# Caesar Shift Cipher

## Theory:

Shift cipher can be achieved by rotating each letter by the key K.

For example - if K is 3, then :

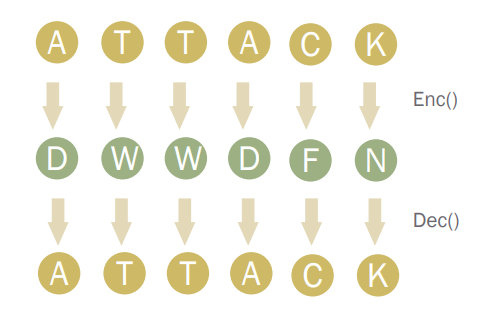
Encryption: A → D, D → G, G → J ……….….. X → A

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 |

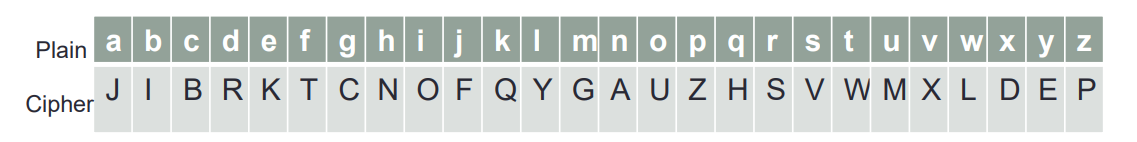
## Procedure:

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:



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

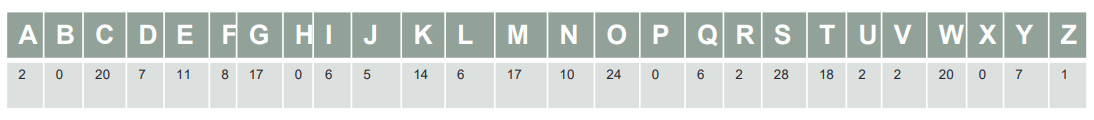
VGWLLSDDOMCOTMCQSTOTGNSOWNCVSNRGCNSICN

WFKGWNCGDTQSKWEMCKSQSEDTQSYLMWMCKUEWFA

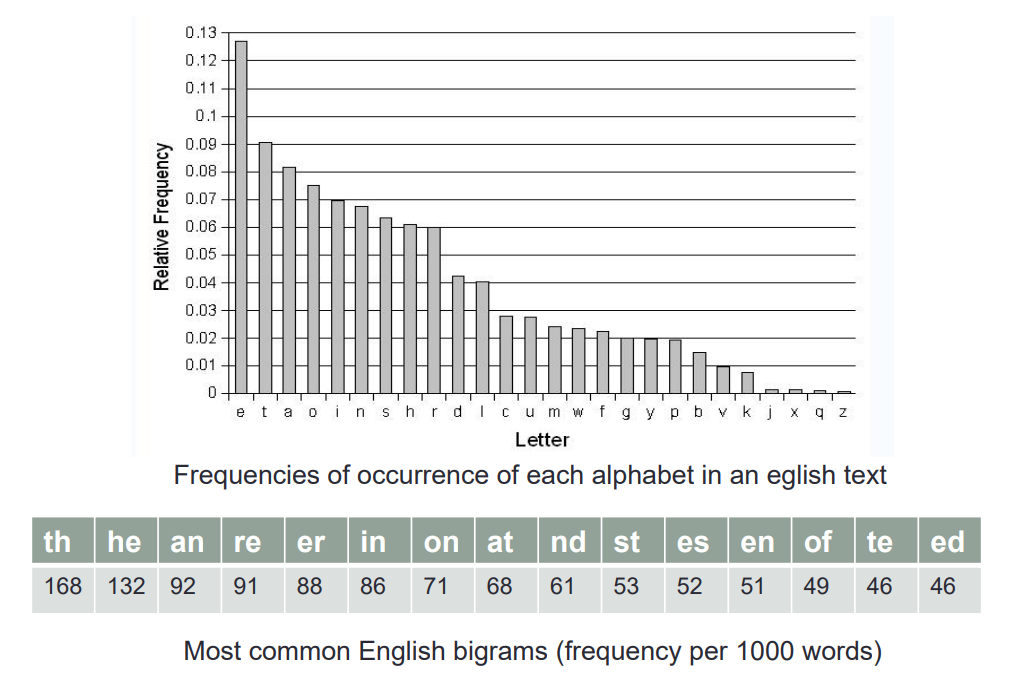
MOOMSKCNSCNWFGOWIKOFYRCGYWIGCOFECDOCDSGO

OWOMSYSOSJOTWGWIJETNSLMTJMTMCQSYWGSCGYLM

COTKOMSESKFDOOMSESTKGWJETNSOWYSOSJO”



Number of occurrences of each alphabet in the given cipher text



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:

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