CS-3002

Information Security

Submitted by: Ahmed Umar Rehman

Part A: Classical Cryptanalysis – Substitution Cipher

Task 1: Encrypt Your Data Using Caesar Cipher

1) **Plaintext:**

   Name: Ahmed

   Personal Information: "ahmed will be in India at midnight be careful now"

   Determine Key:

   Last 2 digits of Roll No = 80

   Key = 80 % 26 = 2

2) **Encrypt:**

   Shift each letter by 2 letters forward:

   a → c, t → v, t → v, a → c, c → e, k → m

   w → y, i → k, l → n, l → n

   b → d, e → g

   i → k, n → p

   I → K, n → p, d → f, i → k, a → c

   a → c, t → v

   m → o, i → k, d → f, n → p, i → k, g → i, h → j, t → v

   b → d, e → g

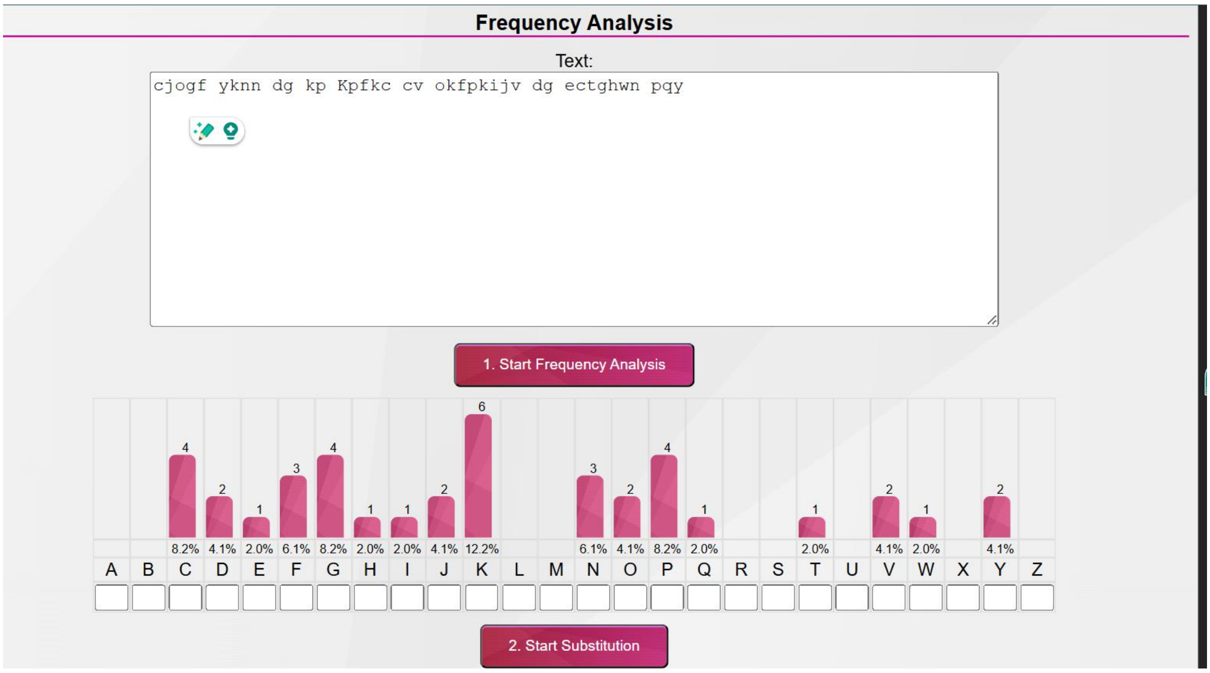
c → e, a → c, r → t, e → g, f → h, u → w, l → n

n → p, o → q, w → y

3) Ciphertext

cjogf yknn dg kp Kpfkc cv okfpkijv dg ectghwn pqy

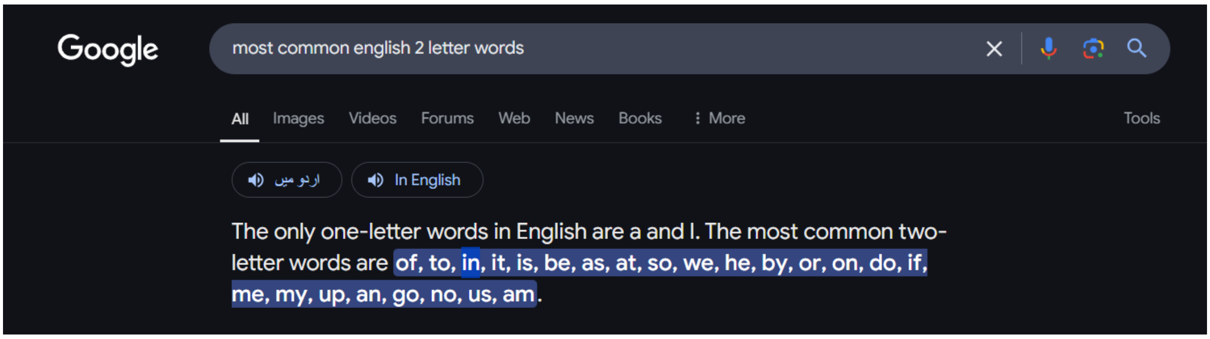
Task 2: Perform Frequency Analysis



```
cjogf yknn dg kp Kpfkc cv okfpkijv dg ectghwn pqy
```

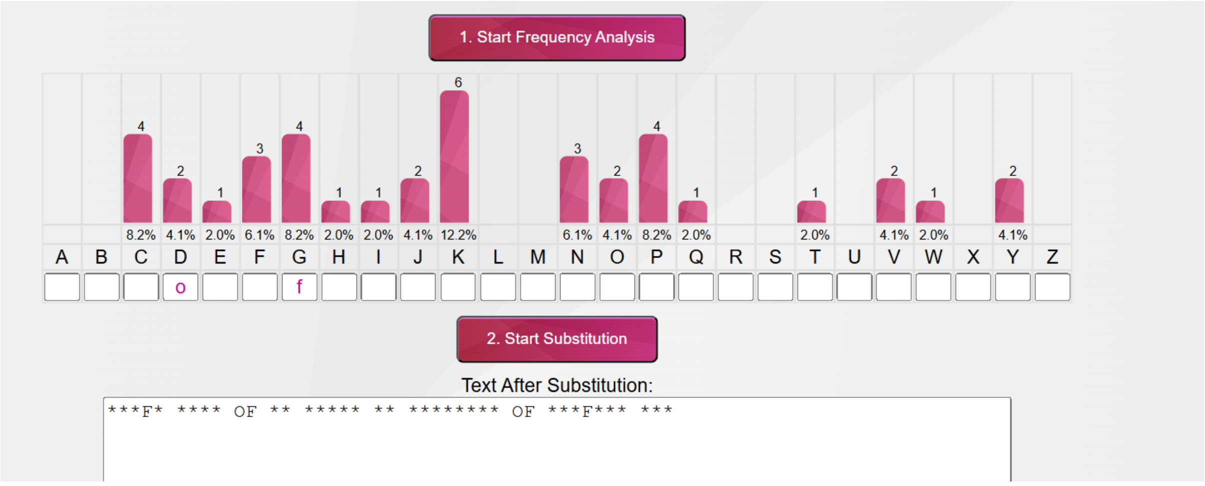
K is most used ciphertext

Task 3:



The only one-letter words in English are a and I. The most common two-letter words are of, to, in, it, is, be, as, at, so, we, he, by, or, on, do, if, me, my, up, an, go, no, us, am.

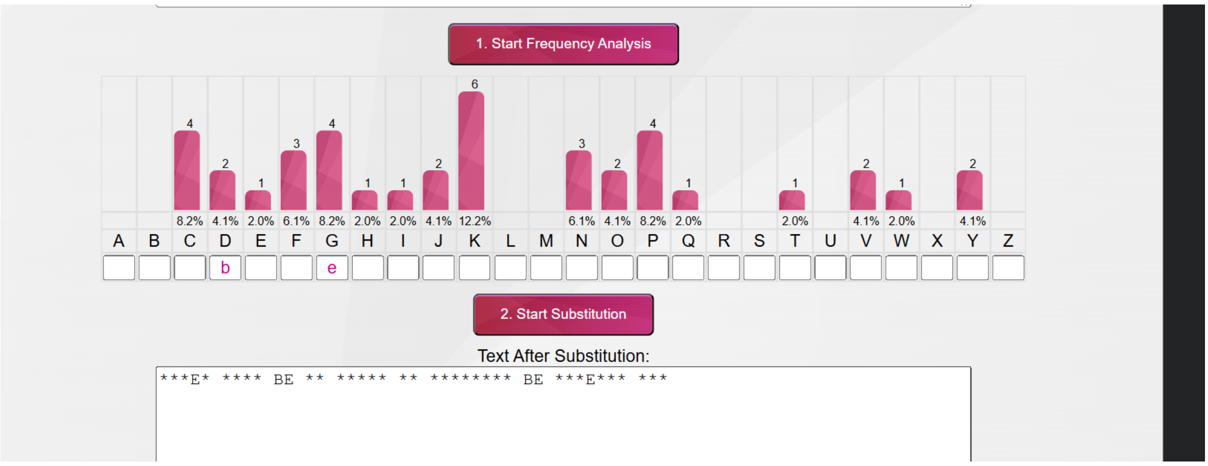
first we will look at **dg** ciphertext and compare with common English words



Text After Substitution:

```
***F* **** OF ** ***** ** ******** OF ***F*** ***
```

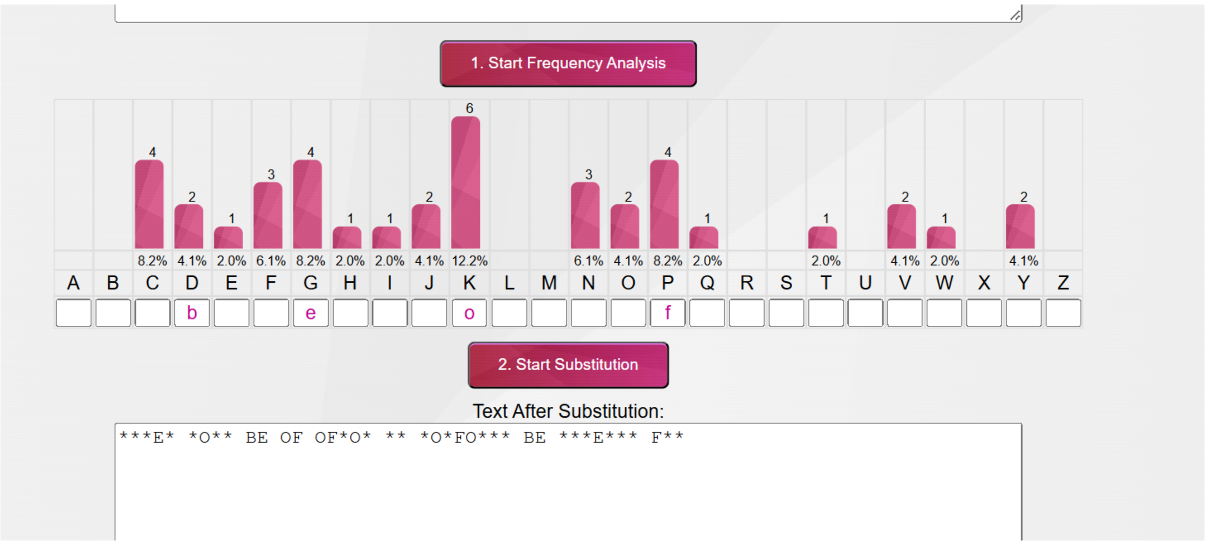
We are seeing that it is not mapping



Text After Substitution:

```
***E* **** BE ** ***** ** ******** BE ***E*** ***
```

The 2 letter word be is mapping and is recovering now. And then will we be looking **kp** ciphertext

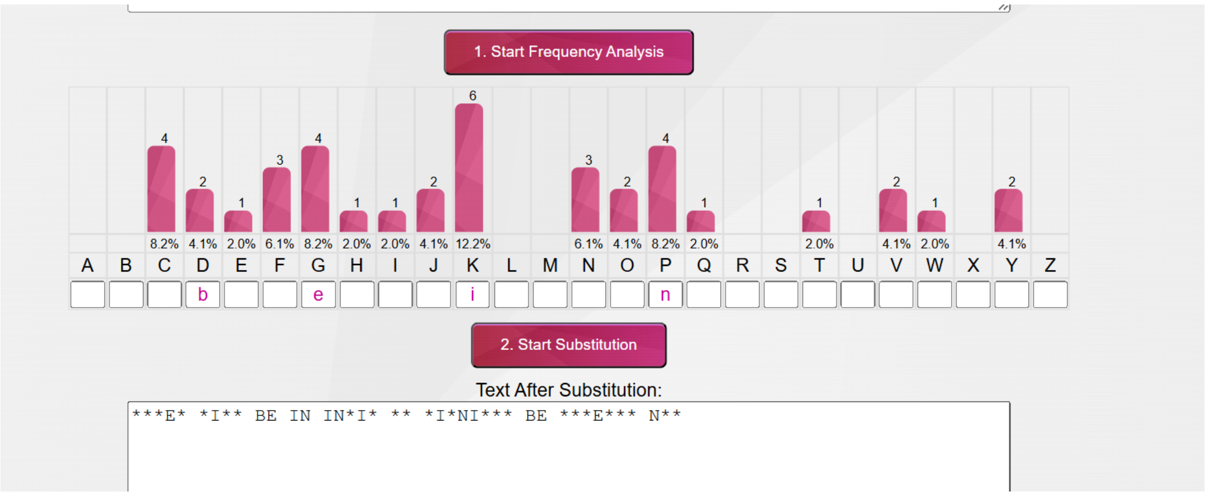


D	G	K	P
b	e	o	f

Text After Substitution:

```
***E* *O** BE OF OF*O* ** *O*FO*** BE ***E*** F**
```

of is not mapping with kp and text is not matching



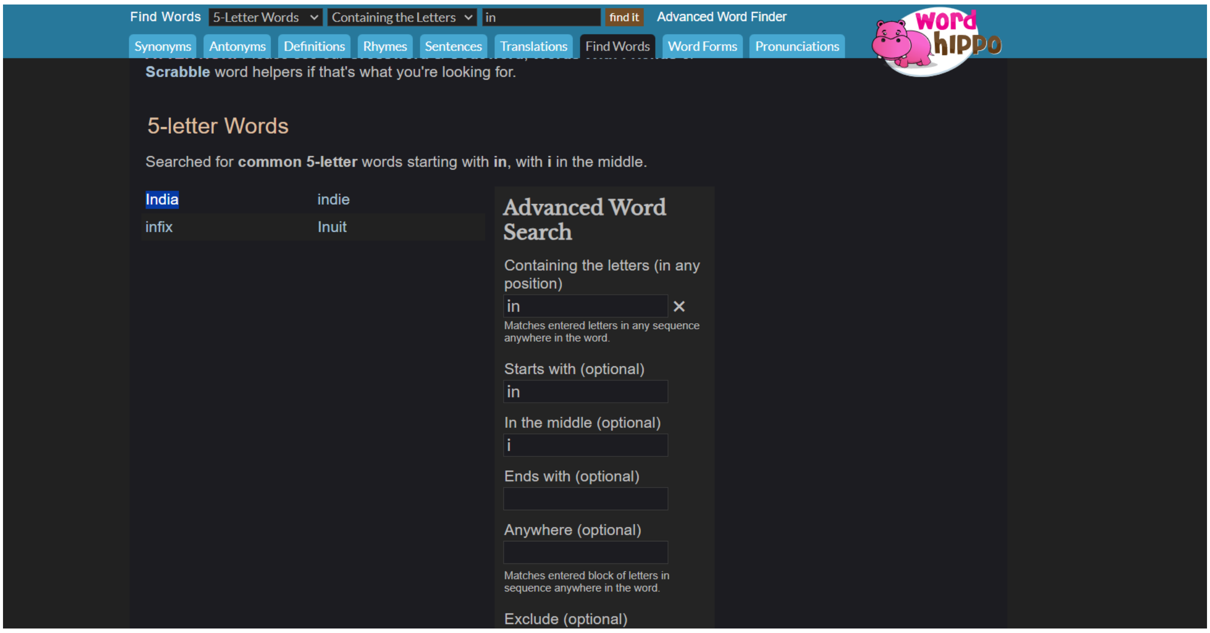
D	G	K	P
b	e	i	n

Text After Substitution:

```
***E* *I** BE IN IN*I* ** *I*NI*** BE ***E*** N**
```

Then **in** is matching with kp and is recovering now

Now we will go to word hippo website to search for the word IN*I*



Scrabble word helpers if that's what you're looking for.

5-letter Words

Searched for **common 5-letter** words starting with **in**, with **i** in the middle.

India	indie
infix	Inuit

Advanced Word Search

Containing the letters (in any position)
in
Matches entered letters in any sequence anywhere in the word.

Starts with (optional)
in

In the middle (optional)
i

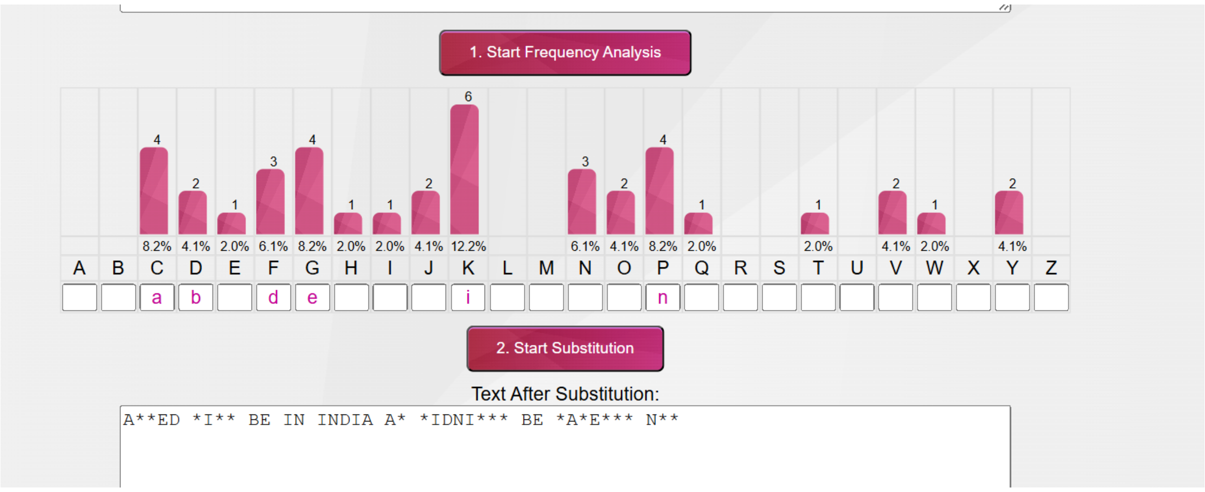
Ends with (optional)

Anywhere (optional)

Matches entered block of letters in sequence anywhere in the word.

Exclude (optional)

We have found the word INDIA

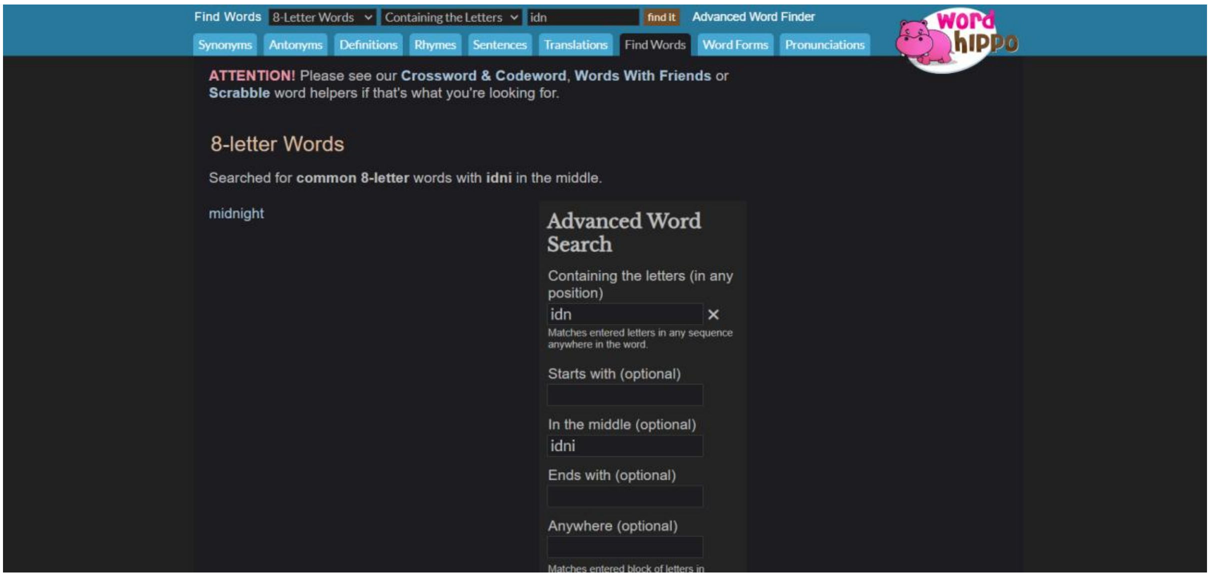


A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
		4	2	1	3	4	1	1	2	6			3	2	4	1			1		2	1		2	
		8.2%	4.1%	2.0%	6.1%	8.2%	2.0%	2.0%	4.1%	12.2%			6.1%	4.1%	8.2%	2.0%			2.0%		4.1%	2.0%		4.1%	
		a	b		d	e				i					n										

Text After Substitution:

```
A**ED *I** BE IN INDIA A* *IDNI*** BE *A*E*** N**
```

The text is now recovering now we will see the word *IDNI*** in word hippo website



ATTENTION! Please see our **Crossword & Codeword**, **Words With Friends** or **Scrabble** word helpers if that's what you're looking for.

8-letter Words

Searched for **common 8-letter** words with **idni** in the middle.

midnight

Advanced Word Search

Containing the letters (in any position)

idn

Matches entered letters in any sequence anywhere in the word.

Starts with (optional)

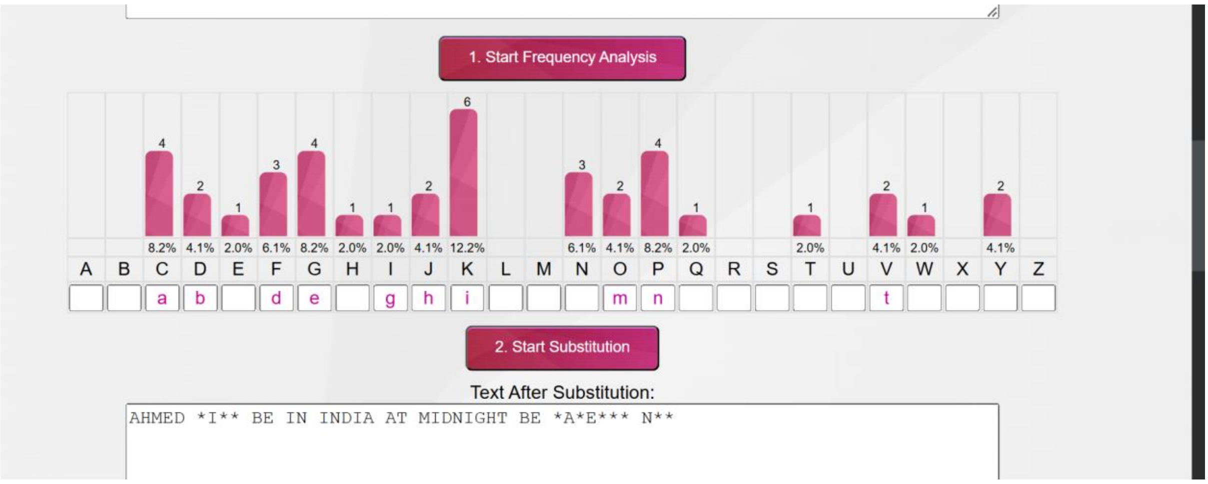
In the middle (optional)

idni

Ends with (optional)

Anywhere (optional)

Matches entered block of letters in

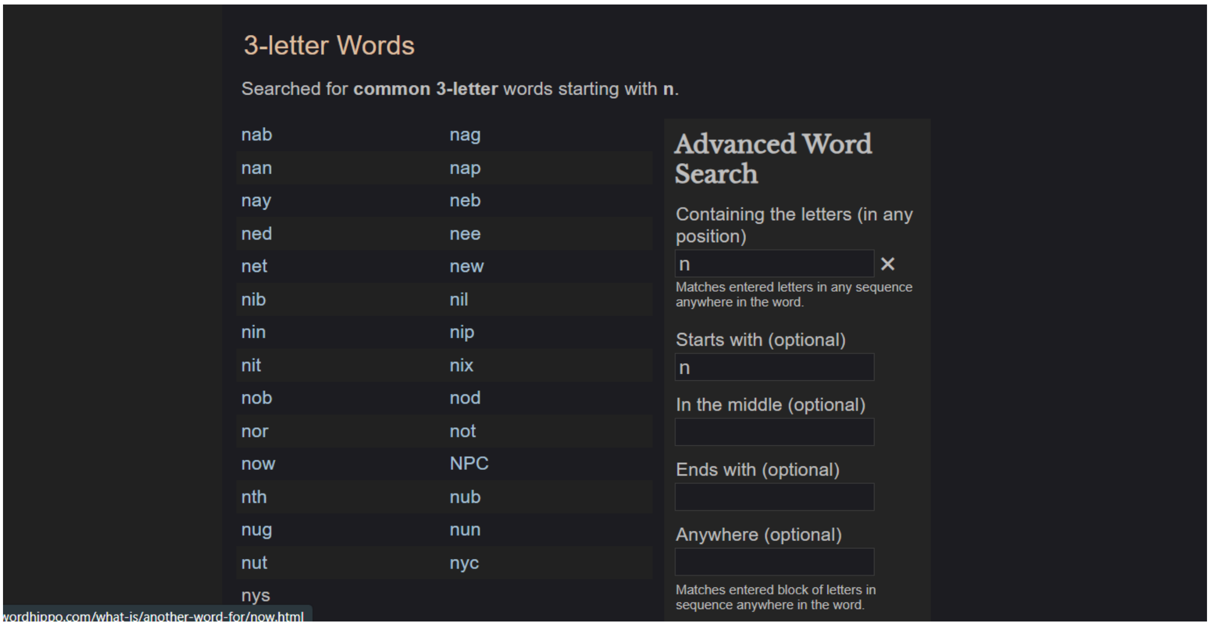


A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
		4	2	1	3	4	1	1	2	6			3	2	4	1			1		2	1		2	
		8.2%	4.1%	2.0%	6.1%	8.2%	2.0%	2.0%	4.1%	12.2%			6.1%	4.1%	8.2%	2.0%			2.0%		4.1%	2.0%		4.1%	
		a	b		d	e		g	h	i				m	n						t				

Text After Substitution:

```
AHMED *I** BE IN INDIA AT MIDNIGHT BE *A*E*** N**
```

We can see it is almost recovered now, we will look N** text



3-letter Words

Searched for **common 3-letter** words starting with **n**.

nab nag
nan nap
nay neb
ned nee
net new
nib nil
nin nip
nit nix
nob nod
nor not
now NPC
nth nub
nug nun
nut nyc
nys

Advanced Word Search

Containing the letters (in any position)

n ✕

Matches entered letters in any sequence anywhere in the word.

Starts with (optional)

n

In the middle (optional)

Ends with (optional)

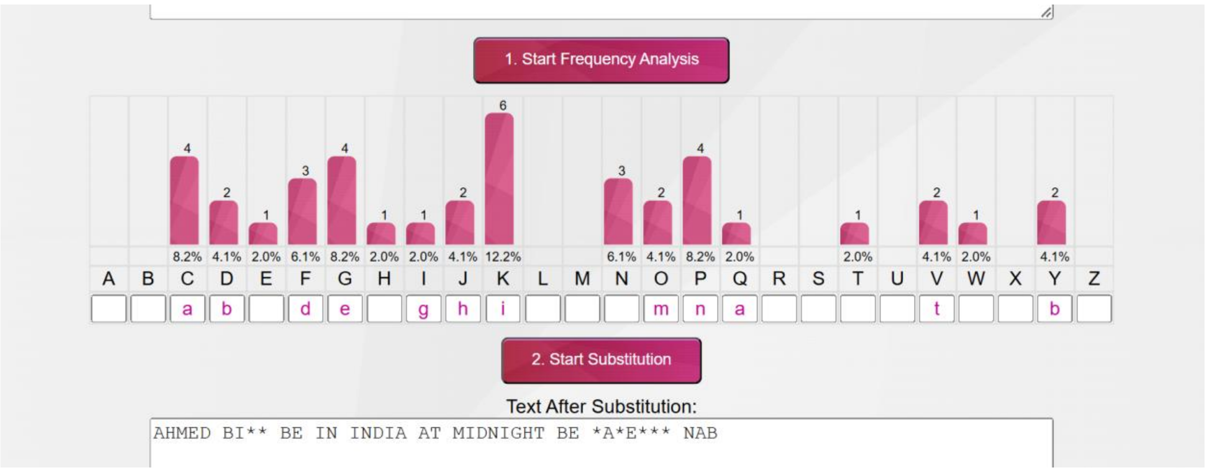
Anywhere (optional)

Matches entered block of letters in sequence anywhere in the word.

wordhippo.com/what-is/another-word-for/now.html

Since there are no other options, we will look word by word in this

We will try **ab** ciphertext first

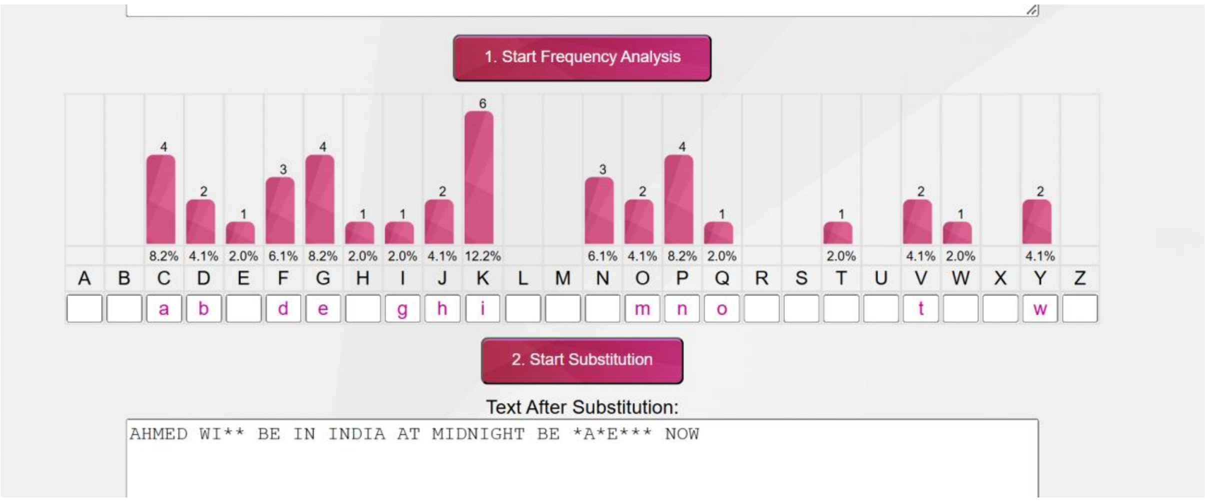


Text After Substitution:

```
AHMED BI** BE IN INDIA AT MIDNIGHT BE *A*E*** NAB
```

It is not making any sense

Now we will try **ow**

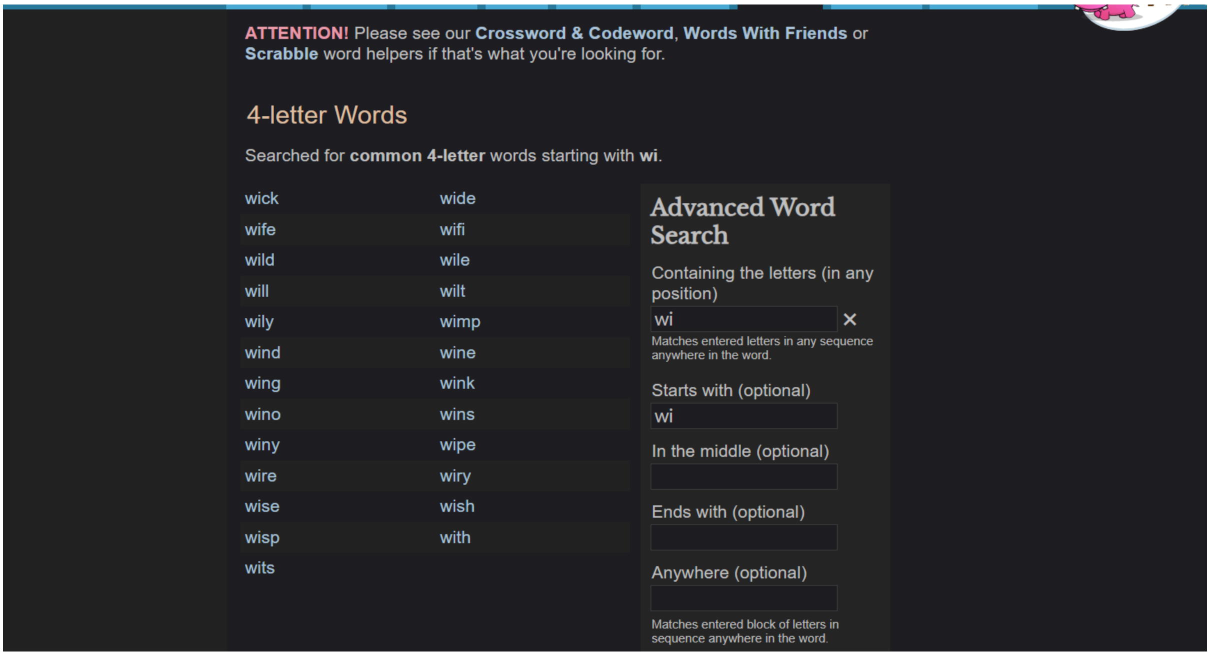


A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
		4	2	1	3	4	1	1	2	6			3	2	4	1			1		2	1		2	
		8.2%	4.1%	2.0%	6.1%	8.2%	2.0%	2.0%	4.1%	12.2%			6.1%	4.1%	8.2%	2.0%			2.0%		4.1%	2.0%		4.1%	
		a	b		d	e		g	h	i				m	n	o					t			w	

Text After Substitution:

```
AHMED WI** BE IN INDIA AT MIDNIGHT BE *A*E*** NOW
```

The NOW word has been recovered now to WI** word



ATTENTION! Please see our **Crossword & Codeword**, **Words With Friends** or **Scrabble** word helpers if that's what you're looking for.

4-letter Words

Searched for **common 4-letter** words starting with **wi**.

wick wide
wife wifi
wild wile
will wilt
wily wimp
wind wine
wing wink
wino wins
winy wipe
wire wiry
wise wish
wisp with
wits

Advanced Word Search

Containing the letters (in any position): wi

Matches entered letters in any sequence anywhere in the word.

Starts with (optional): wi

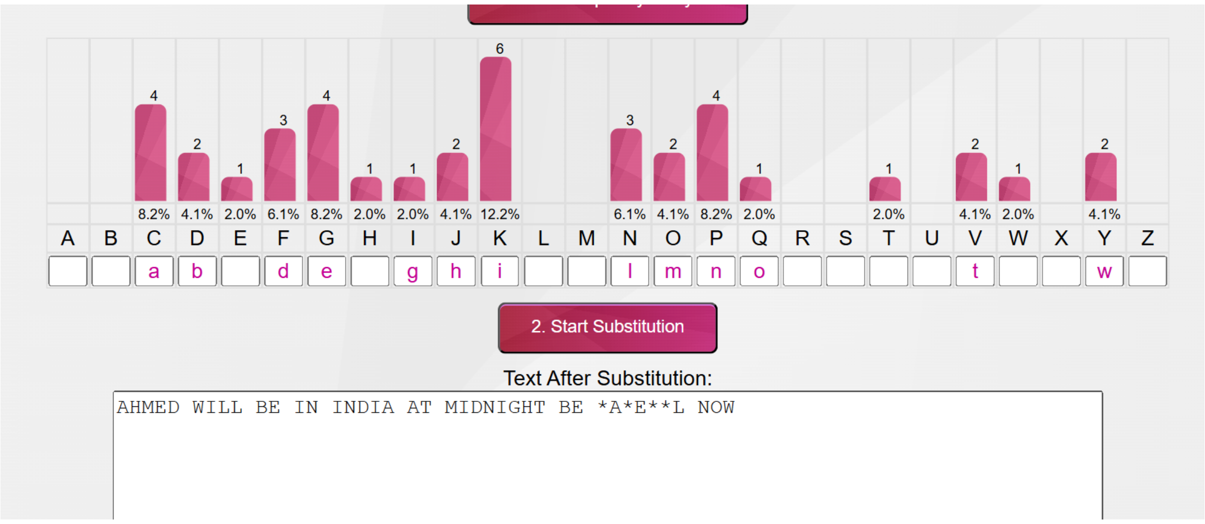
In the middle (optional):

Ends with (optional):

Anywhere (optional):

Matches entered block of letters in sequence anywhere in the word.

Since we have no other option, we will check one by one

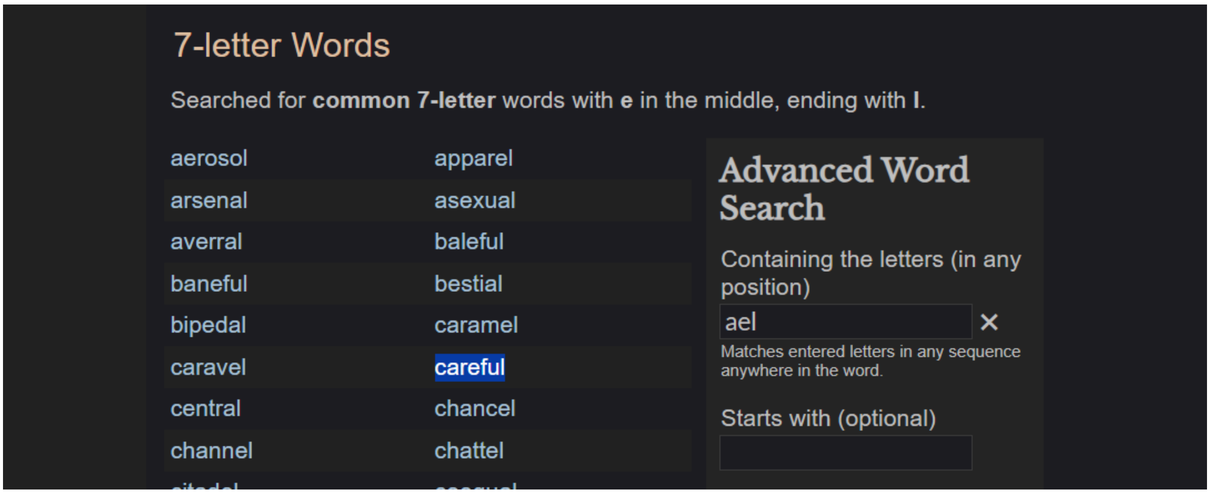


A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
		4	2	1	3	4	1	1	2	6			3	2	4	1			1		2	1		2	
		8.2%	4.1%	2.0%	6.1%	8.2%	2.0%	2.0%	4.1%	12.2%			6.1%	4.1%	8.2%	2.0%			2.0%		4.1%	2.0%		4.1%	
		a	b		d	e		g	h	i			l	m	n	o					t			w	

Text After Substitution:

```
AHMED WILL BE IN INDIA AT MIDNIGHT BE *A*E**L NOW
```

The l word has been mapped successfully since the ciphertext of WILL is YKNN so the one-gram word has been required.



7-letter Words

Searched for **common 7-letter** words with **e** in the middle, ending with **l**.

aerosol apparel
arsenal asexual
averral baleful
baneful bestial
bipedal caramel
caravel careful
central chancel
channel chattel

Advanced Word Search

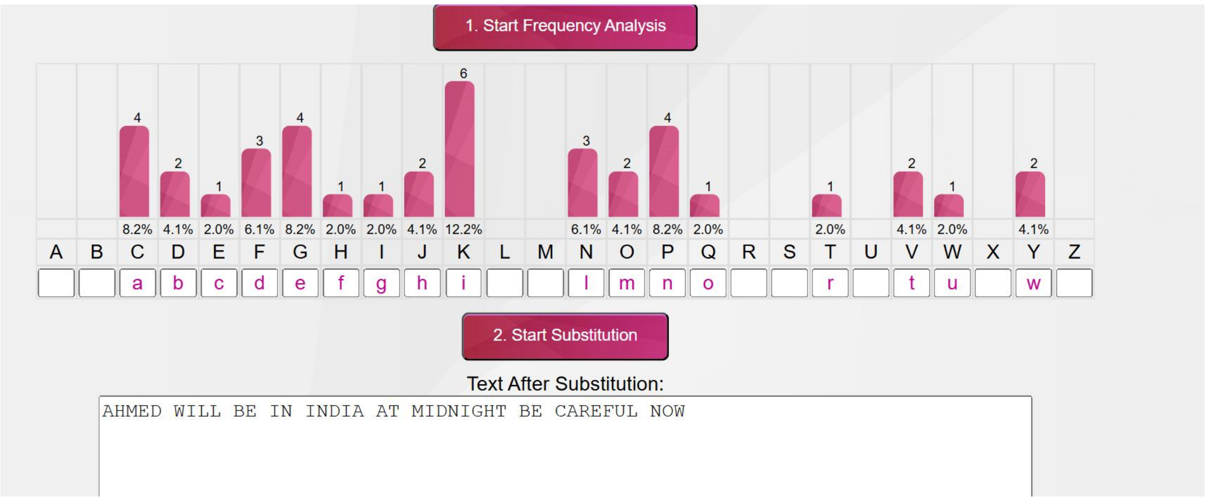
Containing the letters (in any position)

ael

Matches entered letters in any sequence anywhere in the word.

Starts with (optional)

It has been suitable for this ciphertext *A*E**L



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
		4	2	1	3	4	1	1	2	6			3	2	4	1			1		2	1		2	
		8.2%	4.1%	2.0%	6.1%	8.2%	2.0%	2.0%	4.1%	12.2%			6.1%	4.1%	8.2%	2.0%			2.0%		4.1%	2.0%		4.1%	
		a	b	c	d	e	f	g	h	i			l	m	n	o			r		t	u		w	

Text After Substitution:

```
AHMED WILL BE IN INDIA AT MIDNIGHT BE CAREFUL NOW
```

The data has been successfully recovered.

These are the main assumptions during recovering the plaintext,

- **The attacker has access to encrypted messages** – It is assumed that an attacker can obtain ciphertext but does not know the encryption key.
- **Language patterns remain unchanged** – The analysis assumes that the encrypted text follows common letter frequency patterns of English (or another known language).
- **The encryption method is known** – The attacker is aware that a substitution cipher (like Caesar Cipher) is being used, even if the exact shift is unknown.

Substitution ciphers can be broken because some letters appear more often than others in a language. For example, in English, letters like ‘E’ and ‘T’ are used a lot. If a hacker sees a letter appearing many times in a secret message, they can guess what it stands for. Also, common words like “the” and “and” keep their shape even after encryption, making it easier to figure out the key.

The Caesar Cipher is weak for several reasons:

1. **Easy to Guess** – Since there are only 25 possible shifts, a hacker can try all of them quickly.
2. **Pattern Stays the Same** – The same letter always turns into the same new letter, making it predictable.
3. **Frequency Analysis Works** – A hacker can count which letters appear most often and compare them to common letter frequencies in English.
4. **Common Words Are Easy to Spot** – Words like “attack” or “hello” still look similar after encryption, making them easier to recognize.

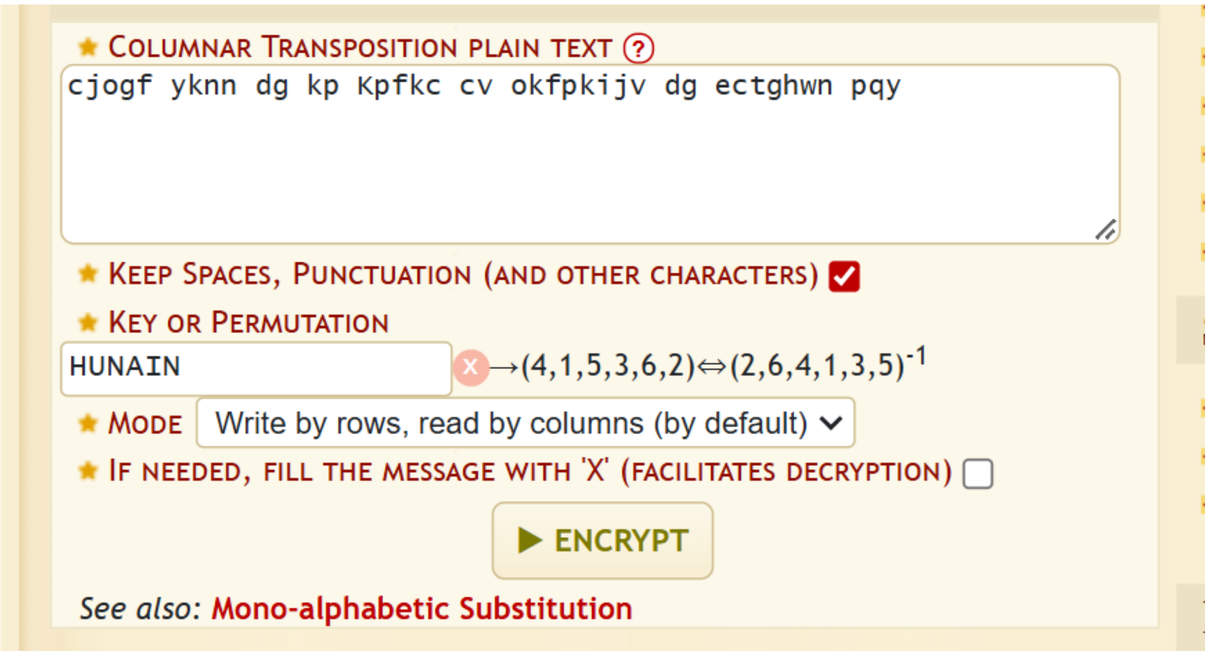
Part B: Advanced Cryptanalysis – Product Cipher (Substitution + Transposition)

Task 4: Transposition Cipher (Columnar Transposition)

1. Take the ciphertext from Part A.

cjogf yknn dg kp Kpfkc cv okfpkijv dg ectghwn pqy

2. Encrypt it again using a Columnar Transposition Cipher with a secret key of length 6.



★ COLUMNAR TRANSPOSITION PLAIN TEXT ?

```
cjogf yknn dg kp Kpfkc cv okfpkijv dg ectghwn pqy
```

★ KEEP SPACES, PUNCTUATION (AND OTHER CHARACTERS) ☑

★ KEY OR PERMUTATION

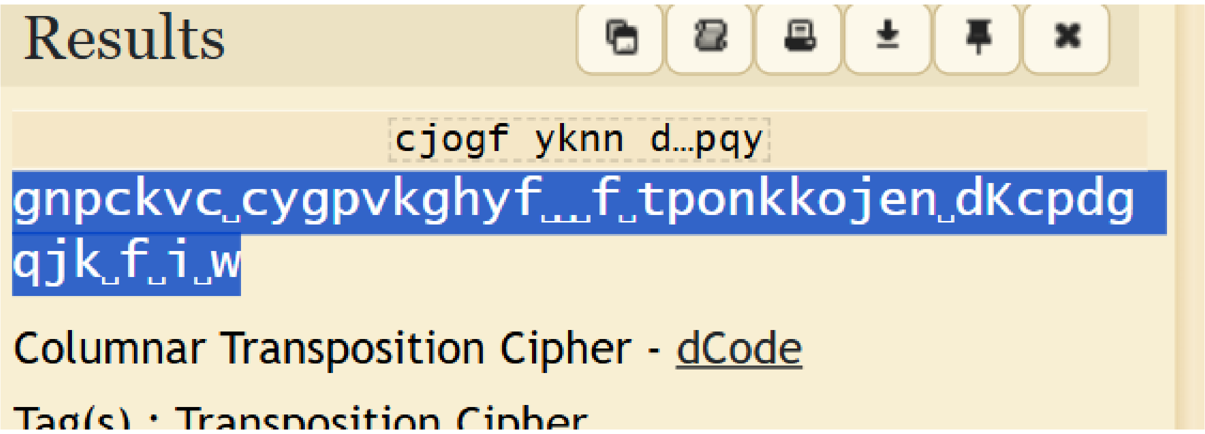
HUNAIN ⓧ→(4,1,5,3,6,2)⇔(2,6,4,1,3,5)$^{-1}$

★ MODE Write by rows, read by columns (by default)

★ IF NEEDED, FILL THE MESSAGE WITH 'X' (FACILITATES DECRYPTION) ☐

See also: Mono-alphabetic Substitution

3. Present the new ciphertext.



Results

cjogf yknn d…pqy

gnpckvc␣cygpvkghyf␣␣␣f␣tponkkojen␣dKcpdg qjk␣f␣i␣w

Columnar Transposition Cipher - dCode

Tag(s) : Transposition Cipher

Here's the summary with the necessary calculations for Task 5:

1. **Attempt to break the transposition cipher:**
   Ciphertext:

gnpckvc cygpvkghyf   f tponkkojen dKcpdgqjk f i w

Key Length = 6, organize ciphertext into rows of 6 characters:

gnpckv

c ygpv

kghyf

f tpo

nkkoj

en dKc

pdgqj

k f i w

2. **Frequency analysis:**
   Letter frequencies are compared with typical English frequencies (E, T, A). No exact calculations needed, but common letters helped guide the decryption.

3. **Plaintext cipher attack:**
   Using common letter patterns like "the", "and", and "attack", columns are rearranged based on educated guesses.

4. **Recovered plaintext:**
   Rearranged grid gives:
   "ahmed will be in India at midnight be careful now"

Modern cryptography is much stronger than old ciphers like Caesar Cipher. Here's why:

1. **Much Harder to Break** – Modern encryption uses complex math, making it almost impossible to crack.

2. **Larger Key Space** – Instead of just 25 shifts, modern encryption uses long keys (128-bit, 256-bit), making brute-force attacks useless.

3. **No Simple Patterns** – Modern encryption scrambles data in a way that doesn't follow clear letter patterns.

4. **Secure Online Communication –** We use strong encryption (like TLS and end-to-end encryption) to keep messages, bank details, and passwords safe from hackers.

Old ciphers are fun to learn but not safe for real-world use. Modern cryptography protects our data much better.