... ciphers

Permutation

Rail Fence (variants)

```
v i t          v   a
a a r            a   i   n
r n            v   i   r   t
```

Key: 3
Plaintext: variant
Ciphertext: VITAARN / VAAINRT

Permutations (variants)

```
123 123 123 123
per mut ati onx
erp utm tia nxo
231 231 231 231
```

Key: (2,3,1)
Plaintext: permutation
Ciphertext: ERPUTMTIANXO

```
123      213
per      erp
mut      utm
ati      tia
onx      nxo
```

Key: (2,3,1)
Plaintext: permutation
Ciphertext: EUTNRTIXPMAO

Substitution

Monoalphabetic

Caesar Cipher (Shift Cipher)

```
a b c d e f g h i j k l m
C D E F G H I J K L M N O
n o p q r s t u v w x y z
P Q R S T U V W X Y Z A B
```

Plaintext: hello
Ciphertext: JGNNQ

No. of keys: 26 ➡ Brute force
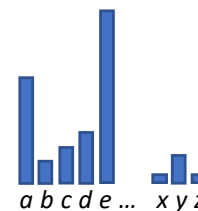
Simple Substitution

```
a b c d e f g h i j k l m
G M I P R S E N B X Z T A
n o p q r s t u v w x y z
L C V J F Y U D K H W O Q
```

Plaintext: hello
Ciphertext: NRTTC

No. of keys: 26! 🕐

Frequency analysis


```
a b c d e ... x y z
```

Polyalphabetic

PlayFair   (I=J)

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

Key: CIPHER
Plaintext: This is a B
Ciphertext: YDPQPQBD

Vigenère cipher

- Vigenère square
  26 Caesar alphabets

```
a b c d e f g h i ...
b c f e f g h i j ...
c d e f g h i j k ...
... ... ... ... ... ...
r s t u v w x y z ...
... ... ... ... ... ...
z a b c d e f g h ...
```

Key: CAR
Plaintext: Secret message
Ciphertext: UEI TEK OEJUAXG