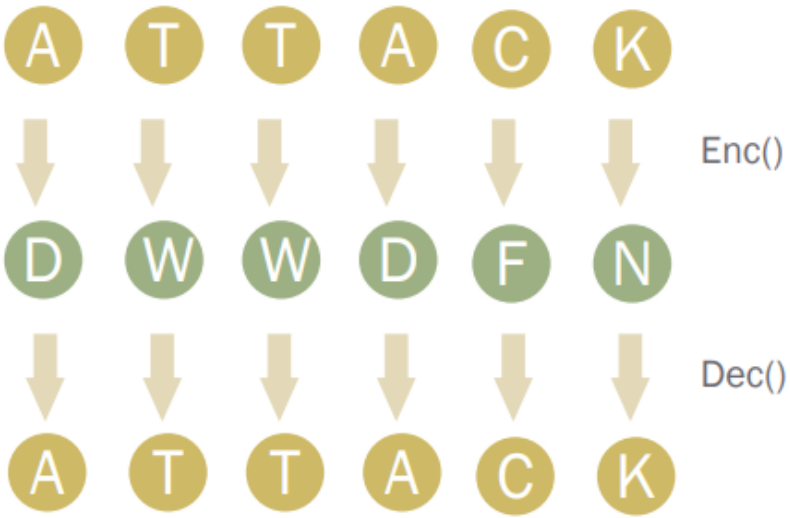
Caesar Shift Cipher

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 Ciphertext
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 for this lab:
https://drive.google.com/file/d/1Tmw95SIsjcuXobwUZi_0J_PLLrYGyoX9/view?usp=sharing

1. **Complete** the decrypt_shift_cipher() and encrypt_shift_cipher() methods.
2. **Decrypt** the ciphertext = `"KYV HLZTB SIFNE WFO"` 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 Batman"` using the summation of last 2 digits of your ID as the key

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

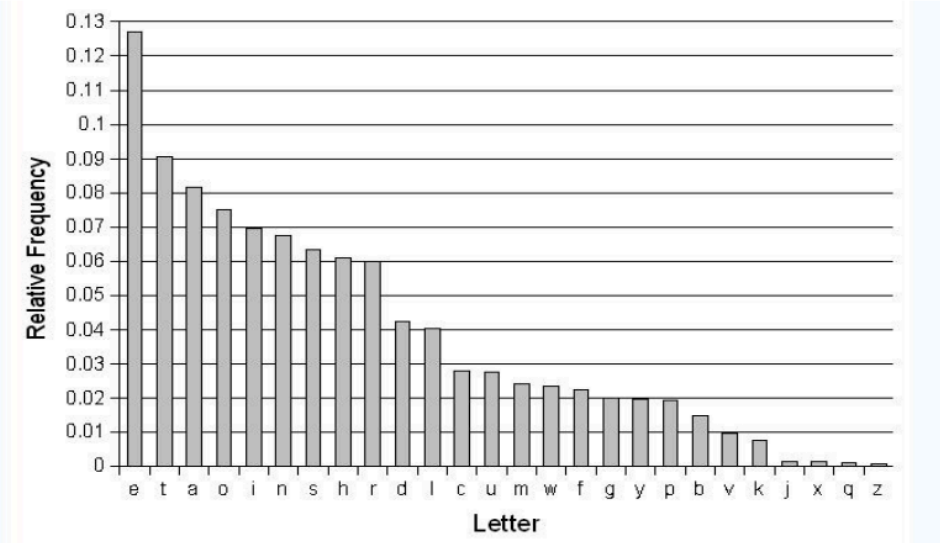
Hence we obtain the cipher text as “BSEZWUCSJZNE”

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 cipher text



Frequencies of occurrence of each alphabet in an eglish text

th	he	an	re	er	in	on	at	nd	st	es	en	of	te	ed
168	132	92	91	88	86	71	68	61	53	52	51	49	46	46

Most common English bigrams (frequency per 1000 words)

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

“LhatiKtheFKeoIhaQiGAUEaiGKiGoFEZEoIeKKioG
iVGoLLeDDthatihaQeitiGNetoNaVeNRGaNeIaN
oFKGoNaGDiQeKoEhaKeQeEDiQeYLhohaKUEoFA ht
theKaNeaNoFGtoIKtFYRaGYoIGatFEaDtaDeGt to the
YeteJtioGoIJEiNeLhiJhihaQeYoGeaGYLh 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 FKeoIhaQiGAUEaiGKiGoFEZEoIeKKioG
iVGowweDDthatihaQeitiGNetoNaVeNRGaNeIaN

oFKGoNaGDiQeKoEhaKeQeEDiQeYwhohaKUEoFA
httheKaNeaNoFGtoIKtFYRaGYoIGatFEaDtaDeGt to the
YeteJtioGoIJEiNewhiJhihaQeYoGeaGYwh 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 FseoIhaQinAUEainsinoFEZEoIession iVnowweDD that I haQe it in Ne to NaVeNRnaNeIaN oFsnoNanDiQesoE has eQeEDiQed who has UEoFA ht the saNeaNoFntoIstFdR and oInatFEaDtaDent to the detectionoIcEiNe 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 ‘oI’ which we can safely deduce to be ‘of’ and so I=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 for this lab:
https://drive.google.com/file/d/1Tmw95SlsjcuXobwUZi_0J_PLLrYGyoX9/view?usp=sharing

1. **Decrypt** the given ciphertext, the function for calculating frequency count is given for you.

```
ciphertext = "xeo iwy djqqod mohzs xeo ezfjrzy, glixjyc l slft, zflyco
chzs lgfzii xeo xflyawjh hlydiglqo.\n l coyxho mfooro fwixhod xeo holkoi
zv xeo xlhh zln xfooi, gfolxjyc l izzxejyc iutqezyu zv ylxwfo'i
tohzdjoi.\n li xsjhjcex doigoydod, xeo ixlfi mocly xz otofco, dzxxjyc xeo
jydjcz glykli zv xeo yjcex inu.\n vjfovhjoi dlygod jy xeo toldzs, xeojf
mjzhwtjyoigoyx hjcexi vhjgnofjyc hjno xjyu hlyxofyi.\n jy xeo djixlygo,
xeo vljyx ewt zv l djixlyx xfljy gzwhd mo eolfd, l fotjydof zv xeo szfhd
mouzyd xeji qolgovwh elkoy.\nl hzyo zsh ezzxod jy xeo djixlygo, mfolnjyc
xeo ijhoygo zv xeo yjcex.\n xeo igoyx zv vfoiehu mlnod mfold slvxod vfzt l
yolfmu gzxxlco, oyxjgjyc lyuzyo vzfxwylxo oyzwce xz glxge l sejvv.\n l
fjkof yolfmu chjixoyod jy xeo tzzyhjcex, jxi slxofi fjqqhjyc coyxhu li jx
vhzsod zyslfd.\n jx sli l tztoyx zv iofoyjxu lyd ixjhhyoii, l qlwio jy xeo
ewixho lyd mwixho zv hjvo, seofo zyo gzwhd ijtqhu opjix lyd ilkzf xeo
molwxu zv xeo szfhd lfzwyd xeot.\n"
```