B210473CS

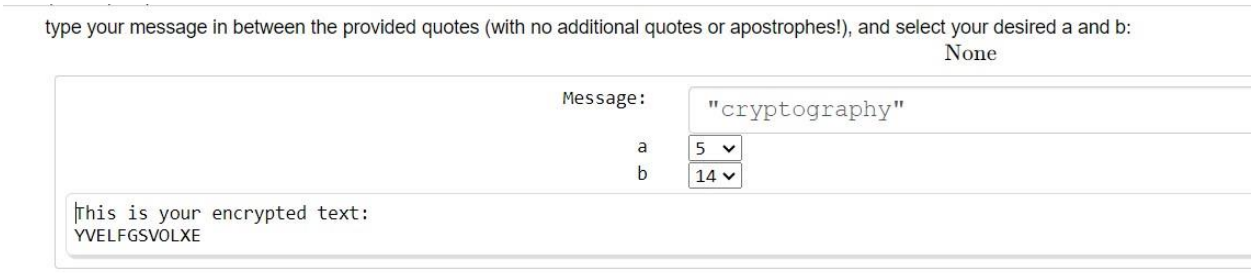
VIVEK K P

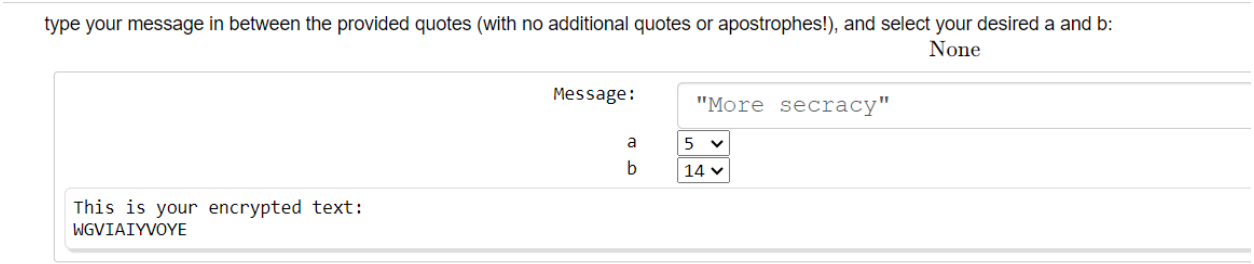
NTC ASSIGNMENT-1

1.Affine cipher

The value a is the multiplier and must be relatively prime to 26 in order to guarantee that each letter is encoded uniquely. The value b is the addend. Each letter's value is multiplied by a, and the product is added to b.

#Code is given as Affine_cipher.sage





The affine cipher encrypts a letter using the following mathematical formula:

C = (a * P + b) % 26

- C is the affine cipher text
- P is the plain text
- a is relatively prime to 26
- b is an integer

Decrypt the text

P = (a^(-1) * (C - b)) % 26

Here, "a^(-1)" is the modular multiplicative inverse of "a" modulo 26. You can calculate this using modular arithmetic.

Here modular multiplicative inverse of a means a*x%m=1 then the x should be the answer.

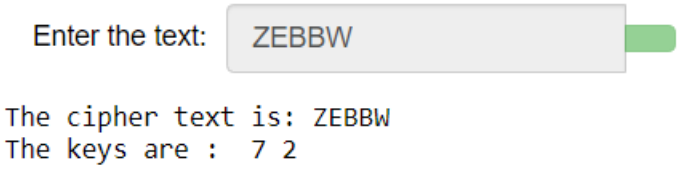
```
suppose if my letter is "abcd"

and key are x=5,y=2

a-> 1*5+2=7 :G
b-> 2*5+2=12 :L
c-> 3*5+2=17 :Q
d-> 4*5+2=22 :V

answer= GLQV
```

cryptanalysis:

1.Key search

Brute force: Since there are only 12 possible values for "a" that are relatively prime to 26 (1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25), we can try each of them in combination with all 26 possible values of "b." This results

in 312 (12 * 26) combinations to check.



Then by grammer analysis we an easily get it the words ,and then analysing the plain text and cipher text we can get it the key

Frequency analysis: If you have a sufficiently long ciphertext and you suspect it's an affine cipher, you can use frequency analysis to guess the key values. Look for patterns in the ciphertext, such as common letters or letter pairs that occur frequently, and use knowledge of English letter frequencies to make educated guesses about "a" and "b."

2.Key search and statistical analysis

We have 312 possible keys can generate here we will do statistical analysis and the find out the additive key used in her then remaining 12 possible multiplicative keys are there
So from there we can easily get the word.

2.Hill cipher

The Hill cipher is a polygraphic substitution cipher used for encrypting and decrypting text. Unlike simple substitution ciphers like the Caesar cipher, the Hill cipher operates on groups of letters (typically pairs or triplets) and uses matrix multiplication for encryption and decryption.

```
ENCRYPTION:

Block 1 (HE):
```

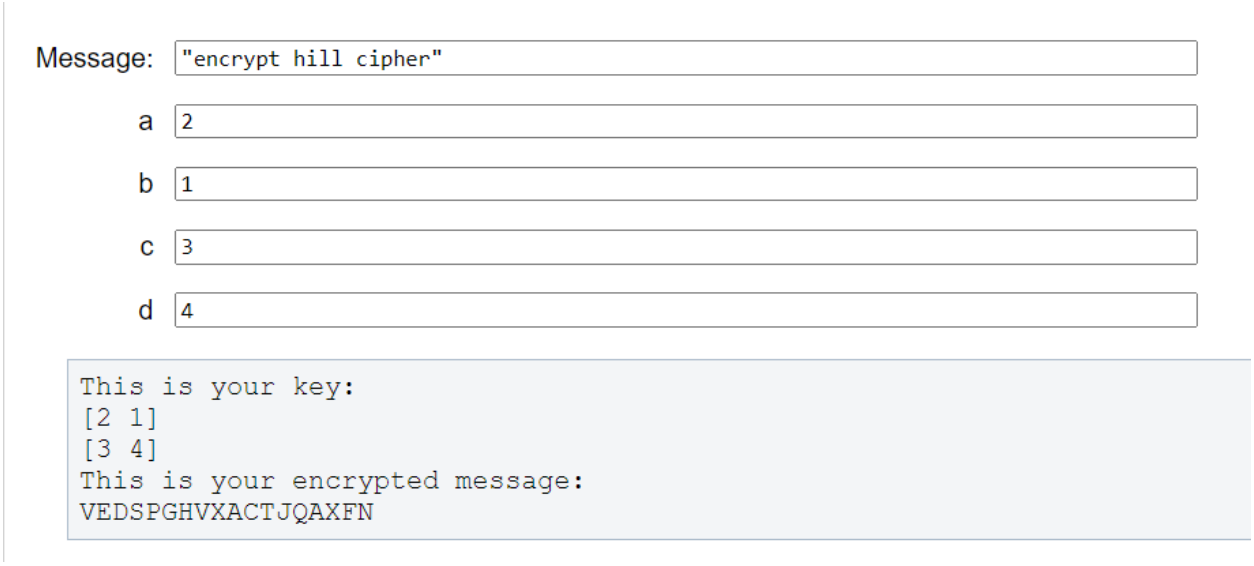
```
| H |
| E |

Block 2 (LL):
| L |
| L |

Encrypted Block 1 (HE):
| 6  24 |   | 7 |   | 198 |   | 16 |
| 13 16 | * | 4 | = | 536 | % | 16 |

Encrypted Block 2 (LL):
| 6  24 |   | 11 |   | 330 |   | 18  |
| 13 16 | * | 11 | = | 509 | % | 15  |

Ciphertext: OOQN
```

Here the matrix must be invertible means inverse must be possible.

Decryption:

To decrypt, you need the inverse of the key matrix, denoted as K^(-1).
Multiply the inverse key matrix by the encrypted block.
Take the result modulo the size of the alphabet to obtain the original plaintext block.
Mathematically, if the inverse key matrix is K^(-1), the encrypted block is C, and the decrypted block is P:

P = K^(-1) * C (mod 26)

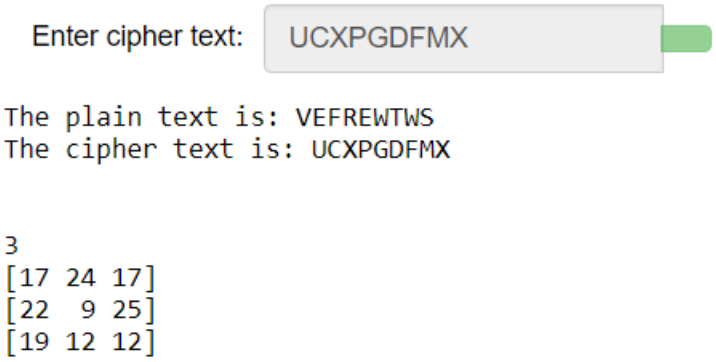


Cryptanalysis:

1.Brute Force Attack: One approach is to try all possible key matrices and check the decrypted text for meaningful words or phrases. This method becomes increasingly impractical as the size of the key matrix and the length of the ciphertext increase. For larger key matrices, the number of possibilities grows exponentially.

2. Known-Plaintext Attack: If an attacker has access to both the plaintext and corresponding ciphertext, they can use this information to deduce the

key matrix. By comparing the known plaintext and ciphertext blocks, the attacker can solve for the key matrix. This attack is effective if the attacker has enough known plaintext-ciphertext pairs.



3. Frequency Analysis: If the attacker knows or can make educated guesses about parts of the plaintext, they can use frequency analysis on the known or guessed parts to deduce parts of the key matrix. For example, if the attacker knows that the word "THE" appears frequently in English, they can analyze the ciphertext to find corresponding patterns and deduce parts of the key.

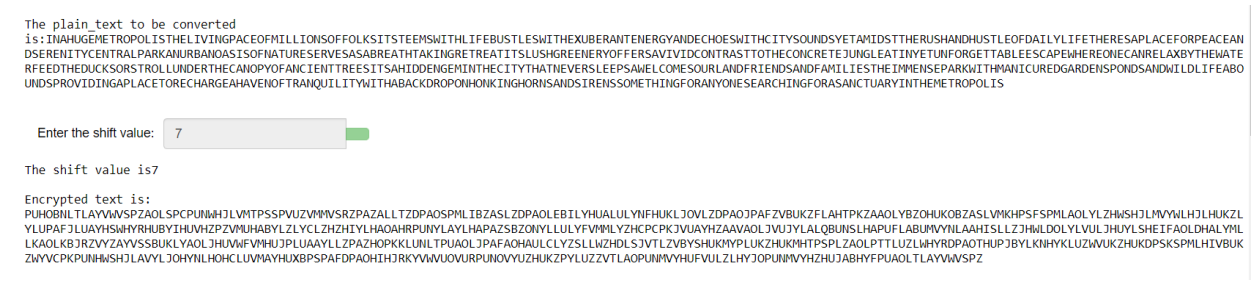
4.Matrix Algebra Techniques: Advanced mathematical techniques can be employed to recover the key matrix from the ciphertext and known plaintext, even when the key matrix is large. Techniques such as Gaussian elimination and linear algebra methods may be used.

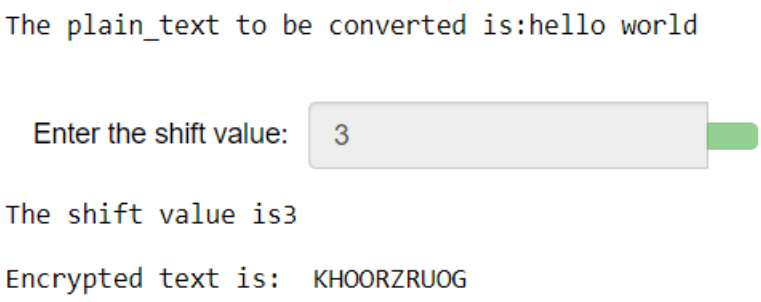
3.Shift Cipher

A shift cipher, also known as a Caesar cipher, is a simple and widely used encryption technique that involves shifting the letters of the alphabet by a fixed number of positions. It's a type of substitution cipher where each letter in the plaintext is replaced by a letter that is a fixed number of positions down or up the alphabet.

#Code is given as shift_cipher.sage

Encryption:





Decryption:

The decryption algorithm shifts 15 characters up (toward the beginning of the alphabet)

```
The plain_text to be converted is: KHOORZRUOG

Enter the shift value:  3

The shift value is3

Encrypted text is:  HELLOWORLD
```

```
The plain_text to be converted
is:PUHOBNLTLAYVWVSPZAOLSPCPUNWHJLVMTPSSPVUZVMMVSRZPAZALLTZDPAOSPMLIBZASLZDPAOLEBILYHUALULYNFHUKLJOVLZDPAOJPAFZVBUKZFLAHTPKZAAOLYBZOHUKOBZASLVMKHPSFSPMLAOLYLZHWSHJLMVYWLHJLHU
KZLYLUPAFJLUAYHSWHYRHUBYIHUVHZPZVMUHABYLZLYCLZHZHIYLHAOAHRPUNYLAYLHAPAZSBZONYLLULYFVMMLYZHCPCPKJVUAYHZAAVAOLJVUJYLALQBUNSLHAPUFLABUMVYNLAAHISLLZJHWLDOLYLVULJHUYLSHEIFAOLDHAL
YMLLKAOLKBJRZVYZAYVSSBUKLYAOLJHUVWFVMHUJPLUAAYLLZPAZHOPKKLUNLTPUAOLJPAFAOHAULCLYZSLLWZHDLSJVTLZVBYSHUKMYPLUKZHUKMHTPSPLZAOLPTTLUZLWHYRDPAOTHUPJBYLKNHYKLUZWVUKZHUKDPSKSPMLHIV
BUKZWYVCPKPUNHWSHJLAVYLJOHYNLHOHCLUVMAYHUXBPSPAFDPAOHIHJRKYVWVUOVURPUNOVYUZHUKZPYLUZZVTLAOPUNMVYHUFVULZLHYJOPUNMVYHZHUJABHYFPUAOLTLAYVWVSPZ

Enter the shift value:  7

The shift value is7

Encrypted text is:
INAHUGEMETROPOLISTHELIVINGPACEOFMILLIONSOFFOLKSITSTEEMSWITHLIFEBUSTLESWITHEXUBERANTENERGYANDECHOESWITHCITYSOUNDSYETAMIDSTTHERUSHANDHUSTLEOFDAILYLIFETHERESAPLACEFORPEACEANDSE
RENITYCENTRALPARKANURBANOASISOFNATURESERVESASABREATHTAKINGRETREATITSLUSHGREENERYOFFERSAVIVIDCONTRASTTOTHECONCRETEJUNGLEATINYETUNFORGETTABLEESCAPEWHEREONECANRELAXBYTHEWATERFE
EDTHEDUCKSORSTROLLUNDERTHECANOPYOFANCIENTTREESITSAHIDDENGEMINTHECITYTHATNEVERSLEEPSAWELCOMESOURLANDFRIENDSANDFAMILIESTHEIMMENSEPARKWITHMANICUREDGARDENSPONDSANDWILDLIFEABOUND
SPROVIDINGAPLACETORECHARGEAHAVENOFTRANQUILITYWITHABACKDROPONHONKINGHORNSANDSIRENSSOMETHINGFORANYONESEARCHINGFORASANCTUARYINTHEMETROPOLIS
```

CryptAnalysis:

1.Brute Force:

Additive ciphers are vulnerable to ciphertext-only attacks using exhaustive key searches (brute-force attacks). The key domain of the additive cipher is very small; there are only 26 keys. However, one of the keys, zero, is useless (the ciphertext is the same as the plaintext). This leaves only 25 possible keys. Eve can easily launch a bruteforce attack on the ciphertext.

Ciphertext: UVACLYFZLJBYL

K = 1	→	**Plaintext:** tuzbkxeykiaxk
K = 2	→	**Plaintext:** styajwdxjhzwj
K = 3	→	**Plaintext:** rsxzivcwigyvi
K = 4	→	**Plaintext:** qrwyhubvhfxuh
K = 5	→	**Plaintext:** pqvxgtaugewtg
K = 6	→	**Plaintext:** opuwfsztfdvsf
K = 7	→	**Plaintext:** notverysecure

2.Statstical analysis:

Additive ciphers are also subject to statistical attacks. This is especially true if the adversary has a long ciphertext. The adversary can use the frequency of occurrence of characters for a particular language.

```
The cipher_text is:
PUHOBNLTLAYVWVSPZAOLSPCPUNWHJLVMTPSSPVUZVMMVSRZPAZALLTZDPAOSPMLIBZASLZDPAOLEBILYHUALULYNFHUKLJOVLZDPAOJPAFZVBUKZFLAHTPKZAAOLYBZOHUKOBZASLVMKHPSFSPMLAOLYLZHWSHJLMVYWLHJLHUKZL
YLUPAFJLUAYHSWHYRHUBYIHUVHZPZVMUHABYLZLYCLZHZHIYLHAOAHRPUNYLAYLHAPAZSBZONYLLULYFVMMLYZHCPCPKJVUAYHZAAVAOLJVUJYLALQBUNSLHAPUFLABUMVYNLAAHISLLZJHWLDOLYLVULJHUYLSHEIFAOLDHALYML
LKAOLKBJRZVYZAYVSSBUKLYAOLJHUVWFVMHUJPLUAAYLLZPAZHOPKKLUNLTPUAOLJPAFAOHAULCLYZSLLWZHDLSJVTLZVBYSHUKMYPLUKZHUKMHTPSPLZAOLPTTLUZLWHYRDPAOTHUPJBYLKNHYKLUZWVUKZHUKDPSKSPMLHIVBUK
ZWYVCPKPUNHWSHJLAVYLJOHYNLHOHCLUVMAYHUXBPSPAFDPAOHIHJRKYVWVUOVURPUNOVYUZHUKZPYLUZZVTLAOPUNMVYHUFVULZLHYJOPUNMVYHZHUJABHYFPUAOLTLAYVWVSPZ
[[86, 11], [57, 7], [54, 0], [54, 20], [46, 15], [46, 24], [45, 25], [39, 21], [30, 14], [27, 18], [24, 10], [22, 9], [19, 12], [18, 1], [14, 13], [14, 22], [13, 5], [12,
19], [9, 3], [8, 8], [7, 2], [7, 17], [2, 4], [1, 16], [1, 23], [0, 6]]
The key is:  7
Encrypted text is:
INAHUGEMETROPOLISTHELIVINGPACEOFMILLIONSOFFOLKSITSTEEMSWITHLIFEBUSTLESWITHEXUBERANTENERGYANDECHOESWITHCITYSOUNDSYETAMIDSTTHERUSHANDHUSTLEOFDAILYLIFETHERESAPLACEFORPEACEANDSE
RENITYCENTRALPARKANURBANOASISOFNATURESERVESASABREATHTAKINGRETREATITSLUSHGREENERYOFFERSAVIVIDCONTRASTTOTHECONCRETEJUNGLEATINYETUNFORGETTABLEESCAPEWHEREONECANRELAXBYTHEWATERFE
EDTHEDUCKSORSTROLLUNDERTHECANOPYOFANCIENTTREESITSAHIDDENGEMINTHECITYTHATNEVERSLEEPSAWELCOMESOURLANDFRIENDSANDFAMILIESTHEIMMENSEPARKWITHMANICUREDGARDENSPONDSANDWILDLIFEABOUND
SPROVIDINGAPLACETORECHARGEAHAVENOFTRANQUILITYWITHABACKDROPONHONKINGHORNSANDSIRENSSOMETHINGFORANYONESEARCHINGFORASANCTUARYINTHEMETROPOLIS
```

My analaysing the bellow table we can easily get the most freq letter and corresponding key from that by analysing with the freq table given below

Crypt analysis code is given as in shift_crypt.sage

Letter	*Frequency*	*Letter*	*Frequency*	*Letter*	*Frequency*	*Letter*	*Frequency*
E	12.7	H	6.1	W	2.3	K	0.08
T	9.1	R	6.0	F	2.2	J	0.02
A	8.2	D	4.3	G	2.0	Q	0.01
O	7.5	L	4.0	Y	2.0	X	0.01
I	7.0	C	2.8	P	1.9	Z	0.01
N	6.7	U	2.8	B	1.5		
S	6.3	M	2.4	V	1.0		

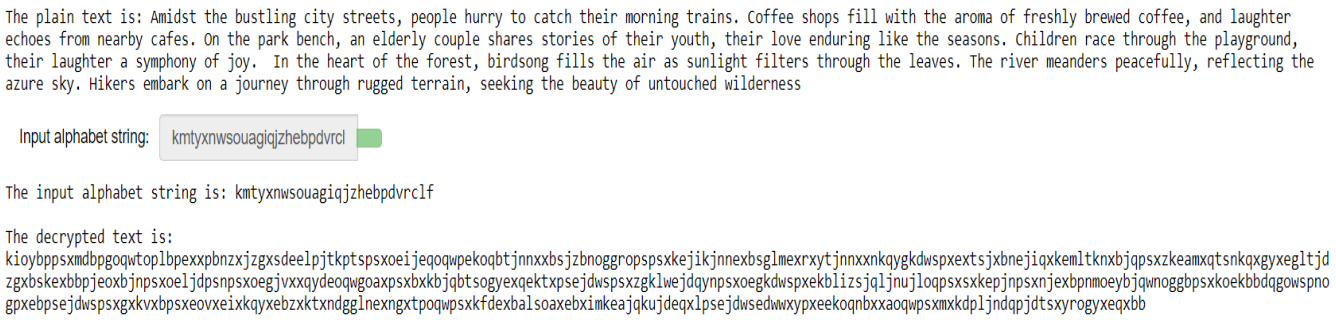
4. Substitution cipher

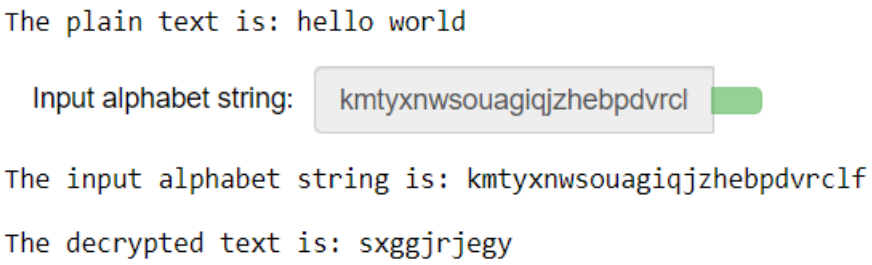
A substitution cipher replaces one symbol with another. If the symbols in the plaintext are alphabetic characters, we replace one character with another. For example, we can replace letter A with letter D, and letter T with letter Z. If the symbols are digits (0 to 9), we can replace 3 with 7, and 2 with 6. Substitution ciphers can be categorized as either monoalphabetic ciphers or polyalphabetic ciphers.

Here I implemented Monoalphabetic Substitution Cipher

Encryption:

Because additive, multiplicative, and affine ciphers have small key domains, they are very vulnerable to brute-force attack. The key is independent from the letters being transferred. A better solution is to create a mapping between each plaintext character and the corresponding ciphertext character. Alice and Bob can agree on a table showing the mapping for each character.





Decryption:

In decryption we just reversily take the order and then again get the plain text from the given cipher text.

```
The plain text is: sxggjrjegy
```

Input alphabet string: kmtyxnwsouagiqjzhebpdvrcl

```
The input alphabet string is: kmtyxnwsouagiqjzhebpdvrclf

The decrypted text is: helloworld


The plain text is: kzzgxmkqkqktsxeelykpxxgyxemxeelnowwekzxsjqxlyxraorogxijqikqwjqxtpkeoqxjekqwx
```

Input alphabet string: kmtyxnwsouagiqjzhebpdvrcl

```
The input alphabet string is: kmtyxnwsouagiqjzhebpdvrclf

The decrypted text is: applebananacherrydateelderberryfiggrapehoneydewkiwilemonmangonectarineorange
```

CryptAnalysis:

1.Brute force attack:

The size of the key space for the monoalphabetic substitution cipher is 26! (almost 4 × 1026). This makes a brute-force attack extremely difficult for Eve even if she is using a powerful computer. However, she can use statistical attack based on the frequency of characters. The cipher does not change the frequency of characters.

2.Known Plain text-attack:

In known plain text attack we know the plain_text and cipher text , and get it the key string by analysing both of them ,

```
The known plain text is: abcdefghijklmnopqrstuvwxyz
The known cipher text is: kmtyxnwsouagiqjzhebpdvrclf

Enter the text to be decrypted: sxggjsxexrxwj

The text to be decrypted is : sxggjsxexrxwj
The result after crypt analysis: helloherewego
```

```
The known plain text is: abcdefghijklmnopqrstuvwxyz
The known cipher text is: kmtyxnwsouagiqjzhebpdvrclf

Enter the text to be decrypted: kioybppsxmdbpgoqwtoplbpe

The text to be decrypted is :
kioybppsxmdbpgoqwtoplbpexxpbnzxjzgxsdeelpjtkptspsxoeijeqoqwpekoqbtjnnxxbsjzbnoggropspsxkejikjnnexbsglmexrxytjnnxxnkqygkdwspxextsjxbnejiqxkemltknxbjqpsxzkeamxqtsnkqxgyxegltjd
zgxbskexbbpjeoxbjnpsxoeljdpsnpsxoegjvxxqydeoqwgoaxpsxbxkbjqbtsogyexqektxpsejdwspsxzgklwejdqynpsxoegkdwspxekblizsjqljnujloqpsxsxkepjnpsxnjexbpnmoeybjqwnoggbpsxkoekbbdqgowspno
gpxebpsejdwspsxgxkvxbpsxeovxeixkqyxebzxktxndgglnexngxtpoqwpsxkfdexbalsoaxebximkeajqkujdeqxlpsejdwsedwwxypxeekoqnbxxaoqwpsxmxkdpljndqpjdtsxyrogyxeqxbb
The result after crypt analysis:
amidstthebustlingcitystreetsfpeoplehurrytocatchtheirmorningtrainscoffeeshopsfillwiththearomaoffreshlybrewedcoffeefandlaughterechoesfromnearbycafesontheparkbenchfanelderlycou
plesharesstoriesoftheiryouthftheirloveenduringliketheseasonschildrenracethroughtheplaygroundftheirlaughterasymphonyofjoyintheheartoftheforestfbirdsongfillstheairassunlightfi
ltersthroughtheleavestherivermeanderspeacefullyfreflectingtheazureskyhikersembarkonajourneythroughruggedterrainfseekingthebeautyofuntouchedwilderness
```

5. Transposition cipher

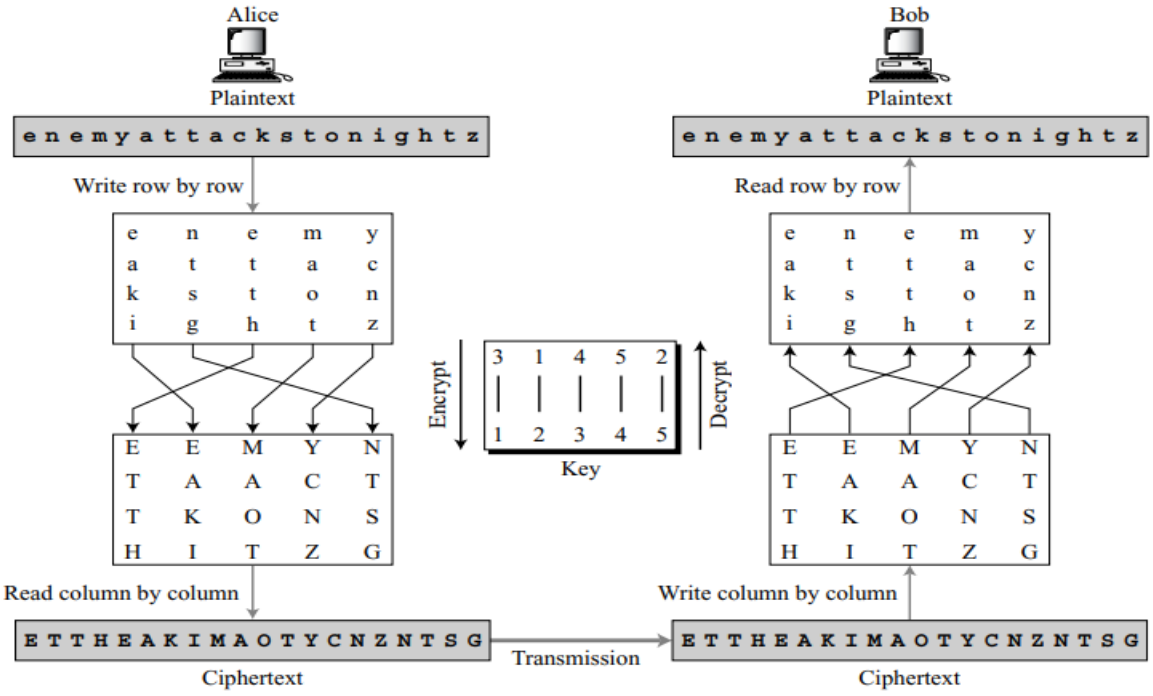
A transposition cipher does not substitute one symbol for another, instead it changes the location of the symbols. A symbol in the first position of the plaintext may appear in the tenth position of the ciphertext. A symbol in the eighth position in the plaintext may appear in the first position of the ciphertext. In other words, a transposition cipher reorders (transposes) the symbols.

There are two transposition ciphers are there

1.keyless transposition

2.keyed transposition

The keyless ciphers permute the characters by using writing plaintext in one way (row by row, for example) and reading it in another way (column by column, for example). The permutation is done on the whole plaintext to create the whole ciphertext. Another method is to divide the plaintext into groups of predetermined size, called blocks, and then use a key to permute the characters in each block separately



Encryption:

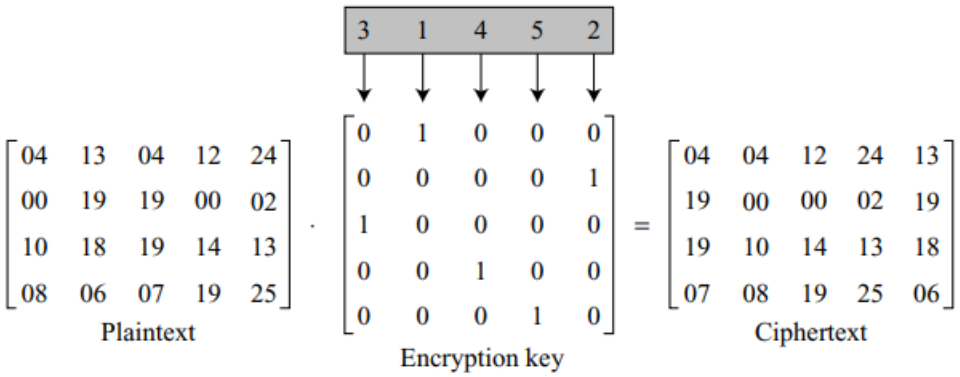
Using Matrices

We can use matrices to show the encryption/decryption process for a transposition cipher. The plaintext and ciphertext are $l \times m$ matrices representing the numerical values of the characters; the keys are square matrices of size $m \times m$. In a permutation matrix, every row or column has exactly one 1 and the rest of the values are 0s. Encryption is performed by multiplying the plaintext matrix by the key matrix to get the ciphertext matrix; decryption is performed by multiplying the ciphertext by the inverse

key matrix to get the plaintext matrix. A very interesting point is that the decryption matrix in this case is the inverse of the encryption matrix. However, there is no need to invert the matrix, the encryption key matrix can simply be transposed (swapping the rows and columns) to get the decryption key matrix.

For example:

The plain text is :"Enemy attacks to night"

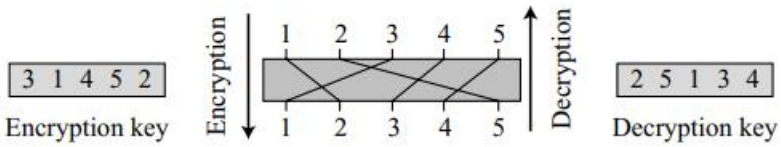


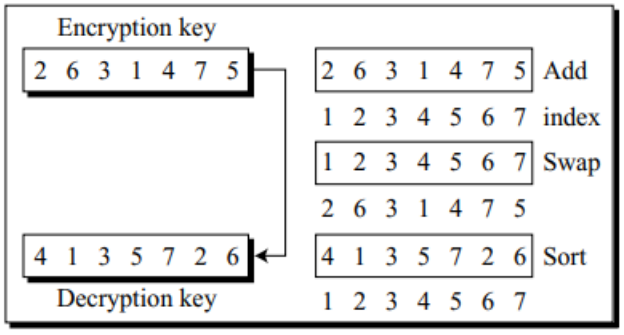
Cipher text is: EHTTMTEIAKNGAOYZCNTS

```
The Plain text is:
Enemy attacks tonight

  Enter permutation key separated by spaces: 3 1 4 5 2

The key list is:
[3, 1, 4, 5, 2]

The Encrypted text is:ETTHEAKIMAOTYCNXNTSG
```

```
The Plain text is:
AppleBananaCherryDateElderberryFigGrapeHoneydewKiwiLemonMangoNectarineOrange

  Enter permutation key separated by spaces: 3 1 4 5 2

The key list is:
[3, 1, 4, 5, 2]

The Encrypted text is:PNHDLEIPEKEAEIAXABARERYROEINOAOELAEADRGEYIMNCNNXENRTERGHDWOGTEGXPACYEBFANWLMNRRX
```

Decryption:



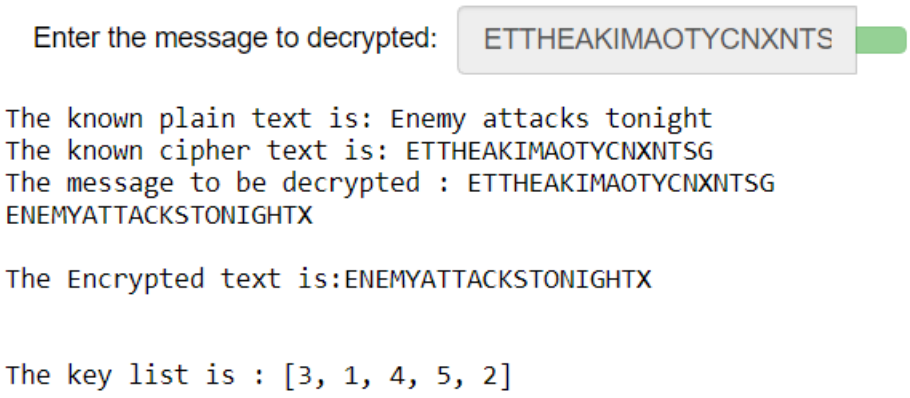


Here we can do the decryption by converting the key set into a matrix

```
The cipher text is:
ETTHEAKIMAOTYCNXNTSG

Enter permutation key separated by spaces: 3 1 4 5 2

The key list is:
[3, 1, 4, 5, 2]

The Decrypted text is:ENEMYATTACKSTONIGHTX
```

CryptAnalysis:

By known plain text attack we will get the key matrix,



Statistical Attack

A transposition cipher does not change the frequency of letters in the ciphertext; it only reorders the letters. So the first attack that can be applied is single-letter frequency analysis. This method can be useful if the length of the ciphertext is long enough. We have seen this attack before. However, transposition ciphers do not preserve the frequency of digrams and trigrams. This means that Eve cannot use these tools. In fact, if a cipher does not preserve the frequency of digrams and trigrams, but does preserve the frequency of single letters, it is probable that the cipher is a transposition cipher.

Brute-Force Attack

Eve can try all possible keys to decrypt the message. However, the number of keys can be huge (1! + 2! + 3! + . . . + L!), where L is the length of the ciphertext. A better approach is to guess the number of columns. Eve knows that the number of columns divides L. For example, if the length of the cipher is 20 characters, then 20 = 1 × 2 × 2 × 5

6.Vigenere Cipher:

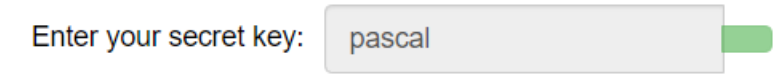
One interesting kind of polyalphabetic cipher was designed by Blaise de Vigenere, a sixteenth-century French mathematician. A Vigenere cipher uses a different strategy to create the key stream. The key stream is a repetition of an initial secret key stream of length m, where we have $1 \leq m \leq 26$. The cipher can be described as follows where.

One important difference between the Vigenere cipher and the other two polyalphabetic ciphers we have looked at, is that the Vigenere key stream does not depend on the plaintext characters; it depends only on the position of the character in the plaintext. In other words, the key stream can be created without knowing what the plaintext is.

Encryption:

Let us see how we can encrypt the message “She is listening” using the 6-character keyword “*PASCAL*”. The initial key stream is (15, 0, 18, 2, 0, 11). The key stream is the repetition of this initial key stream (as many times as needed).

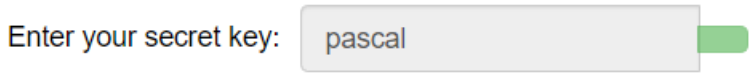
Plaintext:	s	h	e	i	s	l	i	s	t	e	n	i	n	g
P’s values:	18	07	04	08	18	11	08	18	19	04	13	08	13	06
Key stream:	***15***	***00***	***18***	***02***	***00***	***11***	***15***	***00***	***18***	***02***	***00***	***11***	***15***	***00***
C’s values:	**07**	**07**	**22**	**10**	**18**	**22**	**23**	**18**	**11**	**6**	**13**	**19**	**02**	**06**
Ciphertext:	**H**	**H**	**W**	**K**	**S**	**W**	**X**	**S**	**L**	**G**	**N**	**T**	**C**	**G**




```
The plain text is: She is listening
The secret key is: pascal
The cipher text is: HHWKSWXSLGNTCG
```

Decryption:

In decryption we have the key stream and the word to be decrypted




```
The cipher text is: HHWKSWXSLGNTCG
The secret key is: pascal
[15, 0, 18, 2, 0, 11, 15, 0, 18, 2, 0, 11, 15, 0]
[7, 7, 22, 10, 18, 22, 23, 18, 11, 6, 13, 19, 2, 6]
The decrypted text is: SHEISLISTENING
```

CryptAnalysis:

1. Several methods have been devised to find the length of the key. One method is discussed here. In the so-called Kasiski test, the cryptanalyst searches for repeated text segments, of at least three characters, in the ciphertext. Suppose that two of these segments are found and the distance between them is d. The cryptanalyst assumes that d|m where m is the key length. If more repeated segments can be found with distances d1, d2, …, dn, then gcd (d1, d2, …, dn)/m. This assumption is logical because if two characters are the same and are k × m (k = 1, 2, …) characters apart in the plaintext, they are the same and k × m characters apart in the ciphertext. Cryptanalyst uses segments of at least three characters to avoid the cases where the characters in the key are not distinct. Example 3.20 may help us to understand the reason.

2. After the length of the key has been found, the cryptanalyst uses the idea shown in Example 3.18. She divides the ciphertext into m different pieces and applies the method used to cryptanalyze the additive cipher, including frequency attack. Each ciphertext piece can be decrypted and put together to create the whole plaintext. In other words, the whole ciphertext does not preserve the single-letter frequency of the plaintext, but each piece does.


```
The cipher text is:
LIOMWGFEGGDVWGHHCQUCRHRWAGWIOWQLKGZETKKMEVLWPCZVGTHVTSGXQOVGCSVETQLTJSUMVWVEUVLXEWSLGFZMVVWLGYHCUSWXQHKVGSHEEVFLCFDGVSUMPHKIRZDMPHHBVWVWJWIXGFWLTSHGJOUEEHHVUCFVGO
GLW
the keys are:
2
14
3
4
The key word is:  CODE
```