Caesar Shift Cipher

Theory:

Shift cipher can be achieved by rotating each letter by the key K.
For example - if K is 3, then :
Encryption: A → D, D → G, G → J ..... X → A
Decryption: A ← D, D ← G, G ← J ..... X ← A

The general formula for the encryption part: Enc(x) = (x + h) mod 26
The general formula for the decryption part: Dec(x) = (x - h) mod 26

Example: Key = 3 and Plaintext = 'ATTACK':

Problem with Shift ciphers:

- Not enough keys
- If we shift a letter 26 times, we get the same letter back.
    - o A shift of 27 is the same as a shift of 1, etc.
    - So we only have 25 keys (1 to 25).
- Therefore, easy to attack via brute force.

Cryptoanalysis of shift ciphers:

Cipher text: OVDTHUFWVZZPISLRLFZHYLAOLYL

Key Values	Possible Plaintext
1	NUCSGTEVUYYOHRKQKEYGXKZNKXK
2	MTBRFSDUTXXNGQJPJDXFWJYMJWJ
3	LSAQERCTSWWMFPIOICWEVIXLIVI
4	KRZPDQBSRVVLEOHNHBVDUHWKHUH
5	JQYOCPARQUUKDNGMGAUCTGVJGTG
6	IPXNBOZQPTTJCMFLFZTBSFUIFSF
7	**HOWMANYPOSSIBLEKEYSARETHERE**
8	GNVLZMXONRRHAKDJDXRZQDSGDQD
9	FMUKYLWNMQQGZJCICWQYPCRFCPC
10	ELTJXKVMLPPFYIBHBVPXOBQEBOB
11	DKSIWJULKOOEXHAGAUOWNAPDANA
12	CJRHVITKJNNDWGZFZTNVMZOCZMZ
13	BIQGUHSJIMMCVFYEYSMULYNBYLY

Procedure:

Colab Notebook Link: Lab 1 - Caesar Cipher_Substitution Cipher [Fall-2025]

1. **Complete** the decrypt_shift_cipher() and encrypt_shift_cipher() methods.
2. **Decrypt** the ciphertext = `"Pdeo Ykza Nqjo Kj Lqna Dkla Wjz XnwyQ SeBe"` and **find out** the value of the key using the decrypt_shift_cipher() method.
3. **Test** the obtained plaintext and **generate** all possible ciphertexts using the encrypt_shift_cipher() method.
4. Encrypt the given plaintext = `"I am Ironman"` using the summation of last 2 digits of your ID as the key

Monoalphabetic Substitution Cipher

Theory:

Consider we have the plain text “cryptography”. By using the substitution table shown below, we can encrypt our plain text as follows:

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

one permutation of the possible 26!

plaintext: c r y p t o g r a p h y
ciphertext: B S E Z W U C S J Z N E

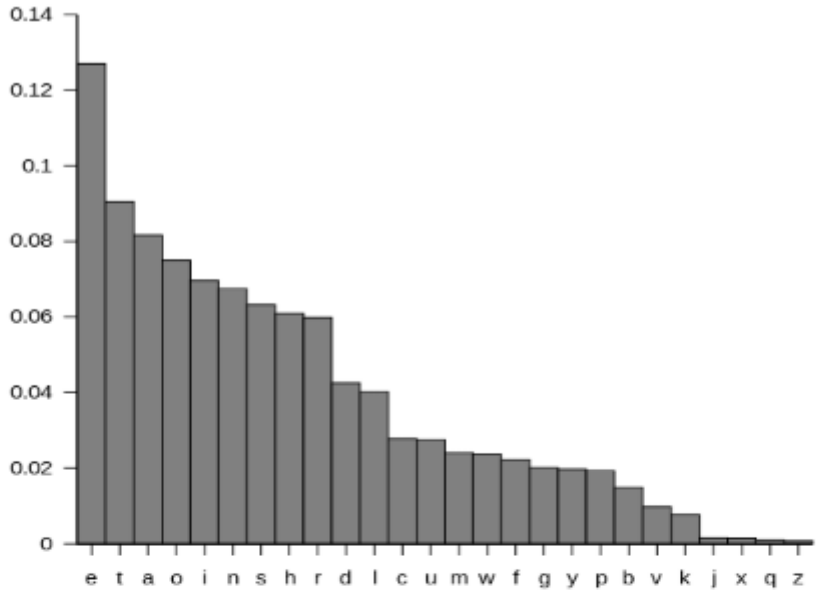
Hence we obtain the cipher text as “BSEZWUCSJZNE”

Cryptoanalysis:

Consider we have the following cipher text:
“LMCOTKOMSFKSWIMCQTGAUECTGKTGWFEZEWISKKTWG
VGWLLSDDOMCOTMCQSTOTGNSOWNCVSNRGCNSICN
WFKGWNCGDTQSKWEMCKSQSEDTQSYLMWMCKUEWFA
MOOMSKCNSCNWFGOWIKOFYRCGYWIGCOFECDOCDSGO
OWOMSYSOSJOTWGWIJETNSLMTJMTMCQSYWGSCGYLM
COTKOMSESKFDOOMSESTKGWJETNSOWYSOSJO”

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
2	0	20	7	11	8	17	0	6	5	14	6	17	10	24	0	6	2	28	18	2	2	20	0	7	1

Number of occurrences of each alphabet in the given ciphertext



English Letter Frequency (based on a sample of 40,000 words)

Top 10 beginning of word letters

Letter	Frequency
t	0.1594
a	0.155
i	0.0823
s	0.0775
o	0.0712
c	0.0597
m	0.0426
f	0.0408
p	0.040
w	0.0382

Top 10 end of word letters

Letter	Frequency
e	0.1917
s	0.1435
d	0.0923
t	0.0864
n	0.0786
y	0.0730
r	0.0693
o	0.0467
l	0.0456
f	0.0408

Most common bigrams (in order)

th, he, in, en, nt, re, er, an, ti, es, on, at, se, nd, or, ar, al, te, co, de, to, ra, et, ed, it, sa, em, ro.

Most common trigrams (in order)

the, and, tha, ent, ing, ion, tio, for, nde, has, nce, edt, tis, oft, sth, men

In the given cipher, we observe that ‘S’ has the highest count followed by ‘O’ Hence we make the substitutions S=e and O=t. Similarly we have C=a, W=o and T=I

“lmatiktmefkeoimaqigaueaigkigofezeoiekkiog ivgolleddtmatimaqeitignetonavenrganeian ofkgonagdiqekoemakeqeediqeylmomakueofa mttmekaneanofgtoiktfyragyoigatfeadtadegt totmeyetejtiogoijeinelmijmimaqeyogeagylm atiktmeeekfdttmeeeikgojeinetoyetejt”

In the above text we observe many trigrams ‘tMe’ which would be ‘the’ and so we can use M=h and obtain the new text as follows

“LhatiKtheFKeolhaQiGAUEaiGKiGoFEZEoleKKioG
iVGoLLeDDthatihaQeitiGNetoNaVeNRGaNelaN
oFKGoNaGDiQeKoEhaKeQeEDiQeYLhohaKUEoFA ht
theKaNeaNoFGtolKtFYRaGYolGatFEaDtaDeGt to the
YeteJtioGolJEiNeLhiJhihaQeYoGeaGYLh atiKtheEeKFDttheEeiKGoJEiNetoYeteJt”

We find ‘Lhat’ at 2 places which can be guessed to be ‘what’ and so we know that L=w. We make these substitutions in our text

“ what iK the FKeolhaQiGAUEaiGKiGoFEZEoleKKioG
iVGowweDDthatihaQeitiGNetoNaVeNRGaNelaN
oFKGoNaGDiQeKoEhaKeQeEDiQeYwhohaKUEoFA
httheKaNeaNoFGtolKtFYRaGYolGatFEaDtaDeGt to the
YeteJtioGolJEiNewhiJhihaQeYoGeaGYwh atiKtheEeKFDttheEeiKGoJEiNetoYeteJt”

Now clearly K=s. Also ‘YeteJt’ would be ‘detect’ and ‘YeteJtioG’ would be ‘detection’ So Y=d and J=c and G=n

“ what is the FseolhaQinAUEainsinoFEZEolession iVnowweDD that I haQe it in Ne to NaVeNRnaNelaN oFsnoNanDiQesoE has eQeEDiQed who has UEoFA ht the saNeaNoFntolstFdR and olnatFEaDtaDent to the detectionolcEiNe which i haQe done and what is the EesFDttheEe is no cEiNe to detect”

A little inspection of the above text would suggest that : F=u, Q=v , A=g and E=r. Also we find many digrams ‘ol’ which we can safely deduce to be ‘of’ and so l=f.

“ what is the use of having Urains in our Zr of ession i VnowweDD that i have it in Ne to NaVeNRnaNefaN ous no NanDives or has ever Dived who has Uroug ht the saNeaNount of studR and of naturaDtaDent to the detection of criNe which i have done and what is the resuDtthere is no criNe to detect”

Now it is easy to make the remaining substitutions by just observing the text and we finally get our plain text as follows

“ what is the use of having brains in our profession. I know well that I have it in me to make my name famous. No man lives, or has ever lived, who has brought the same amount of study and of natural talent to the detection of crime, which i have done And what is the result There is no crime to detect”

Procedure:

Colab Notebook Link: Lab 1 - Caesar Cipher_Substitution Cipher [Fall-2025]

Decrypt the given ciphertext, the function for calculating frequency count and bar chart is given for you.

```
ciphertext = "awbix ildxz kolf a dkzeplld afu zbjjbfm lf bj bz a rwkx
iajxpobwwap zdlgbfm a ellgae.\n jex iajxpobwwap ykxzjblfz awbix afu zex
audbjz jl exp ikppxfj buxfjbjt ipbzbz, ildolkfuxu rt exp bfarbwbjt jl
pxdxdrxp a olxd.\n rxnlpx ipahwbfm ahat, jex iajxpobwwap jxwwz awbix jeaj
lfx zbux ln jex dkzeplld hbww dagx exp jawwxp afu jex ljexp zbux hbww dagx
exp zelpjxp.\n zex rpxagz lnn jhl obxixz npld jex dkzeplld.\n lfx zbux
dagxz exp zepbfg zdawwxp jeaf xcxp, hebwx afljexp iakzxz exp fxig jl mplh
ebme bfjl jex jpxxz, hexpx a obmxlf dbzjagxz exp nlp a zxpoxfj.\n hbje
zldx xnnlpj, awbix rpbfmz expzxwn raig jl exp kzkaw exbmej.\n zex zjkdrwxz
kolf a zdaww xzjajx afu kzxz jex dkzeplld jl pxaie a dlpx aooplopbajx
exbmej."
```