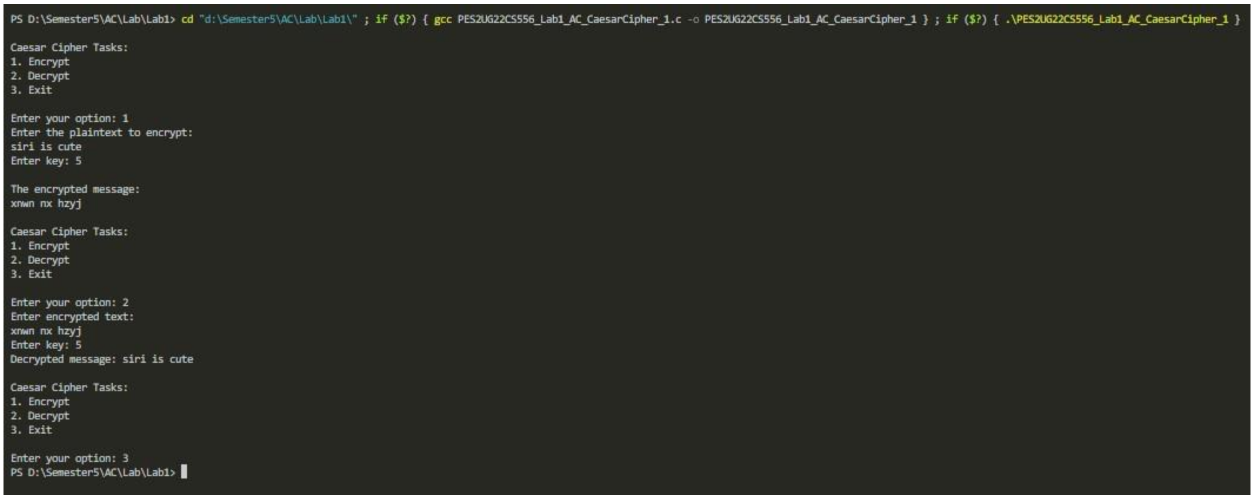
Name: Siri N Shetty SRN: PES2UG22CS556

Problem 1: Caesar Cipher

Tasks:

1. Encryption and Decryption:
i)Write a function to encrypt a plaintext message using a given shift value.
ii)Write a function to decrypt a ciphertext message using the same shift value.

Expected Deliverables -
i) Code Output Screenshot (Terminal should have SRN visible)



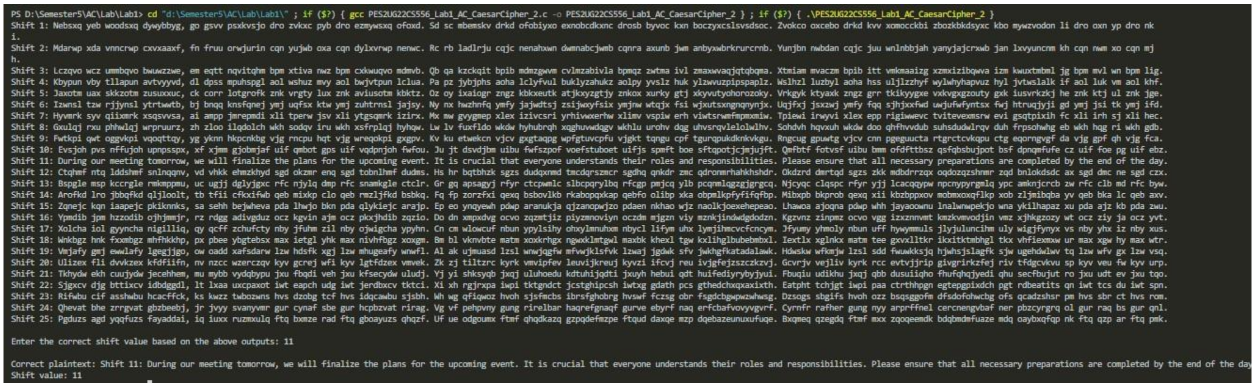
```
PS D:\Semester5\AC\Lab\Lab1> cd "d:\Semester5\AC\Lab\Lab1\" ; if ($?) { gcc PES2UG22CS556_Lab1_AC_CaesarCipher_1.c -o PES2UG22CS556_Lab1_AC_CaesarCipher_1 } ; if ($?) { .\PES2UG22CS556_Lab1_AC_CaesarCipher_1 }

Caesar Cipher Tasks:
1. Encrypt
2. Decrypt
3. Exit

Enter your option: 1
Enter the plaintext to encrypt:
siri is cute
Enter key: 5

The encrypted message:
xnwn nx hzyj

Caesar Cipher Tasks:
1. Encrypt
2. Decrypt
3. Exit

Enter your option: 2
Enter encrypted text:
xnwn nx hzyj
Enter key: 5
Decrypted message: siri is cute

Caesar Cipher Tasks:
1. Encrypt
2. Decrypt
3. Exit

Enter your option: 3
PS D:\Semester5\AC\Lab\Lab1> 
```

2. Breaking the Cipher: The following text was encrypted with a substitution cipher. Implement a brute-force attack to break the Caesar cipher without knowing the shift value. Find the plaintext, shift value.

Ofctyr zfc xppetyr ezxzcczh, hp htww qtylwtkp esp awlyd qzc esp fanzxtyr pgpye. Te td ncfntlw esle pgpcjzyp fyopcdelyod esptc czwpd lyo cpdazydtmtwtetpd. Awpldp pydfcp esle lww ypnpddlcj acpalcletzyd lcp nzxawpepo mj esp pyo zq esp olj.

Expected Deliverables -

i) Code Output Screenshot (Terminal should have SRN visible, each decryption with key value should be visible).



```
PS D:\Semester5\AC\Lab\Lab1> cd "d:\Semester5\AC\Lab\Lab1\" ; if ($?) { gcc PES2UG22CS556_Lab1_AC_CaesarCipher_2.c -o PES2UG22CS556_Lab1_AC_CaesarCipher_2 } ; if ($?) { .\PES2UG22CS556_Lab1_AC_CaesarCipher_2 }
Shift 1: Nebsxq yeb woodsxq dywybbyg, go gsvv psxkvsjo dro zvkxc pyb dro ezmywsxq ofoxd. Sd sc mbemskv drkd ofobiyxo exnobcdkxnc drosb byvoc kxn boczyxcslsvsdsoc. Zvokco oxcebo drkd kvv xomocckbi zbozkbkdsyxc kbo mywzvodon li dro oxn yp dro nk
i.
Shift 2: Mdarwp xda vnncrwp cxvxaaxf, fn fruu orwjurin cqn yujwb oxa cqn dylxvrwp nenwc. Rc rb ladlrju cqjc nenahxwn dwmnabcjwmb cqnra axunb jwm anbyxwbrkrurcrnb. Yunjbn nwbdan cqjc juu wnlnbbjah yanyjajcrxwb jan lxvyuncnm kh cqn nwm xo cqn mj
h.
Shift 3: Lczqvo wcz ummbqvo bwuwzzwe, em eqtt nqvitqhm bpm xtiva nwz bpm cxkwuqvo mdmvb. Qb qa kzckqit bpib mdmzgwvm cvlmzabivla bpmqz zwtma ivl zmaxwvaqjqtqbqma. Xtmiam mvaczm bpib itt vmkmaaizg xzmxizibqwva izm kwuxtmbml jg bpm mvl wn bpm lig.
Shift 4: Kbypun vby tllapun avtvyyvd, dl dpss mpuhspgl aol wshuz mvy aol bwjvtpun lclua. Pa pz jybjphs aoha lclyfvul buklyzahukz aolpy yvslz huk ylzwvuzpipspaplz. Wslhzl luzbyl aoha hss uljlzzhyf wylwhyhapvuz hyl jvtwslalk if aol luk vm aol khf.
Shift 5: Jaxotm uax skkzotm zusuxxuc, ck corr lotgrofk znk vrgty lux znk aviusotm kbktz. Oz oy ixaiogr zngz kbkxeutk atjkxyzgtjy znkox xurky gtj xkyvutyohorozoky. Vrkgyk ktyaxk zngz grr tkikyygxe vxkvgxgzouty gxk iusvrkzkj he znk ktj ul znk jge.
Shift 6: Izwnsl tzw rjjynsl ytrtwwtb, bj bnqq knsfqnej ymj uqfsx ktw ymj zuhtrnsl jajsy. Ny nx hwzhnfq ymfy jajwdtsj zsijwxyfsix ymjnw wtqjx fsi wjxutsxngnqnynjx. Uqjfxj jsxzwj ymfy fqq sjhjxxfwd uwjufwfyntsx fwj htruqjyji gd ymj jsi tk ymj ifd.
Shift 7: Hyvmrk syv qiixmrk xsqsvvsa, ai ampp jmrepmdi xli tperw jsv xli ytgsqmrk izirx. Mx mw gvygmep xlex izivcsri yrhivwxerhw xlimv vspiw erh viwtsrwmfmpmxmiw. Tpiewi irwyvi xlex epp rigiwwevc tvitevexmsrw evi gsqtpixih fc xli irh sj xli hec.
Shift 8: Gxulqj rxu phhwlqj wrpruurz, zh zloo ilqdolch wkh sodqv iru wkh xsfrplqj hyhqw. Lw lv fuxfldo wkdw hyhubrqh xqghuvwdqgv wkhlu urohv dqg uhvsrqvlelolwlhv. Sohdvh hqvxuh wkdw doo qhfhvvdub suhsdudwlrqv duh frpsohwhg eb wkh hqg ri wkh gdb.
Shift 9: Fwtkpi qwt oggvkpi vqoqttqy, yg yknn hkpcnkbg vjg rncpu hqt vjg wreqokpi gxgpv. Kv ku etwekcn vjcv gxgtaqpg wpfgtuvcpfu vjgkt tqngu cpf tgurqpukdknkvkgu. Rngcug gpuwtg vjcv cnn pgeguucta rtgrctcvkqpu ctg eqorngvgf da vjg gpf qh vjg fca.
Shift 10: Evsjoh pvs nffujoh upnpsspx, xf xjmm gjobmjaf uif qmbot gps uif vqdpnjoh fwfou. Ju jt dsvdjbm uibu fwfszpof voefstuboet uifjs spmft boe sftqpotjcjmjujft. Qmfbtf fotvsf uibu bmm ofdfttbsz qsfqbsbujpot bsf dpnqmfufe cz uif foe pg uif ebz.
Shift 11: During our meeting tomorrow, we will finalize the plans for the upcoming event. It is crucial that everyone understands their roles and responsibilities. Please ensure that all necessary preparations are completed by the end of the day.
Shift 12: Ctqhmf ntq lddshmf snlnqqnv, vd vhkk ehmzkhyd sgd okzmr enq sgd tobnlhmf dudms. Hs hr bqtbhzk sgzs dudqxnmd tmcdqrszmcr sgdhq qnkdr zmc qdronmrhahkhshdr. Okdzrd dmrtqd sgzs zkk mdbdrrzqx oqdozqzshnmr zqd bnlokdsdc ax sgd dmc ne sgd czx.
Shift 13: Bspgle msp kccrgle rmkmppmu, uc ugjj dglyjgxc rfc njylq dmp rfc snamkgle ctclr. Gr gq apsagyj rfyr ctcpwmlc slbcpqrylbq rfcgp pmjcq ylb pcqnmlqgzgjgrgcq. Njcyqc clqspc rfyr yjj lcacqqypw npcnypyrgmlq ypc amknjcrcb zw rfc clb md rfc byw.
Shift 14: Arofkd lro jbbqfkd qljloolt, tb tfii cfkxifwb qeb mixkp clo qeb rmzljfkd bsbkq. Fq fp zorzfxi qexq bsbovlkb rkabopqxkap qebfo olibp xka obpmlkpfyfifqfbp. Mibxpb bkprob qexq xii kbzbppxov mobmxoxqflkp xob zljmibqba yv qeb bka lc qeb axv.
Shift 15: Zqnejc kqn iaapejc pkiknnks, sa sehh bejwheva pda lhwjo bkn pda qlykiejc arajp. Ep eo ynqyewh pdwp aranukja qjzanopwjzo pdaen nkhao wjz naolkjoexehepeao. Lhawoa ajoqna pdwp whh jayaoownu lnalwnwpekjo wna ykilhapaz xu pda ajz kb pda zwu.
Shift 16: Ypmdib jpm hzzodib ojhjmmjr, rz rdgg adivgduz ocz kgvin ajm ocz pkxjhdib zqzio. Do dn xmpxdvg ocvo zqzmtjiz piyzmnoviyn oczdm mjgzn viy mznkjindwdgdodzn. Kgzvnz zinpmz ocvo vgg izxznnvmt kmzkvmvodjin vmz xjhkgzozy wt ocz ziy ja ocz yvt.
Shift 17: Xolcha iol gyyncha nigilliq, qy qcff zchufcty nby jfuhm zil nby ojwigcha ypyhn. Cn cm wlowcuf nbun ypylsihy ohxylmnuhxm nbycl lifym uhx lymjihmcvcfcncym. Jfyumy yhmoly nbun uff hywymmuls jlyjuluncihm uly wigjfynyx vs nby yhx iz nby xus.
Shift 18: Wnkbgz hnk fxxmbgz mhfhkkhp, px pbee ybgtebsx max ietgl yhk max nivhfbgz xoxgm. Bm bl vknvbte matm xoxkrhgx ngwxklmtgwl maxbk khexl tgw kxlihglbubebmbxl. Iextlx xglnkx matm tee gxvxlltkr ikxitktmbhgl tkx vhfiexmxw ur max xgw hy max wtr.
Shift 19: Vmjafy gmj ewwlafy lgegjjgo, ow oadd xafsdarw lzw hdsfk xgj lzw mhugeafy wnwfl. Al ak ujmuasd lzsl wnwjqgfw mfvwjklsfvk lzwaj jgdwk sfv jwkhgfkatadalawk. Hdwskw wfkmjw lzsl sdd fwuwkksjq hjwhsjslagfk sjw ugehdwlwv tq lzw wfv gx lzw vsq.
Shift 20: Ulizex fli dvvkzex kfdfiifn, nv nzcc wzerczqv kyv gcrej wfi kyv lgtfdzex vmvek. Zk zj tiltzrc kyrk vmvipfev leuvijkreuj kyvzi ifcvj reu ivjgfejzszczkzvj. Gcvrjv vejliv kyrk rcc evtvjjrip givgrirkzfej riv tfdgcvkvu sp kyv veu fw kyv urp.
Shift 21: Tkhydw ekh cuujydw jecehhem, mu mybb vydqbypu jxu fbqdi veh jxu kfsecydw uludj. Yj yi shksyqb jxqj uluhoedu kdtuhijqdti jxuyh hebui qdt huifediyrybyjyui. Fbuqiu udikhu jxqj qbb dusuiiqho fhufqhqjyedi qhu secfbujut ro jxu udt ev jxu tqo.
Shift 22: Sjgxcv djg bttixcv idbdggdl, lt lxaa uxcpaxot iwt eapch udg iwt jerdbxcv tktci. Xi xh rgjrxpa iwpi tktgndct jcstghipcsh iwtxg gdath pcs gthedchxqxaxixth. Eatpht tchjgt iwpi paa ctrthhpgn egtepgpixdch pgt rdbeatits qn iwt tcs du iwt spn.
Shift 23: Rifwbu cif asshwbu hcacffck, ks kwzz twbozwns hvs dzobg tcf hvs idqcawbu sjsbh. Wh wg qfiqwoz hvoh sjsfmcbs ibrsfghobrg hvswf fczsg obr fsgdcbgwpwzwhwsg. Dzsogs sbgifs hvoh ozz bsqsggofm dfsdofohwcbg ofs qcadzshsr pm hvs sbr ct hvs rom.
Shift 24: Qhevat bhe zrrgvat gbzbeebj, jr jvyy svanyvmr gur cynaf sbe gur hcpbzvat rirag. Vg vf pehpvny gung rirelbar haqrefgnaqf gurve ebyrf naq erfcbafvovyvgvrf. Cyrnfr rafher gung nyy arprffnel cercnengvbaf ner pbzcyrgrq ol gur raq bs gur qnl.
Shift 25: Pgduzs agd yqqfuzs fayaddai, iq iuxx ruzmxulq ftq bxmze rad ftq gboayuzs qhqzf. Uf ue odgoumx ftmf qhqdkazq gzpqdefmzpe ftqud daxqe mzp dqebazeunuxufuqe. Bxqmeq qzegdq ftmf mxx zqoqeemdk bdqbmdmfuaze mdq oaybxqfqp nk ftq qzp ar ftq pmk.

Enter the correct shift value based on the above outputs: 11

Correct plaintext: Shift 11: During our meeting tomorrow, we will finalize the plans for the upcoming event. It is crucial that everyone understands their roles and responsibilities. Please ensure that all necessary preparations are completed by the end of the day
Shift value: 11
```

ii) Write in text the final key value deciphered.

The final text is: During our meeting tomorrow, we will finalize the plans for the upcoming event. It is crucial that everyone understands their role and responsibilities. Please ensure that all necessary preparations are completed by the end of the day.

Shift value: 11

Problem 2 : Vigenère Cipher Tasks:

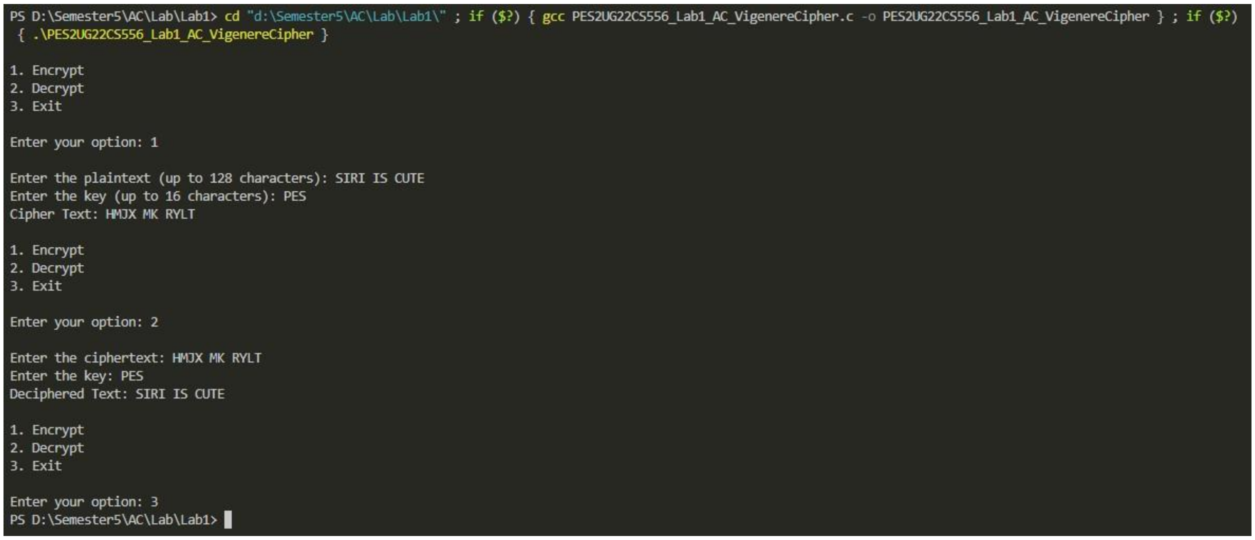
Tasks: Encryption and Decryption:

i)Write a function to encrypt a plaintext message using a given keyword.

ii)Write a function to decrypt a ciphertext message using the same keyword.

Expected Deliverables -

i) Code Output Screenshot (Terminal should have SRN visible)



```
PS D:\Semester5\AC\Lab\Lab1> cd "d:\Semester5\AC\Lab\Lab1\" ; if ($?) { gcc PES2UG22CS556_Lab1_AC_VigenereCipher.c -o PES2UG22CS556_Lab1_AC_VigenereCipher } ; if ($?)
 { .\PES2UG22CS556_Lab1_AC_VigenereCipher }

1. Encrypt
2. Decrypt
3. Exit

Enter your option: 1

Enter the plaintext (up to 128 characters): SIRI IS CUTE
Enter the key (up to 16 characters): PES
Cipher Text: HMJX MK RYLT

1. Encrypt
2. Decrypt
3. Exit

Enter your option: 2

Enter the ciphertext: HMJX MK RYLT
Enter the key: PES
Deciphered Text: SIRI IS CUTE

1. Encrypt
2. Decrypt
3. Exit

Enter your option: 3
PS D:\Semester5\AC\Lab\Lab1> █
```

Problem 3 : Hill Cipher Description :

Tasks:

1. Matrix Operations:

Write functions for matrix multiplication and finding the inverse of a matrix modulo 26.

2. Encryption and Decryption:

Write functions to encrypt and decrypt a message using a given key matrix.

3. Exercises:

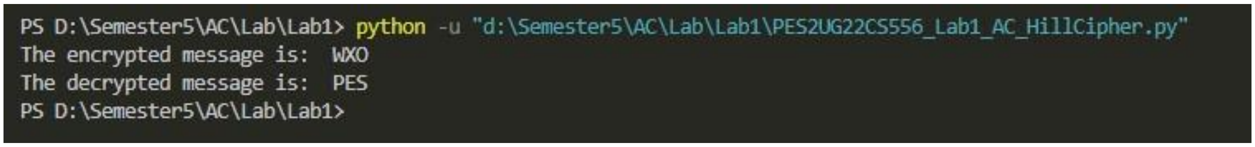
i)Define a key matrix.

ii)Encrypt and decrypt a message using the key matrix.

iii)Discuss the mathematical principles behind the Hill cipher.

Expected Deliverables -

i) Code Output Screenshot (Terminal should have SRN visible)



```
PS D:\Semester5\AC\Lab\Lab1> python -u "d:\Semester5\AC\Lab\Lab1\PES2UG22CS556_Lab1_AC_HillCipher.py"
The encrypted message is:  WXO
The decrypted message is:  PES
PS D:\Semester5\AC\Lab\Lab1>
```

iii) Write in text the mathematical principles behind Hill Cipher.

Hill cipher is based on linear algebra principles, providing a foundation for learning and understanding more advanced encryption techniques. It offers an opportunity to explore the relationship between matrices and encryption algorithms.

One obtains a cipher-text vector by multiplying the plaintext vector by the key matrix. This vector is finally converted back into text. Since the characters are represented as numbers, all arithmetic is done modulo 26 to ensure the results stay within this range. To decrypt a Hill cipher message, one needs to compute the inverse of the key matrix modulo 26. This inverse matrix is then multiplied It is multiplied, modulo 26, by the inverse of the ciphertext vector. For decryption to be possible, the determinant of the key matrix has to be nonzero and co-prime with 26.