Problem-1

Here, using the Caesar cipher-

Decryption:

$$De = (En - K) \ mod \ 26$$

Here ciphertext is "krclxrwrbxwnxocqnlxxunbcrwencrxwbrwanlnwccrvnb" and the key is not given. We have to decrypt the message repeatedly, using all the keys from 1 to 25 (because we don't know which is the 'actual' key!), until we get 'something' that makes sense.

Representation of plaintext and ciphertext characters in Z_{26}

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	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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

K=1,

Ciphertext: krclxrwrbxwnxocqnlxxunbcrwencrxwbrwanlnwccrvnb

Decipher for 1st letter,

$$De = (En - K) \ mod \ 26$$

$$De = (k - 1) \ mod \ 26$$

$$De = (10 - 1) \ mod \ 26$$

$$De = 9 \ mod \ 26$$

$$De = 9$$

Value 9 is assigned for " j ". So,

Deciphertext: jqbkwqvqawvmwnbpmkwwtmabqvdmbqwvaqvzmkmvbbquma

K=2,

Ciphertext: krclxrwrbxwnxocqnlxxunbcrwencrxwbrwanlnwccrvnb

Deciphertext: ipajvpupzvulvmaoljvvslzapuclapvuzpuyljluaaptlz

K=3,

Ciphertext: krclxrwrbxwnxocqnlxxunbcrwencrxwbrwanlnwccrvnb

Deciphertext: hoziuotoyutkulznkiuurkyzotbkzoutyotxkiktzzosky

K=4,

Ciphertext: `krclxrwrbxwnxocqnlxxunbcrwencrxwbrwanlnwccrvnb`
Deciphertext: `gnyhtnsnxtsjtkymjhttqjxynsajyntsxnswjhjsyynrjx`

K=5,

Ciphertext: `krclxrwrbxwnxocqnlxxunbcrwencrxwbrwanlnwccrvnb`
Deciphertext: `fmxgsmrmwsrisjxligsspiwxmrzixmsrwmrvigirxxmqiw`

K=6,

Ciphertext: `krclxrwrbxwnxocqnlxxunbcrwencrxwbrwanlnwccrvnb`
Deciphertext: `elwfrlqlvrqhriwkhfrrohvwlqyhwlrqvlquhfhqwwlphv`

K=7,

Ciphertext: `krclxrwrbxwnxocqnlxxunbcrwencrxwbrwanlnwccrvnb`
Deciphertext: `dkveqkpkuqpgqhvjgeqqnguvkpxgvkqpukptgegpvvkogu`

K=8,

Ciphertext: `krclxrwrbxwnxocqnlxxunbcrwencrxwbrwanlnwccrvnb`
Deciphertext: `cjudpjojtpofpguifdppmftujowfujpotjosfdfouujnft`

K=9,

Ciphertext: `krclxrwrbxwnxocqnlxxunbcrwencrxwbrwanlnwccrvnb`
Deciphertext: `bitcoinisoneofthecoolestinvetionsinrecenttimes`

For k=9, we get a message that makes sense. The message is

`bitcoinisoneofthecoolestinvetionsinrecenttimes`

Problem-2(Cipher-1)

The ciphertext has been encrypted with Monoalphabetic Substitution Cipher. First We find out the alphabet's frequency from the ciphertext.

T	(48) 13.6%	Y	(8) 2.3%
M	(43) 12.1%	S	(7) 2%
N	(39) 11%	H	(6) 1.7%
F	(31) 8.8%	W	(6) 1.7%
I	(30) 8.5%	B	(4) 1.1%
G	(22) 6.2%	Q	(4) 1.1%
K	(19) 5.4%	R	(4) 1.1%
Z	(16) 4.5%	U	(3) 0.8%
O	(15) 4.2%	X	(3) 0.8%
D	(14) 4%	P	(1) 0.3%
J	(14) 4%	A	0
C	(9) 2.5%	L	0
E	(8) 2.3%	V	0

The alphabets' frequency in this order in standard English,

e	t	a	o	n	h	i	s	r	d	l	u	w	m	g	c	f	y	b	p	k	v	j	x	q	z

Substitution table:

T	M	N	F	I	G	K	Z	O	D	J	C	E	Y	S	H	W	B	Q	R	U	X	P	A	L	V
e	t	a	o	n	h	i	s	r	d	l	u	w	m	g	c	f	y	b	p	k	v	j	x	q	z

Step-1:
The most frequent letters here are T, M, N. We substitute these letters with e, t, a.
After substitution,

Ie CaJ FGt EeKtaOF CIetIeK **tIe** JWF JIGFe GK YGK **tIat** SatteK CIetIeK Ot CaJ ZaB GK FOUIt Ie CaJ aJIaSeZ tG aJQ aDD tIe HDaFet JeeSeZ tG DOXe ReFeatI SetaD tIe SeaD GY CIOEI Ie IaZ PWJt HaKtaQeF IaZ ReeF DaReDeZ DWFEIeGF RWt tIeKe CeKe SaFB HDaFetJ CIOEI DOXeZ a JtaFZaKZ tOSeJEaDe tIat tGGQ FG aEEGWFt GY tIe HeKIaHJ OFEGFXeFOeFt aDteKFatOGF GY ZaB aFZ FOUIt. tIe Kate GY HDaFetaKB tWKFOFUJ ZOYYeKeZ, aFZ Ie ZOZ FGt QFGC tIat GY tKaFtGK

Step-2:
From the substitution table, we have to substitute "I" with 'n'. For this, "Ie", " tIe", "tIat", words are converted into "ne", " tne", "tnat". These words have no meaning. If we substitute "I" with the closest letters of 'n' ('o', 'h', 'a', 'i'), then only using 'h', we get some meaningful words ("he", " the", "that"). After substitution,

he CaJ FGt EeKtaOF ChetheK the JWF JhGFe GK YGK that SatteK ChetheK Ot CaJ ZaB GK FOUht he CaJ aJhaSeZ tG aJQ aDD the HDaFet JeeSeZ tG DOXe ReFeath SetaD the SeaD GY ChOEh he haZ PWJt HaKtaQeF haZ ReeF DaReDeZ DWFEheGF RWt **theKe** CeKe SaFB HDaFetJ ChOEh DOXeZ a JtaFZaKZ tOSeJEaDe that tGGQ FG aEEGWFt GY the HeKhaHJ OFEGFXeFOeFt aDteKFatOGF GY ZaB aFZ FOUht. the **Kate** GY HDaFetaKB tWKFOFUJ ZOYYeKeZ, aFZ he ZOZ FGt QFGC that GY tKaFtGK

Step-3:
From the substitution table, we have to substitute "K" with 'i'. For this, "Kate", "theKe", words are converted into "iate", "theie". These words have no meaning. If we substitute "K" with the closest letters of 'i' ('h', 's', 'n', 'r'), then only using 'r', we get some meaningful words ("rate", "there"). After substitution,

he CaJ FGt EertaOF **Chether** the JWF JhGFe Gr YGr that Satter Chether Ot CaJ ZaB Gr FOUht he CaJ aJhaSeZ tG aJQ aDD the HDaFet JeeSeZ tG DOXe ReFeath SetaD the SeaD GY ChOEh he haZ PWJt HartaQeF haZ ReeF DaReDeZ DWFEheGF RWt there **Cere** SaFB HDaFetJ ChOEh DOXeZ a JtaFZarZ tOSeJEaDe that tGGQ FG aEEGWFt GY the HerhaHJ OFEGFXeFOeFt

aDterFatOGF GY ZaB aFZ FOUht. the rate GY HDaFetarB tWrFOFUJ ZOYYereZ, aFZ he ZOZ FGt QFGC that GY traFtGr

Step-4:
From the substitution table, we have to substitute “C” with ‘u’. For this, “Chether”, “ Cere”, words are converted into “uhether”, “ uere”,. These words have no meaning. If we substitute “C” with the closest letters of ‘u’ (‘w’, ‘l’, ‘d’, ‘m’), then only using ‘w’, we get some meaningful words (“whether”, “ were”). After substitution,

he waJ FGt EertaOF whether the JWF JhGFe **Gr** YGr that Satter whether Ot waJ ZaB Gr FOUht he waJ aJhaSeZ tG aJQ aDD the HDaFet JeeSeZ **tG** DOXe ReFeath SetaD the SeaD GY whOEh he haZ PWJt HartaQeF haZ ReeF DaReDeZ DWFEheGF RWt there were SaFB HDaFetJ whOEh DOXeZ a JtaFZarZ tOSeJEaDe that tGGQ FG aEEGWFt GY the HerhaHJ OFEGFXeFOeFt aDterFatOGF GY ZaB aFZ FOUht. the rate GY HDaFetarB tWrFOFUJ ZOYYereZ, aFZ he ZOZ FGt QFGw that GY traFtGr

Step-5:
From the substitution table, we have to substitute “G” with ‘h’ for ‘Gr’, ’tG’ words. But ‘h’ is already used. If we substitute “G” with the closest letters of ‘h’ (‘n’, ‘i’, ‘o’, ‘s’), then only using ‘o’, we get some meaningful words (‘or’, ’to’). After substitution,

he waJ Fot EertaOF whether the JWF JhoFe or **Yor** that Satter whether Ot waJ ZaB or FOUht he waJ aJhaSeZ to aJQ aDD the HDaFet JeeSeZ to DOXe ReFeath SetaD the SeaD oY whOEh he haZ PWJt HartaQeF haZ ReeF DaReDeZ DWFEheoF RWt there were SaFB HDaFetJ whOEh DOXeZ a JtaFZarZ tOSeJEaDe that tooQ Fo aEEoWFt **oY** the HerhaHJ OFEoFXeFOeFt aDterFatOoF oY ZaB aFZ FOUht. the rate oY HDaFetarB tWrFOFUJ ZOYYereZ, aFZ he ZOZ Fot QFow that oY traFtor

Step-6:
From the substitution table, we have to substitute “Y” with ‘m’. For this, “Yor”, “oY”, words are converted into “mor”, “om”. These words have no meaning. If we substitute “Y” with the closest letters of ‘m’ (‘u’, ‘w’, ‘g’, ‘c’, ‘f’), then only using ‘f’, we get some meaningful words (“for”, “of”). After substitution,

he waJ **Fot** EertaOF whether the JWF JhoFe or for that Satter whether Ot waJ ZaB or FOUht he waJ aJhaSeZ to aJQ aDD the HDaFet JeeSeZ to DOXe ReFeath SetaD the SeaD of whOEh he haZ PWJt HartaQeF haZ ReeF DaReDeZ DWFEheoF RWt there were SaFB HDaFetJ whOEh DOXeZ a JtaFZarZ

tOSeJEaDe that tooQ **Fo** aEEoWFt of the HerhaHJ OFEoFXeFOeFt aDterFatOoF of ZaB aFZ FOUht. the rate of HDaFetarB tWrFOFUJ ZOffereZ, aFZ he ZOZ Fot QFow that of traFtor

Step-7:

From the substitution table, we have to substitute “F” with ‘o’ for ‘Fot’, ‘Fo’ words. But ‘o’ already used. If we substitute “F” with the closest letters of ‘o’ (‘a’, ‘n’, ‘t’, ‘h’), then only using ‘n’, we get some meaningful words (‘not’, ‘no’). After substitution,

he waJ not EertaOn whether the JWn Jhone or for that Satter whether Ot waJ ZaB or nOUht he waJ aJhaSeZ to aJQ aDD the HDanet JeeSeZ to DOXe Reneath SetaD the SeaD of whOEh he haZ PWJt HartaQen **haZ** Reen DaReDeZ DWnEheon RWt there were SanB HDanetJ whOEh DOXeZ a JtanZarZ tOSeJEaDe that tooQ no aEEoWnt of the HerhaHJ OnEonXenOent aDternatOon of ZaB **anZ** nOUht. the rate of HDanetarB tWrnOnUJ ZOffereZ, anZ he ZOZ not Qnow that of trantor

Step-8:

From the substitution table, we have to substitute “Z” with ‘s’. For this, “haZ”, “anZ”, words are converted into “has”, “ans”. Here “ans” have no meaning. If we substitute “Z” with the closest letters of ‘s’ (‘i’, ‘r’, ‘h’, ‘d’), then only using ‘d’, we get some meaningful words (“had”, “and”). After substitution,

he waJ not EertaOn whether the JWn Jhone or for that Satter whether **Ot** waJ daB or nOUht he waJ aJhaSed to aJQ aDD the HDanet JeeSed to DOXe Reneath SetaD the SeaD of whOEh he had PWJt HartaQen had Reen DaReDed DWnEheon RWt there were SanB HDanetJ whOEh DOXed a Jtandard tOSeJEaDe that tooQ no aEEoWnt of the HerhaHJ OnEonXenOent aDternatOon of daB and nOUht. the rate of HDanetarB tWrnOnUJ **dOffered,** and he **dOd** not Qnow that of trantor

Step-9:

From the substitution table, we have to substitute “O” with ‘r’ for “Ot”, “dOffered”, “dOd” words. But ‘r’ already used. If we substitute “O” with the closest letters of ‘r’ (‘i’, ‘s’, ‘d’, ‘l’), then only using ‘i’, we get some meaningful words (“it”, “differed”, “did”). After substitution,

he waJ not Eertain whether the JWn Jhone or for that Satter whether it waJ daB or niUht he waJ aJhaSed to aJQ aDD the HDanet JeeSed to DiXe Reneath SetaD the SeaD of whiEh he had PWJt HartaQen had Reen DaReDed DWnEheon RWt there were SanB HDanetJ whiEh DiXed a Jtandard

tiSeJEaDe that **tooQ** no aEEoWnt of the HerhaHJ inEonXenient aDternation of daB and niUht. the rate of HDanetarB tWrninUJ differed, and he did not **Qnow** that of trantor

Step-10:

From the substitution table, we have to substitute "Q" with 'b'. For this, "tooQ", "Qnow", words are converted into "toob", "bnow". These words have no meaning. If we substitute "Q" with the closest letters of 'b' ('f', 'y', 'p', 'k'), then only using 'k', we get some meaningful words ("took", "know"). After substitution,

he **waJ** not Eertain whether the JWn **Jhone** or for that Satter whether it waJ daB or niUht he waJ aJhaSed to **aJk** aDD the HDanet JeeSed to DiXe Reneath SetaD the SeaD of whiEh he had PWJt Hartaken had Reen DaReDed DWnEheon RWt there were SanB HDanetJ whiEh DiXed a Jtandard tiSeJEaDe that took no aEEoWnt of the HerhaHJ inEonXenient aDternation of daB and niUht. the rate of HDanetarB tWrninUJ differed, and he did not know that of trantor

Step-11:

From the substitution table, we have to substitute "J" with 'l'. For this, "waJ", "Jhone","aJk" words are converted into "wal", "lhone","alk". These words have no meaning. If we substitute "J" with the closest letters of 'l' ('s', 'r', 'd', 'u', 'w'), then only using 's', we get some meaningful words ("was", "shone","ask"). After substitution,

he was not **Eertain** whether the sWn shone or for that Satter whether it was daB or niUht he was ashaSed to ask aDD the HDanet seeSed to DiXe Reneath SetaD the SeaD of **whiEh** he had PWst Hartaken had Reen DaReDed DWnEheon RWt there were SanB HDanets whiEh DiXed a standard tiSesEaDe that took no aEEoWnt of the HerhaHs inEonXenient aDternation of daB and niUht. the rate of HDanetarB tWrninUs differed, and he did not know that of trantor

Step-12:

From the substitution table, we have to substitute "E" with 'w' for "Eertain", "whiEh" words. But 'w' already used. If we substitute "E" with the closest letters of 'w' ('l', 'u', 'm', 'g', 'c'), then only using 'c', we get some meaningful words ("certain", "which"). After substitution,

he was not certain whether the sWn shone or for that **Satter** whether it was daB or niUht he was **ashaSed** to ask aDD the HDanet **seeSed** to DiXe Reneath SetaD the SeaD of which he had PWst Hartaken had Reen

DaReDed DWncheon RWt there were SanB HDanets which DiXed a standard tiSescaDe that took no accoWnt of the HerhaHs inconXenient aDternation of daB and niUht. the rate of HDanetarB tWrninUs differed, and he did not know that of trantor

Step-13:
From the substitution table, we have to substitute “S” with ‘g’. For this, “ashaSed”, “seeSed”, ”Satter” words are converted into “ashaged”, “seeged”,”gatter”. These words have no meaning. If we substitute “S” with the closest letters of ‘g’ (‘m’, ‘u’), then only using ‘m’, we get some meaningful words (“ashamed”, “seemed”, ”matter”). After substitution,

he was not certain whether the sWn shone or for that matter whether it was daB or niUht he was ashamed to ask aDD the HDanet seemed to DiXe **Reneath** metaD the meaD of which he had PWst Hartaken had Reen DaReDed DWncheon RWt there were manB HDanets which DiXed a standard timescaDe that took no accoWnt of the HerhaHs inconXenient aDternation of daB and niUht. the rate of HDanetarB tWrninUs differed, and he did not know that of trantor

Step-14:
From the substitution table, we have to substitute “R” with ‘p’. For this, “Reneath”, “Reen” words are converted into “peneath”, “peen”. These words have no meaning. If we substitute “R” with the closest letters of ‘p’ (‘b’, ‘k’), then only using ‘b’, we get some meaningful words (“beneath”, “been”). After substitution,

he was not certain whether the sWn shone or for that matter whether it was daB or niUht he was ashamed to ask **aDD** the HDanet seemed to DiXe beneath **metaD** the **meaD** of which he had PWst Hartaken had been DabeDed DWncheon bWt there were manB HDanets which DiXed a standard timescaDe that took no accoWnt of the HerhaHs inconXenient aDternation of daB and niUht. the rate of HDanetarB tWrninUs differed, and he did not know that of trantor

Step-15:
From the substitution table, we have to substitute “D” with ‘d’ for “aDD”, “metaD”, “meaD” words. But ‘d’ already used. If we substitute “D” with the closest letters of ‘d’ (‘l’, ‘g’), then only using ‘l’, we get some meaningful words (“all”, “metal”, “meal”). After substitution,

he was not certain whether the **sWn** shone or for that matter whether it was daB or niUht he was ashamed to ask all the Hlanet seemed to liXe beneath metal the meal of which he had PWst Hartaken had been labeled **lWncheon** bWt there were manB Hlanets which liXed a standard timescale that took no **accoWnt** of the HerhaHs inconXenient alternation of daB and niUht. the rate of HlanetarB tWrninUs differed, and he did not know that of trantor

Step-16:
From the substitution table, we have to substitute "W" with 'f' for "sWn", "lWncheon", "accoWnt" words. But 'f' already used. If we substitute "W" with the closest letters of 'f' ('u', 'g'), then only using 'u', we get some meaningful words ("sun", "luncheon", "account"). After substitution,

he was not certain whether the sun shone or for that matter whether it was daB or niUht he was ashamed to ask all the **Hlanet** seemed to liXe beneath metal the meal of which he had Pust **Hartaken** had been labeled luncheon but there were manB Hlanets which liXed a standard timescale that took no account of the **HerhaHs** inconXenient alternation of daB and niUht. the rate of HlanetarB turninUs differed, and he did not know that of trantor

Step-17:
From the substitution table, we have to substitute "H" with 'c' for "Hlanet", "Hartaken", "HerhaHs" words. But 'c' already used. If we substitute "H" with the closest letters of 'c' ('p', 'g'), then only using 'p', we get some meaningful words ("planet", "partaken", "perhaHs"). After substitution,

he was not certain whether the sun shone or for that matter whether it was daB or niUht he was ashamed to ask all the planet seemed to **liXe** beneath metal the meal of which he had Pust partaken had been labeled luncheon but there were manB planets which **liXed** a standard timescale that took no account of the perhaps **inconXenient** alternation of daB and niUht. the rate of planetarB turninUs differed, and he did not know that of trantor

Step-18:

From the substitution table, we have to substitute “X” with ‘v’ for “liXe”, “inconXenient”, “liXed” words. We get some meaningful words (“live”, “inconvenient”, “lived”). After substitution,

he was not certain whether the sun shone or for that matter whether it was **daB** or niUht he was ashamed to ask all the planet seemed to live beneath metal the meal of which he had Pust partaken had been labeled luncheon but there were **manB** planets which lived a standard timescale that took no account of the perhaps inconvenient alternation of daB and niUht. the rate of **planetarB** turninUs differed, and he did not know that of trantor

Step-19:

From the substitution table, we have to substitute “B” with ‘y’ for “daB”, “manB”, “planetarB” words. We get some meaningful words (“day”, “many”, “planetary”). After substitution,

he was not certain whether the sun shone or for that matter whether it was day or **niUht** he was ashamed to ask all the planet seemed to live beneath metal the meal of which he had **Pust** partaken had been labeled luncheon but there were many planets which lived a standard timescale that took no account of the perhaps inconvenient alternation of day and niUht. the rate of planetary turninUs differed, and he did not know that of trantor

Step-20:

Rest of the letters “U”, “P” are substituted with ‘g’, ‘j’. After substitution,

he was not certain whether the sun shone or for that matter whether it was day or night he was ashamed to ask all the planet seemed to live beneath metal the meal of which he had just partaken had been labeled luncheon but there were many planets which lived a standard timescale that took no account of the perhaps inconvenient alternation of day and night. the rate of planetary turnings differed, and he did not know that of trantor

Problem-2(Cipher-2)

The ciphertext has been encrypted with Monoalphabetic Substitution Cipher. First we find out the alphabet's frequency from the ciphertext.

U	(234) 12.6%	T	(48) 2.6%
V	(178) 9.6%	G	(47) 2.5%
E	(146) 7.9%	O	(43) 2.3%
L	(139) 7.5%	K	(42) 2.3%
H	(136) 7.3%	N	(30) 1.6%
S	(136) 7.3%	P	(24) 1.3%
C	(112) 6%	Z	(21) 1.1%
M	(109) 5.9%	A	(14) 0.8%
F	(103) 5.5%	R	(8) 0.4%
D	(90) 4.8%	X	(8) 0.4%
Y	(86) 4.6%	J	(2) 0.1%
B	(51) 2.7%	Q	(1) 0.1%
I	(48) 2.6%	W	(1) 0.1%

The alphabets' frequency in this order in standard English,

e	t	a	o	n	h	i	s	r	d	l	u	w	m	g	c	f	y	b	p	k	v	j	x	q	z

Substitution table:

U	V	E	L	H	S	C	M	F	D	Y	B	I	T	G	O	K	N	P	Z	A	R	X	J	Q	W
e	t	a	o	n	h	i	s	r	d	l	u	w	m	g	c	f	y	b	p	k	v	j	x	q	z

Step-1:
The most frequent letters here are U, V, E, L, H. We substitute these letters with e, t, a, o, n. After substitution,

tDeMe NaC a NaFF aDeaY **St** ZeOan DSOD **Sn** tDe aSM anY eRtenYeY BKNaMY oBt oI CSODt St NaC MSYYFeY NStD DoFeC tDat NeMe tDe GoBtDC oI tBnneFC OaaF'C taRS GoAeY toNaMY one……

Step-2:
From the substitution table, we have to substitute “S” with ‘h’. For this, “St”, “ Sn”, “Snto”, words are converted into “ht”, “ hn”, “hnto”. These words have no meaning. If we substitute “S” with the closest letters of ‘h’ (‘o’, ‘i’), then only using ‘i’, we get some meaningful words (“it”, “ in”, “into”). After substitution,

tDeMe NaC a NaFF aDeaY it ZeOan DiOD in **tDe** aiM anY eRtenYeY BKNaMY oBt oI CiODt it NaC MiYYFeY NitD DoFeC **tDat** NeMe tDe GoBtDC oI tBnneFC OaaF'C taRi GoAeY toNaMY one……

Step-3:
From the substitution table, we have to substitute “D” with ‘d’. For this, “tDe”, “ tDat”, “tDen”, words are converted into “tde”, “ tdat”, “tden”. These words have no meaning. If we substitute “D” with the closest letters of ‘d’ (‘h’, ‘s’, ‘r’, ‘l’), then only using ‘h’, we get some meaningful words (“the”, “ that”, “then”). After substitution,

theMe NaC a NaFF aheaY it ZeOan hiOh in the aiM anY eRtenYeY BKNaMY oBt oI CiOht it NaC MiYYFeY Nith hoFeC that NeMe the GoBthC oI tBnneFC OaaF'C taRi GoAeY toNaMY one then KFBnOeY into it IoM a GoGent OaaF NonYeMeY iYFP hoN **hiC** YMiAeM……

Step-4:

From the substitution table, we have to substitute “C” with ‘i’ for “hiC”, “Co”,”Ceen” words. But ‘i’ already used. If we substitute “C” with the closest letters of ‘i’ (‘s’, ‘r’), then only using ‘s’, we get some meaningful words (“his”, “so”,”seen”). After substitution,

theMe Nas a NaFF aheaY it ZeOan **hiOh** in the aiM anY eRtenYeY BKNaMY oBt oI **siOht** it Nas MiYYFeY Nith hoFes that NeMe the GoBths oI tBnneFs OaaF's taRi GoAeY toNaMY one……

Step-5:
From the substitution table, we have to substitute “O” with ‘c’. For this, “hiOh”, “ siOht”, “aOainst”, words are converted into “hich”, “ sicht”, “acainst”. These words have no meaning. If we substitute “O” with the closest letters of ‘c’ (‘g’, ‘f’), then only using ‘g’, we get some meaningful words (“high”, “ sight”, “against”). After substitution,

theMe Nas a NaFF aheaY it Zegan high in the aiM anY eRtenYeY BKNaMY oBt oI sight it Nas MiYYFeY Nith **hoFes** that NeMe the GoBths oI tBnneFs **gaaF's** taRi GoAeY toNaMY one……

Step-6:
From the substitution table, we have to substitute “F” with ‘r’. For this, “gaaF's”, “ Fight”, “hoFes”, “signaF” words are converted into “gaar's”, “ right”, “hores”, “signar”. Here “gaar's”,“signar” has no meaning. If we substitute “F” with the closest letters of ‘r’ (‘d’, ‘l’), then only using ‘l’, we get some meaningful words (“gaal's”, “ light”, “holes”, “signal”). After substitution,

theMe Nas a Nall **aheaY** it Zegan high in the aiM **anY** eRtenYeY BKNaMY oBt oI sight it Nas MiYYleY Nith holes that NeMe the GoBths oI tBnnels gaal's taRi GoAeY toNaMY one……

Step-7:
From the substitution table, we have to substitute “Y” with ‘l’ for “aheaY”, “anY”,”leaneY” words. But ‘l’ already used. If we substitute “Y” with the closest letters of ‘l’ (‘d’, ‘u’), then only using ‘d’, we get some meaningful words (“ahead”, “and”,”leaned”). After substitution,

theMe Nas a Nall ahead it Zegan high in the **aiM** and eRtended BKNaMd oBt oI sight it Nas Middled Nith holes that NeMe the GoBths oI tBnnels gaal's taRi GoAed toNaMd one……

Step-8:
From the substitution table, we have to substitute “M” with ‘s’ for “theMe”, “aiM”,”Mising” words. But ‘s’ already used. If we substitute “M” with the closest letters of ‘s’ (‘r’, ‘u’), then only using ‘r’, we get some meaningful words (“there”, “air”,”rising”). After substitution,

there Nas a Nall ahead it Zegan high in the air and eRtended BKNard **oBt** oI sight it Nas riddled Nith holes that Nere the GoBths oI **tBnnels** gaal's taRi GoAed toNard one……

Step-9:
From the substitution table, we have to substitute “B” with ‘u’ for “oBt”, “tBnnels”, “soBnd” words. We get some meaningful words (“out”, “tunnels”, “sound”). After substitution,

there Nas a Nall ahead it Zegan high in the air and eRtended uKNard out oI sight it Nas riddled Nith holes that Nere the **Gouths** oI tunnels gaal's taRi GoAed toNard one……

Step-10:
From the substitution table, we have to substitute “G” with ‘g’ for “Gouths”, “glooG”, ”GoGent” words. But ‘g’ already used. If we substitute “G” with the closest letters of ‘g’ (‘m’, ‘c’), then only using ‘m’, we get some meaningful words (“mouths”, “gloom”, ”moment”). After substitution,

there Nas a Nall ahead it Zegan high in the air and eRtended uKNard out oI sight it Nas riddled Nith holes that Nere the mouths oI tunnels gaal's taRi moAed toNard one then Klunged into it Ior a moment gaal Nondered **idlP** hoN his driAer Tould KiTX out one among so **manP** there Nas noN **onlP** ZlaTXness……

Step-11:
From the substitution table, we have to substitute “P” with ‘b’. For this, “idlP”, “ manP”, “onlP”, words are converted into “idlb”, “ manb”, “onlb”. These words have no meaning. If we substitute “P” with the closest letters of ‘b’ (‘y’, ‘p’), then only using ‘y’, we get some meaningful words (“idly”, “ many”, “only”,). After substitution,

there Nas a Nall ahead it Zegan high in the air and eRtended uKNard out **oI** sight it Nas riddled Nith holes that Nere the mouths oI tunnels gaal's taRi moAed toNard one, then Klunged into it **Ior** a moment gaal Nondered idly hoN his driAer Tould KiTX out one among so many there Nas noN……

Step-12:
From the substitution table, we have to substitute “I” with ‘w’. For this, “Ior”, “ oI”, “Ilashing”, words are converted into “wor”, “ ow”, “wlashing”. These words have no meaning. If we substitute “I” with the closest letters of ‘w’ (‘c’, ‘f’), then only using ‘f’, we get some meaningful words (“for”, “ of”, “flashing”). After substitution,

there Nas a Nall ahead it Zegan high in the air and eRtended uKNard out of sight it Nas riddled Nith holes that Nere the mouths of tunnels gaal's taRi moAed toNard one, then Klunged into it for a moment gaal Nondered idly hoN his driAer Tould KiTX out one among so many there Nas noN only ZlaTXness Nith nothing Zut the Kast-flashing of a **Tolored** signal light……

Step-13:
From the substitution table, we have to substitute “T” with ‘m’ for “Tolored”, “deTeleration”, ”desTended” words. But ‘m’ already used. If we substitute “T” with the closest letters of ‘m’ (‘c’, ‘w’), then only using ‘c’, we get some meaningful words (“colored”, “deceleration”, ”descended”). After substitution,

there Nas a Nall ahead it Zegan high in the air and eRtended uKNard out of sight it Nas riddled Nith holes that Nere the mouths of tunnels gaal's taRi moAed toNard one, then **Klunged** into it for a moment gaal Nondered idly……

Step-14:
From the substitution table, we have to substitute “K” with ‘f’ for “Klunged”, “Kast”, “KoKKed” words. But ‘f’ already used. If we substitute “K” with the closest letters of ‘f’ (‘w’, ‘p’), then only using ‘p’, we get some meaningful words (“plunged”, “past”, “popped”). After substitution,

there **Nas** a **Nall** ahead it Zegan high in the air and eRtended upNard out of sight it Nas riddled **Nith** holes that Nere the mouths of tunnels gaal's taRi moAed toNard one then plunged into it for a moment gaal Nondered idly hoN his driAer could picX out one among so many there Nas noN only ZlacXness Nith nothing Zut the past……

Step-15:

From the substitution table, we have to substitute "N" with 'y' for "Nas", "Nall", "Nith" words. But 'y' already used. If we substitute "N" with the closest letters of 'y' ('w', 'b'), then only using 'w', we get some meaningful words ("was", "wall", "with"). After substitution,

there was a wall ahead it Zegan high in the air and eRtended upward out of sight it was riddled with holes that were the mouths of tunnels gaal's taRi moAed toward one……

Step-16:

Finally substitute "Z", "A", "R", "X", "J", "Q", "W" with 'b', 'v', 'x', 'k', 'q', 'z', 'j'. After substitution,

there was a wall ahead it began high in the air and extended upward out of sight it was riddled with holes that were the mouths of tunnels gaal's taxi moved toward one, then plunged into it for a moment gaal wondered idly how his driver could pick out one among so many there was now only blackness with nothing but the past-flashing of a colored signal light to relieve the gloom the air was full of a rushing sound gaal leaned forward against deceleration then and the taxi popped out of the tunnel and descended to ground-level once more the luxor hotel said the driver unnecessarily he helped gaal with his baggage accepted a tenth-credit tip with a businesslike air picked up a waiting passenger and was rising again in all this from the moment of debarkation there had been no glimpse of sky trantor at the beginning of the thirteenth millennium this tendency reached its climax as the center of the imperial government for unbroken hundreds of generations and located as it was toward the central regions of the galaxy among the most densely populated and industrially advanced worlds of the system, it could scarcely help being the densest and richest clot of humanity the race had ever seen its urbanization, progressing steadily had finally reached the ultimate. all the land surface of trantor square miles in extent was a single city the population at its height was well in excess of forty billions this enormous population was devoted

almost entirely to the administrative necessities of empire and found themselves all too few for the complications of the task (it is to be remembered that the impossibility of proper administration of the galactic empire under the uninspired leadership of the later emperors was a considerable factor in the fall) daily fleets of ships in the tens of thousands brought the produce of twenty agricultural worlds to the dinner tables of trantor its dependence upon the outer worlds for food and indeed for all necessities of life made trantor increasingly vulnerable to conquest by siege in the last millennium of the empire the monotonously numerous revolts made emperor after emperor conscious of this and imperial policy became little more than the protection of trantor's delicate jugular vein

Second one is easier than the first one. Here in Second one, after replacing the first five most frequent letters with universal order, assuming meaningful words was more easier to swap than the first one. That's why, it seems pretty easier to break.

Problem-3

For the Vigenere cryptosystem

Encryption:

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

Decryption:

$$D_i = (E_i - K_i) \ mod \ 26$$

Representation of plaintext and ciphertext characters in Z_{26}

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	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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

For encryption,

Input: Ethereum is an open-source, public, blockchain-based distributed computing platform and operating system featuring smart contract functionality

Key: pinkfloyd

For 1st letter,

Plaintext = E, value of “E” = 4

Key = p, value of “p” = 15

So, output is:

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

$$E_1 = (P_1 + K_1) \ mod \ 26$$

$$E_1 = (4 + 15) \ mod \ 26$$

E_1 = 19

Value 19 is assigned for “ t ”.

After calculating the values of P_i, K_i, E_i are as follows,

P_i	E	t	h	e	r	e	u	m	i	s	a	n	o	p	e	n	s	o	u
Value	4	19	7	4	17	4	20	12	8	18	0	13	14	15	4	13	18	14	20
K_i	p	i	n	k	f	l	o	y	d	p	i	n	k	f	l	o	y	d	p
Value	15	8	13	10	5	11	14	24	3	15	8	13	10	5	11	14	24	3	15
E_i	19	1	20	14	22	15	8	10	11	7	8	0	24	20	15	1	16	17	9
Output	t	b	u	o	w	p	i	k	l	h	i	a	y	u	p	b	q	r	j

For decryption,

Input: `tbuowpik lh ia yupb-qrjzpo, ufpjlr, jyyhvqfdxv-okxpr blhbesgfhcg rwzzzewlj etndkzfk dcl bzjcorlco fixesk itigewtbe vbied hzbrupkg pzyqrldvnvnem`

Key: pinkfloyd

For 1st letter,

Plaintext = t, value of “t” = 19

Key = p, value of “p” = 15

So, output is:

$$D_i = (E_i - K_i) \ mod \ 26$$

$$D_1 = (E_1 - K_1) \ mod \ 26$$

$$D_1 = (19 - 15) \ mod \ 26$$

D_1 = 4

Value 4 is assigned for " E ".

After calculating the values of P_i, K_i, E_i are as follows,

E_i	t	b	u	o	w	p	i	k	l	h	i	a	y	u	p	b	q	r	j
Value	**19**	**1**	**20**	**14**	**22**	**15**	**8**	**10**	**11**	**7**	**8**	**0**	**24**	**20**	**15**	**1**	**16**	**17**	**9**
K_i	p	i	n	k	f	l	o	y	d	p	i	n	k	f	l	o	y	d	p
Value	**15**	**8**	**13**	**10**	**5**	**11**	**14**	**24**	**3**	**15**	**8**	**13**	**10**	**5**	**11**	**14**	**24**	**3**	**15**
D_i	4	19	7	4	17	4	20	12	8	18	0	13	14	15	4	13	18	14	20
Output	**E**	**t**	**h**	**e**	**r**	**e**	**u**	**m**	**i**	**s**	**a**	**n**	**o**	**p**	**e**	**n**	**s**	**o**	**u**