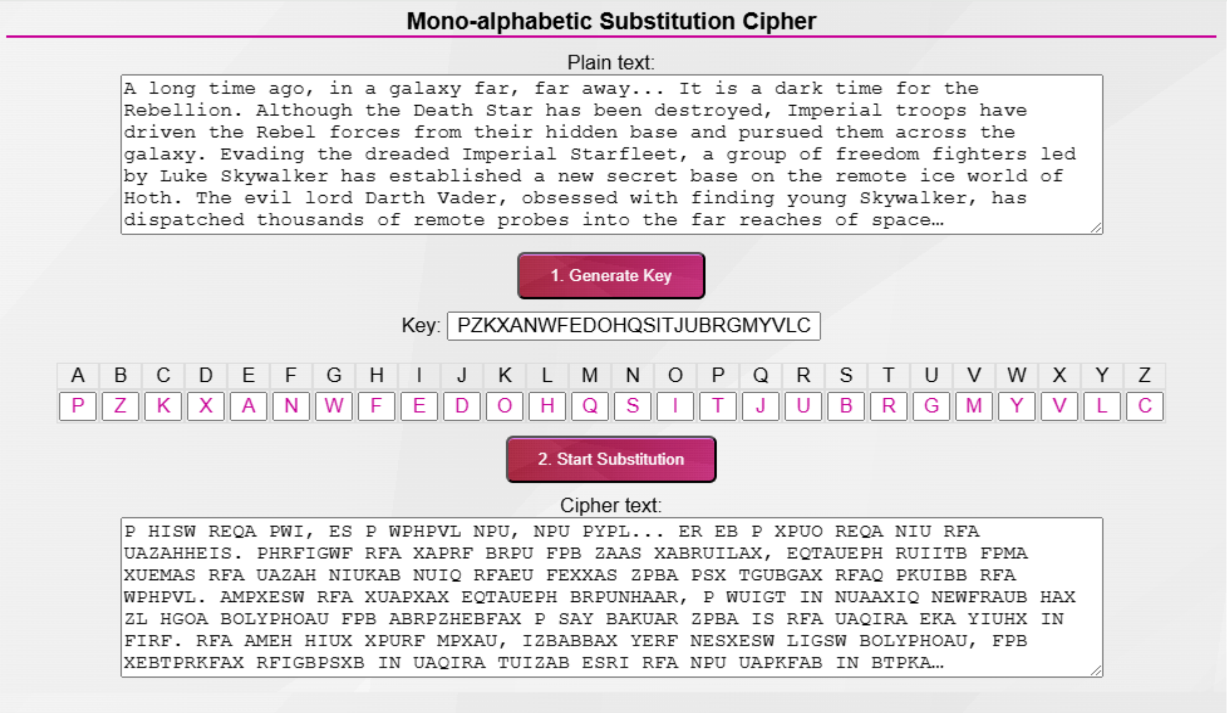
2. Monoalphabetic Cipher

A **mono-alphabetic cipher** (aka **simple substitution cipher**) is a substitution cipher where each letter of the plain text is replaced with another letter of the alphabet. It uses a **fixed key** which consist of the 26 letters of a “shuffled alphabet”.



Mono-alphabetic Substitution Cipher

Plain text:

```
A long time ago, in a galaxy far, far away... It is a dark time for the
Rebellion. Although the Death Star has been destroyed, Imperial troops have
driven the Rebel forces from their hidden base and pursued them across the
galaxy. Evading the dreaded Imperial Starfleet, a group of freedom fighters led
by Luke Skywalker has established a new secret base on the remote ice world of
Hoth. The evil lord Darth Vader, obsessed with finding young Skywalker, has
dispatched thousands of remote probes into the far reaches of space…
```

Key: PZKXANWFEDOHQSITJUBRGMYVLC

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

Cipher text:

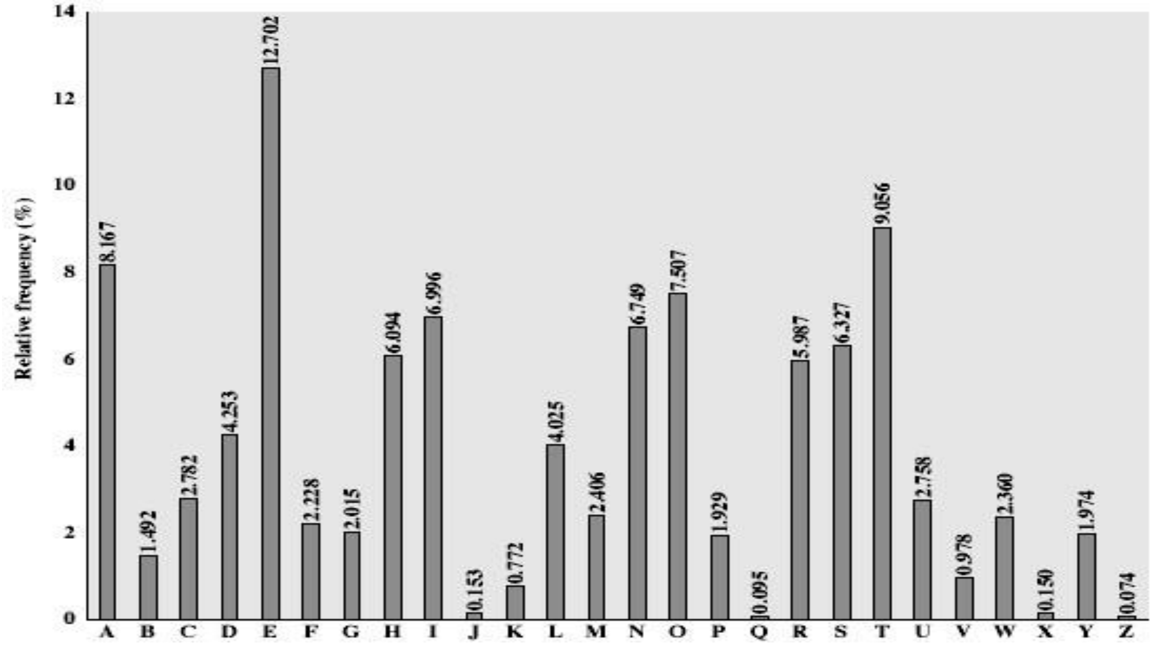
```
P HISW REQA PWI, ES P WPHPVL NPU, NPU PYPL... ER EB P XPUO REQA NIU RFA
UAZAHHEIS. PHRFIGWF RFA XAPRF BRPU FPB ZAAS XABRUILAX, EQTAUEPH RUIITB FPMA
XUEMAS RFA UAZAH NIUKAB NUIQ RFAEU FEXXAS ZPBA PSX TGUBGAX RFAQ PKUIBB RFA
WPHPVL. AMPXESW RFA XUAPXAX EQTAUEPH BRPUNHAAR, P WUIGT IN NUAAXIQ NEWFRAUB HAX
ZL HGOA BOLYPHOAU FPB ABRPZHEBFAX P SAY BAKUAR ZPBA IS RFA UAQIRA EKA YIUHX IN
FIRF. RFA AMEH HIUX XPURF MPXAU, IZBABBAX YERF NESXESW LIGSW BOLYPHOAU, FPB
XEBTPRKFAX RFIGBPSXB IN UAQIRA TUIZAB ESRI RFA NPU UAPKFAB IN BTPKA…
```

With the above key, all “A” letters in the plain text will be encoded to an “P”.

This type of cipher is a form of **symmetric encryption** as the same key can be used to both **encrypt** and **decrypt** a message.
Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet.
Prone to guessing attack using the English letters frequency of occurrence of letters.
The English Language is used so the nature of plain text is known.

Frequency Analysis

One approach used to help decrypt a mono-alphabetic substitution cipher is to use a frequency analysis based on counting the number of occurrence of each letter to help identify the most recurrent letters. (e.g. In the English language, letters E, T and A).



Frequency counts for English alphabet

- guess **A** & **R** are e and t
- guess **RFA** is the and hence **ZWP** is the • proceeding with trial and error finally get the plaintext

- 3. **Playfair Cipher:**

The **Playfair cipher** was the first practical digraph substitution cipher. The scheme was invented in **1854** by **Charles Wheatstone** but was named after Lord Playfair who promoted the use of the cipher. In Playfair cipher unlike traditional cipher we encrypt a pair of alphabets(digraphs) instead of a single alphabet.

Encryption Technique

For the encryption process let us consider the following example:

Key: monarchy
Plaintext: instruments

The Playfair Cipher Encryption Algorithm:
The Algorithm consists of 2 steps:

1. **Generate the key Square(5×5):**

   - The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I.

   - The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.

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

2. **Algorithm to encrypt the plain text:** The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.
   For example:

```
PlainText: "instruments"
After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz'
```

1. Pair cannot be made with same letter. Break the letter in single and add a bogus letter to the previous letter.

Plain Text: “hello”

After Split: ‘he’ ‘lx’ ‘lo’

Here **‘x’** is the bogus letter.

2. If the letter is standing alone in the process of pairing, then add an extra bogus letter with the alone letter

Plain Text: “helloe”

AfterSplit: ‘he’ ‘lx’ ‘lo’ ‘ez’

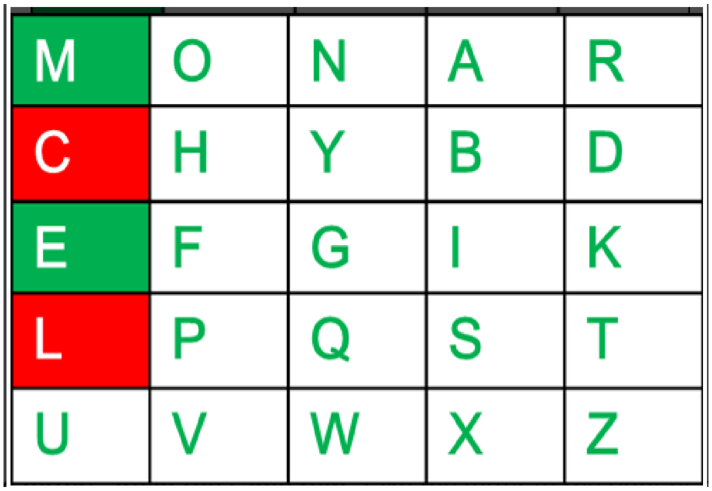
Here **‘z’** is the bogus letter.

Rules for Encryption:

- **If both the letters are in the same column**: Take the letter below each one (going back to the top if at the bottom).

  For example:

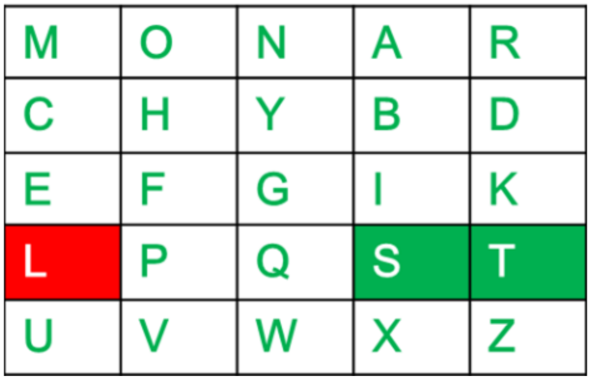
```
Diagraph: "me"
Encrypted Text: cl
Encryption:
  m -> c
  e -> l
```



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

- **If both the letters are in the same row**: Take the letter to the right of each one (going back to the leftmost if at the rightmost position). **For example:**

```
Diagraph: "st"
Encrypted Text: tl
Encryption:
  s -> t
  t -> l
```

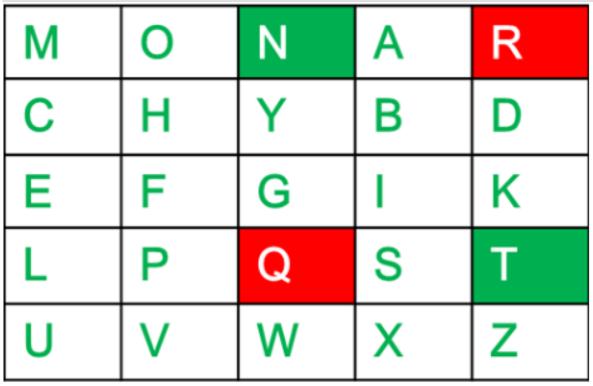


M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

- **If neither of the above rules is true**: Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

For example:

```
Diagraph: "nt"
Encrypted Text: rq
Encryption:
  n -> r
  t -> q
```

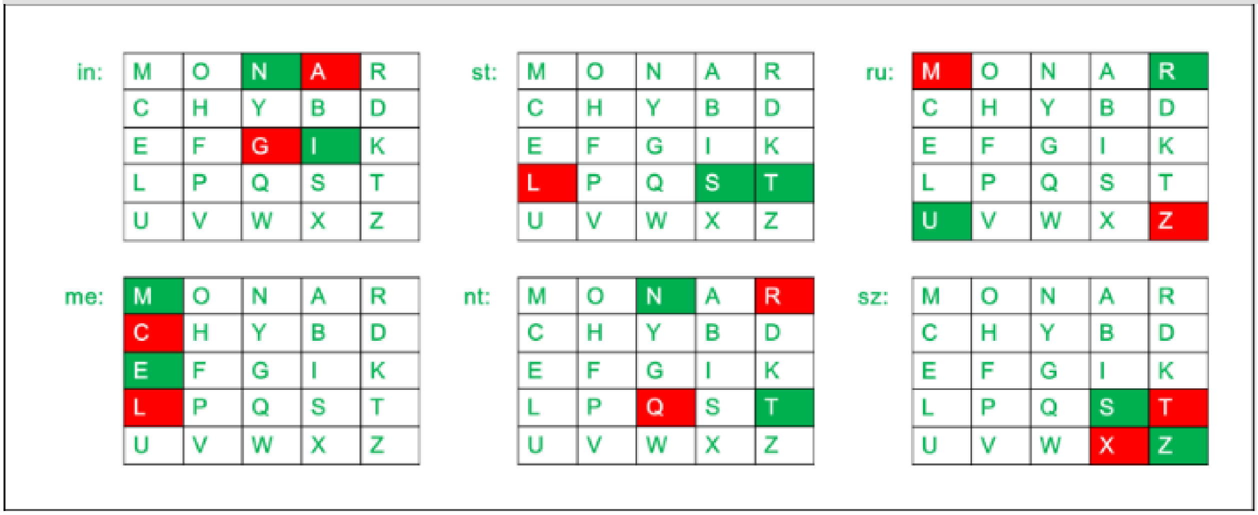


M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

For example:

```
Plain Text: "instrumentsz"
Encrypted Text: gatlmzclrqtx
Encryption:

  i -> g
  n -> a
  s -> t
  t -> l
  r -> m
  u -> z
  m -> c
  e -> l
  n -> r
  t -> q
  s -> t
  z -> x
```



in:

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

st:

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

ru:

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

me:

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

nt:

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

sz:

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

Decryption Technique

Decrypting the Playfair cipher is as simple as doing the same process in reverse. The receiver has the same key and can create the same key table, and then decrypt any messages made using that key.

Key: monarchy

ciphertext: gatlmzclrqtx

The Playfair Cipher Decryption Algorithm:

The Algorithm consists of 2 steps:

1. **Generate the key Square (5×5) at the receiver's end:**

   - The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I.

   - The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.

2. **Algorithm to decrypt the ciphertext:** The ciphertext is split into pairs of two letters (digraphs).

Note: *The* ***ciphertext*** *always have* ***even*** *number of characters.*

- **For example:**

```
CipherText: "gatlmzclrqtx"
After Split: 'ga' 'tl' 'mz' 'cl' 'rq' 'tx'
```

- **Rules for Decryption:**
  - **If both the letters are in the same column**: Take the letter above each one (going back to the bottom if at the top).
    For example:

```
Diagraph: "cl"
Decrypted Text: me
Decryption:
  c -> m
  l -> e
```

- **If both the letters are in the same row**: Take the letter to the left of each one (going back to the rightmost if at the leftmost position). **For example:**

```
Diagraph: "tl"
Decrypted Text: st
Decryption:
  t -> s
  l -> t
```

- **If neither of the above rules is true**: Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

For example:

```
Diagraph: "rq"
Decrypted Text: nt
Decryption:
  r -> n
  q -> t
```

For example:

```
Plain Text: "gatlmzclrqtx"
Decrypted Text: instrumentsz
Decryption:
(red)-> (green)
  ga -> in
  tl -> st
  mz -> ru
  cl -> me
  rq -> nt
  tx -> sz
```

in:

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

st:

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

ru:

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

me:

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

nt:

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

sz:

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