HackerFrogs Afterschool
Classical Ciphers (Part 2)

Class:
Cryptography

Workshop Number:
AS-CRY-03

Document Version:
1.75

Special Requirements:
Registered account at
picoctf.org

Welcome to HackerFrogs Afterschool!

Hey there HackerFrogs! This workshop is the third session for cryptography basics

In the last session we learned about the following cryptography concepts

Cryptography Terms

`Cipher` – A cryptographic algorithm used in encryption and decryption

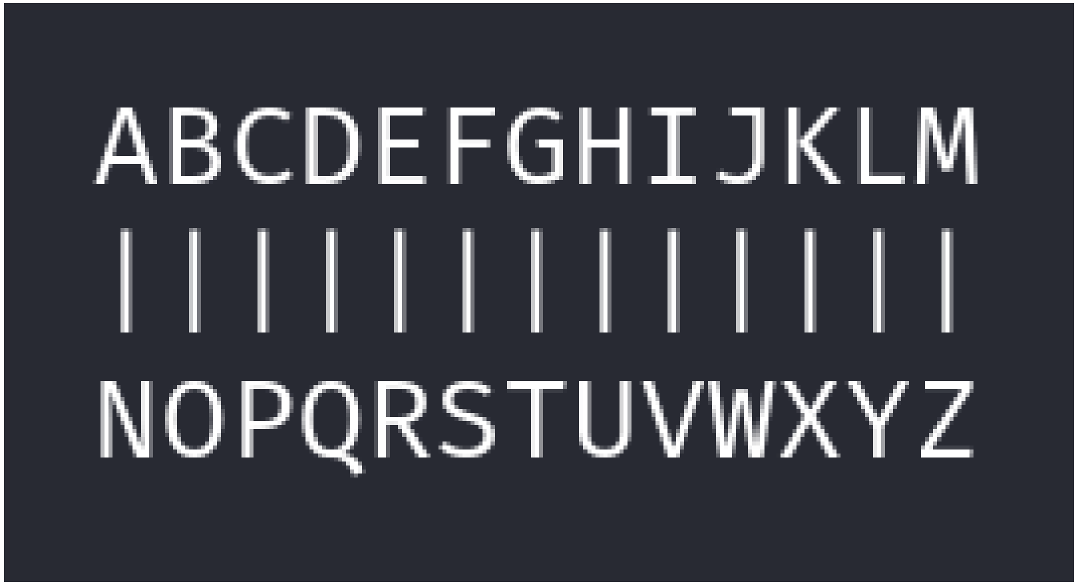
`Plaintext` – A message or piece of text that is not encrypted

`Ciphertext` – An encrypted message or piece of text

`Encryption` – The act of transforming plaintext into ciphertext

`Decryption` – The act of transforming ciphertext into plaintext

ROT13 Cipher

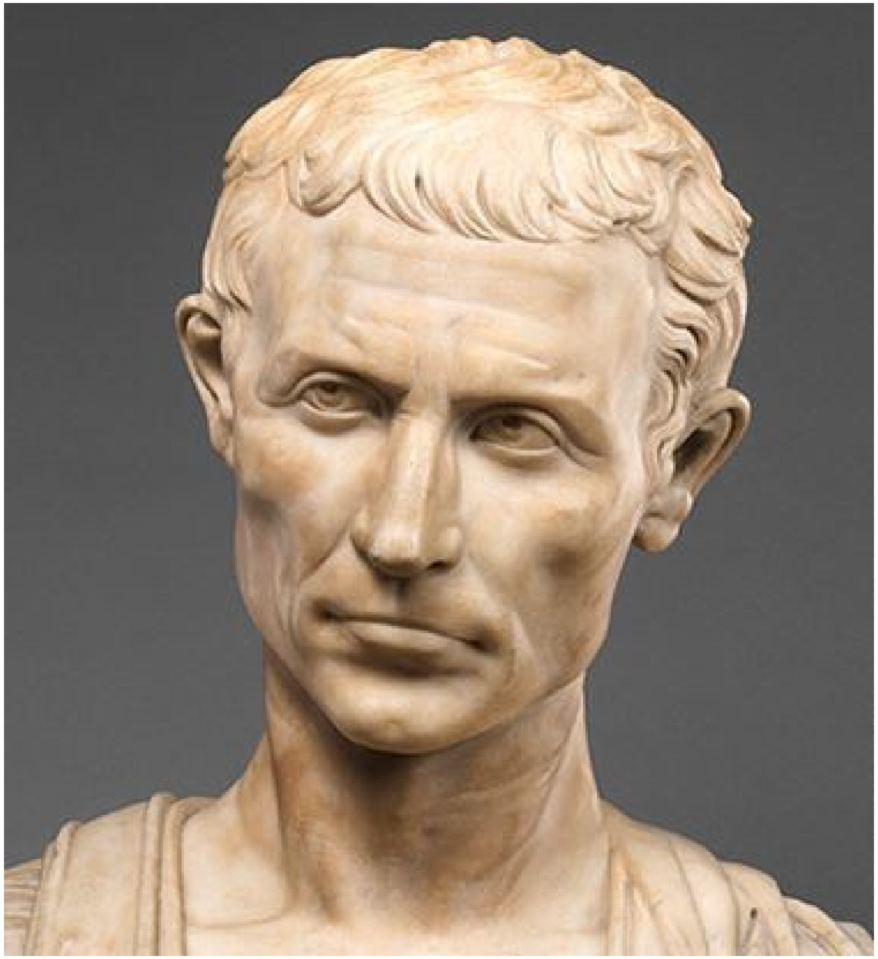


```
ABCDEFGHIJKLM
|||||||||||||
NOPQRSTUVWXYZ
```

The ROT13 cipher is a simple substitution cipher where the encryption method is shift each plaintext letter 13 positions in the alphabet to form the ciphertext

The Caesar Cipher

The Caesar Cipher is a substitution cipher where the method of encryption is to shift each letter of the plaintext by a specific number of letters in the alphabet, called the shift or key



This Session's Topics

- Vigenere Cipher

- Rail-Fence Cipher

- Transposition Cipher

The Vigenere Cipher

The Vigenere Cipher is another type of symmetrical substitution cipher. While the typical Caesar Cipher uses an **rotation number** which substitutes plaintext letters for ciphertext letters--

The Vigenere Cipher

the Vigenere Cipher uses a **key** which is mapped to the plaintext characters before encryption can take place.

The Vigenere Cipher

In cryptographic terms, a key is a string of numbers or letters which is used in a cipher's encryption and decryption process.

The Vigenere Cipher

In the case of the Vigenere Cipher, the key is a alphabetic string of varying length, with each plaintext letter mapped to a letter in the key.

The Vigenere Cipher

The first letter of plaintext is mapped to the first letter of the key, the second letter of plaintext is mapped to the second letter of the key,
and so on..

The Vigenere Cipher

For example, given the plaintext `CROCODILE` and the key `ANIMAL`, the two would be mapped in the following way:

```
CROCODILE
ANIMALANI
```

The Vigenere Cipher

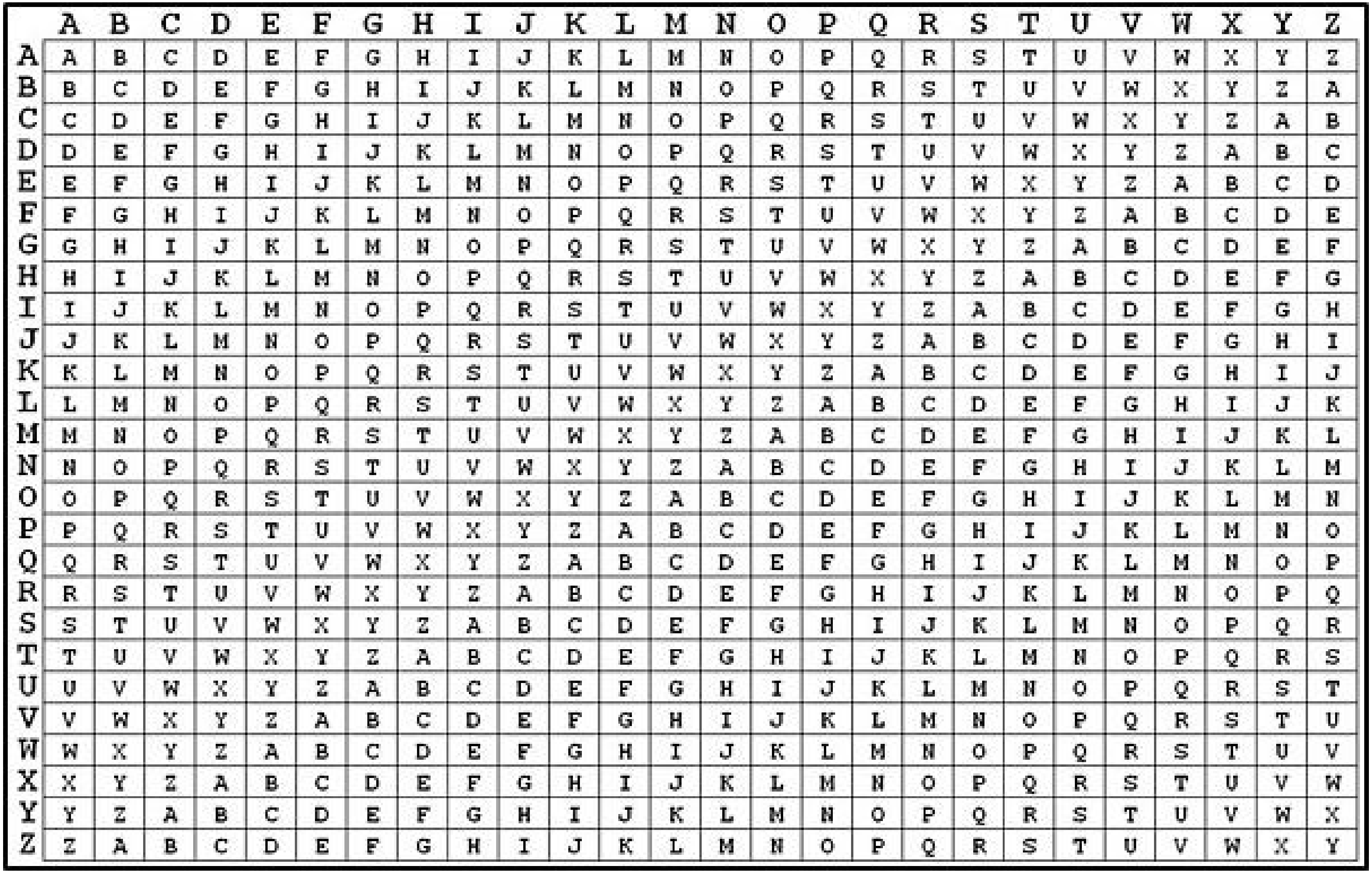
```
CROCODILE
ANIMALANI
```

As indicated by the example above, if the number of letters in the key is shorter than the number of letters in the plaintext, the letters in the key will repeat from the beginning letter of the key until all of the letters in the plaintext are accounted for.

The Vigenere Cipher

After the letters in the plaintext and key are mapped to each other, each plaintext letter / key letter pair needs to be looked up on the Vigenere table, which is a 26 x 26 table that looks like the following:

The Vigenere Cipher



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

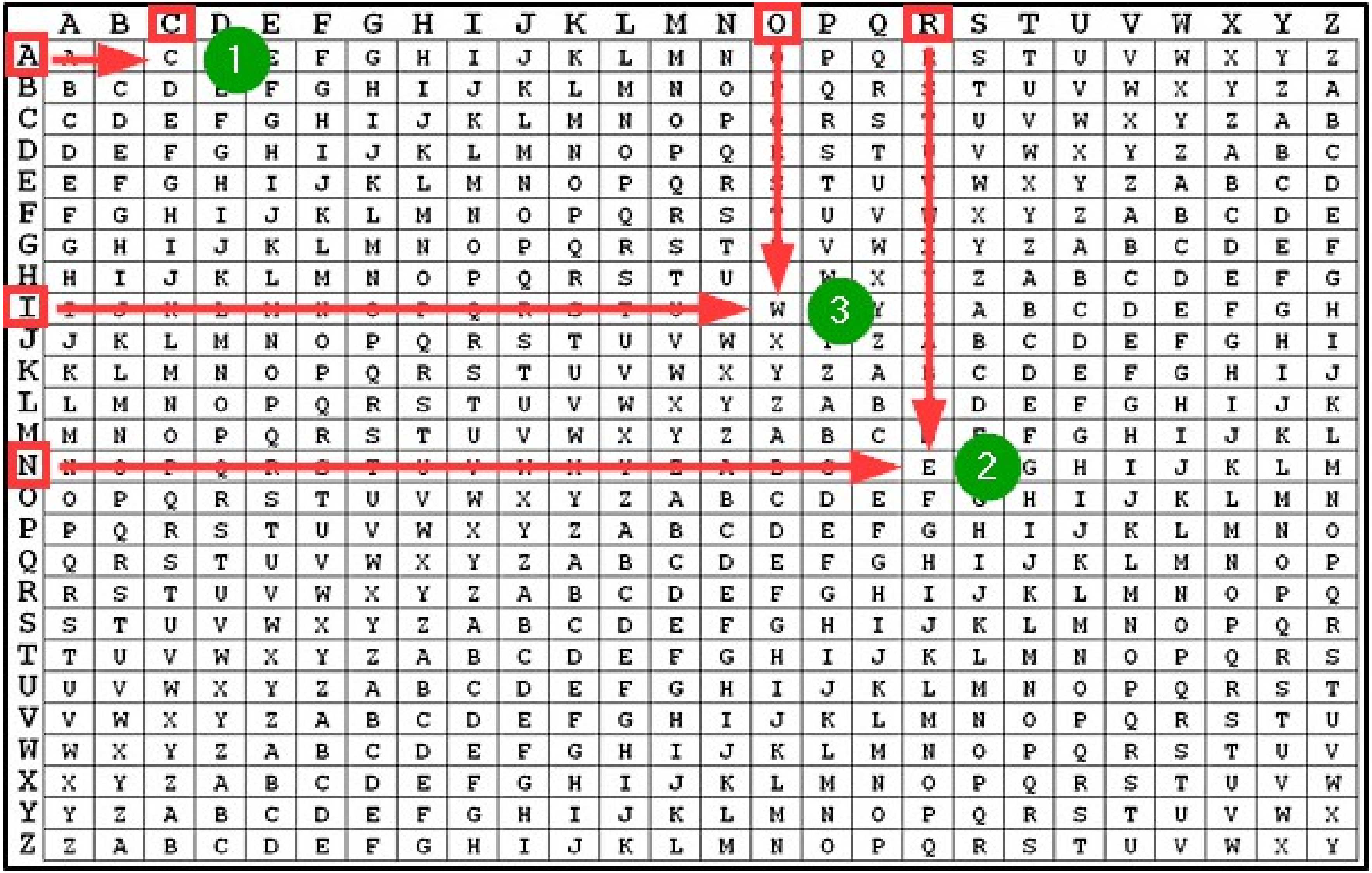
The Vigenere Cipher

For each of the plaintext / key pair, find the plaintext letter on the top row of the table, and the key letter on the left-most column of the table. The letter that is intersected by both the plaintext letter and the key letter is substituted in the place of a plaintext letter as a ciphertext letter.

The Vigenere Cipher

In the following screenshot, you will see the resulting ciphertext letters for the plaintext / key combinations of `C/A`, `R/N`, and `O/I`.

The Vigenere Cipher



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

The Vigenere Cipher

As we can see, the resulting ciphertext letters for `C/A`, `R/N`, and `O/I` are `C`, `E`, and `W`, respectively.

If we complete the example and encrypt the plaintext `CROCODILE` and the key `ANIMAL` using the Vigenere cipher, the resulting ciphertext is `CEWOOOIYM`.

The Vigenere Cipher

Manual decryption of ciphertext encrypted using the Vigenere Cipher is possible if the key is available.

First, identify the key letter / ciphertext letter combinations, then for each key / ciphertext letter pairs, find the key letter on the left-most column, then find the ciphertext letter on the key cell's row.

The Vigenere Cipher

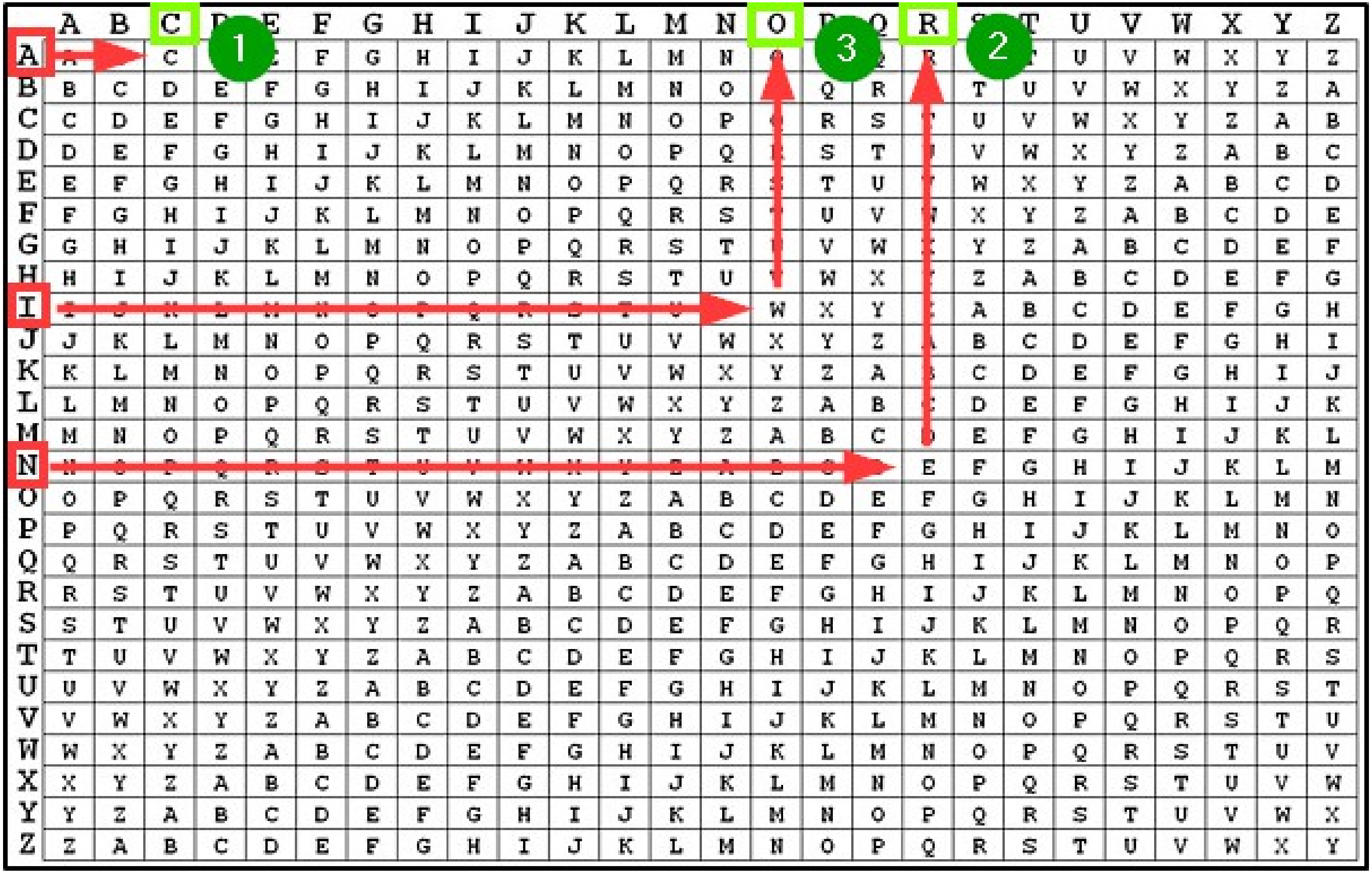
Once found, the letter at the top of the ciphertext letter's column is the plaintext letter.

For example, given the ciphertext `CEWOOOIYM` and provided the key `ANIMAL`, we can again use the Vigenere table for decryption.

The Vigenere Cipher

We'll demonstrate the first 3 key /ciphertext pairs, those are A/C, N/E, and I/W. After mapping the key letters and ciphertext letters on the table, we find the plaintext letters C, R, and O
(key letters outlined in red, plaintext letters outlined in green)

The Vigenere Cipher



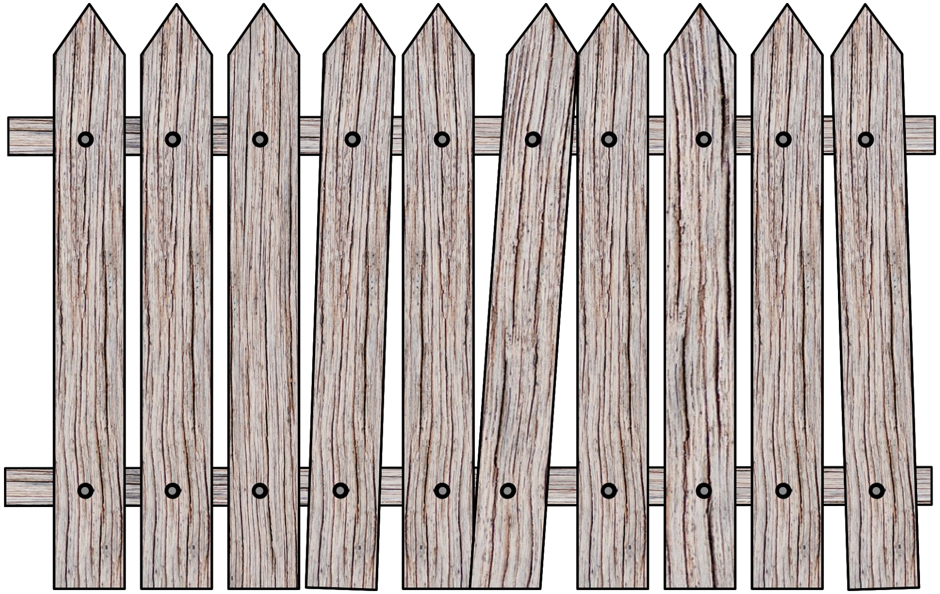
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	[illegible]	C	[illegible]	E	F	G	H	I	J	K	L	M	N	O	[illegible]	Q	R	[illegible]	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	[illegible]	Q	R	[illegible]	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P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

PicoCTF - Vigenere

Let's learn more about Vigenere cipher by working through a challenge on PicoCTF. Navigate to the following URL

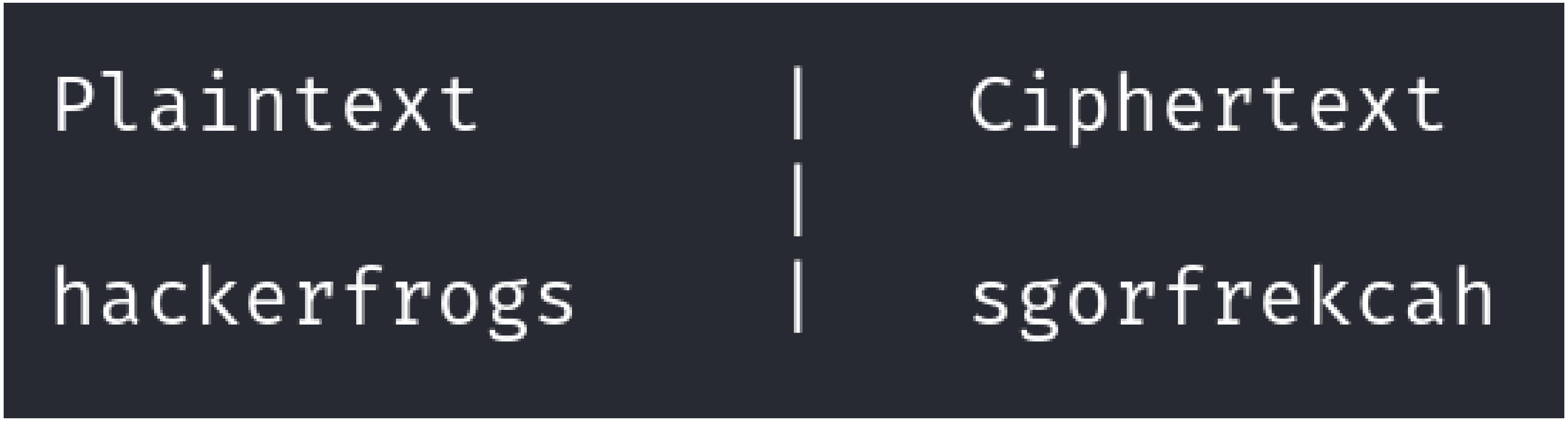
https://play.picoctf.org/practice/challenge/316?category=2&page=1

The Rail-Fence Cipher



Another well-known classical cipher is the Rail-Fence cipher, which is not a substitution cipher, but rather a transposition cipher.

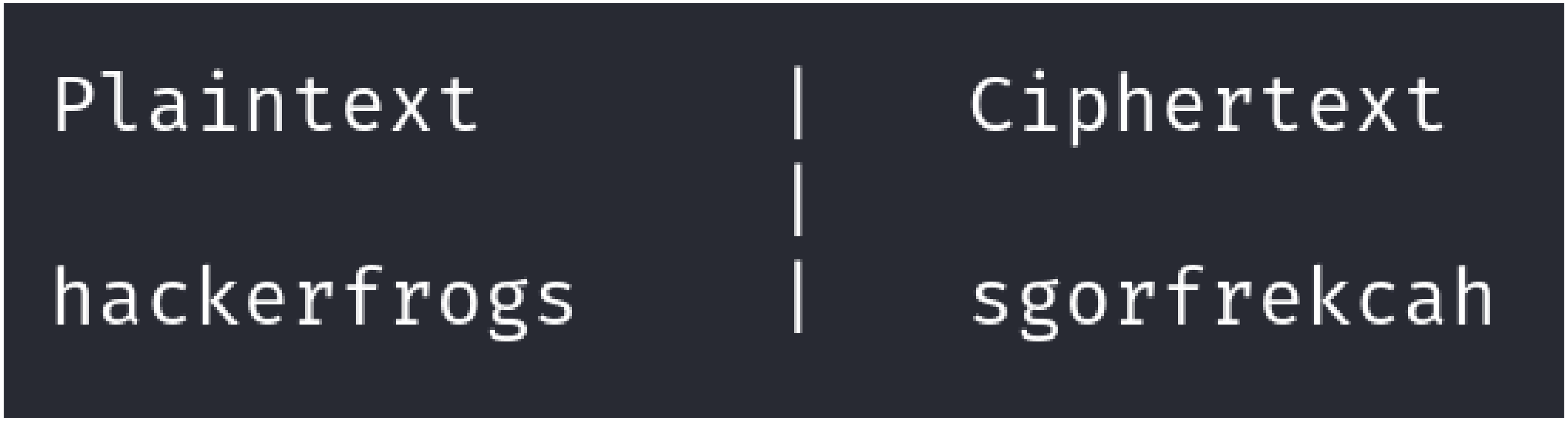
The Rail-Fence Cipher



```
Plaintext         |   Ciphertext
                  |
hackerfrogs       |   sgorfrekcah
```

Transposition ciphers are ciphers where the content of the plaintext are rearranged to form the ciphertext

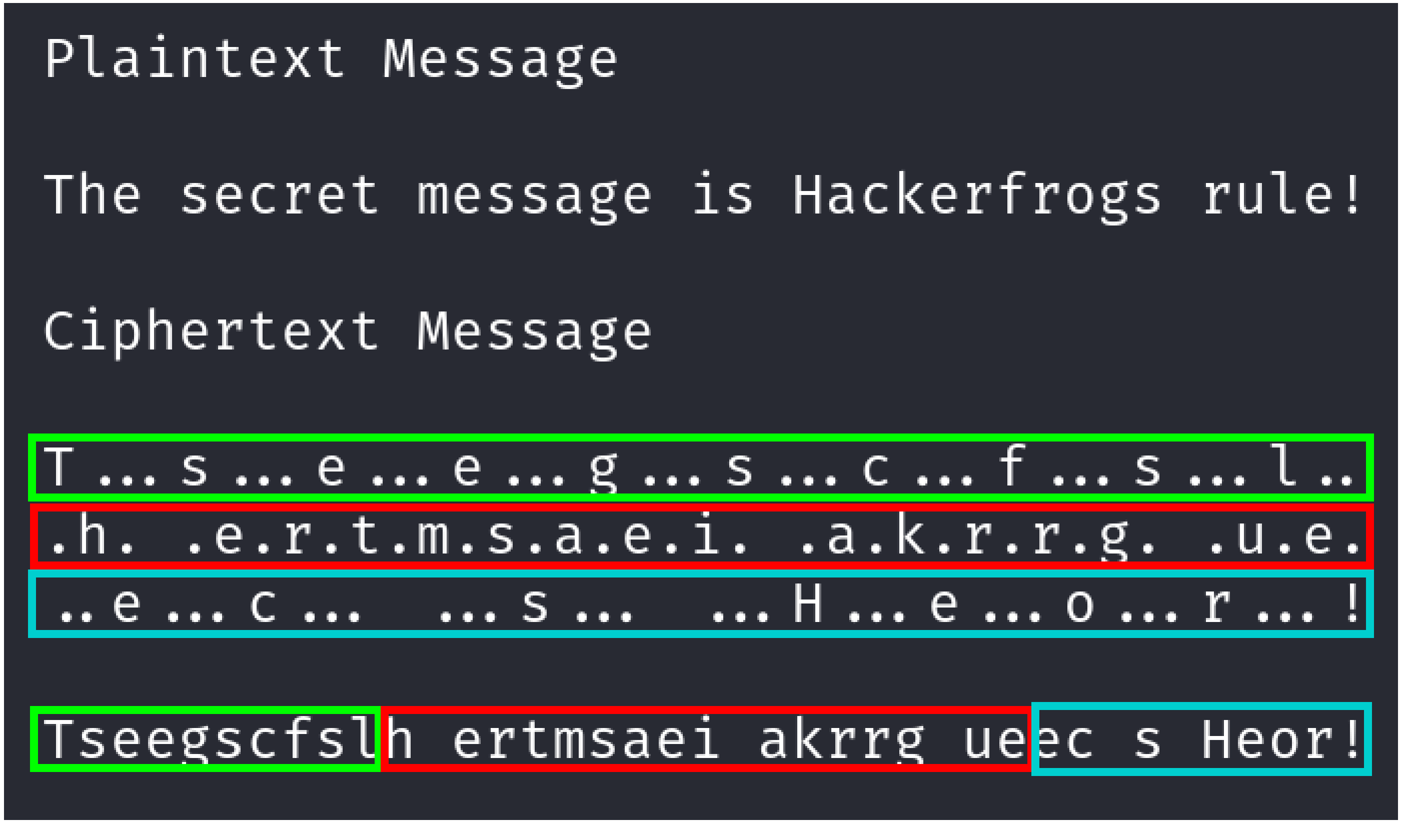
The Rail-Fence Cipher



```
Plaintext           |   Ciphertext
                    |
hackerfrogs         |   sgorfrekcah
```

In the example above, the plaintext string has been reversed to form the ciphertext

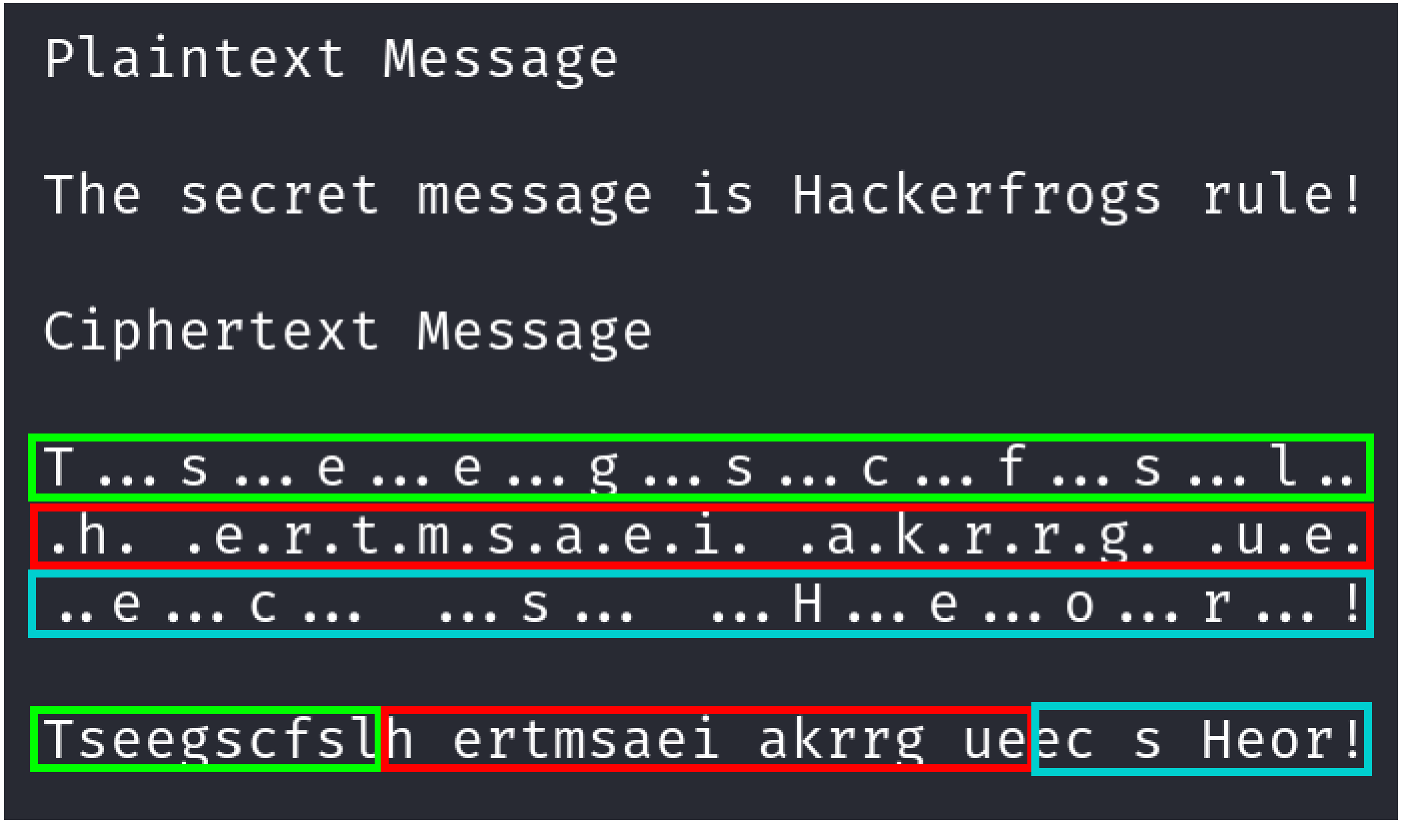
The Rail-Fence Cipher



```
Plaintext Message

The secret message is Hackerfrogs rule!

Ciphertext Message

T...s...e...e...g...s...c...f...s...l..
.h. .e.r.t.m.s.a.e.i. .a.k.r.r.g. .u.e.
..e...c... ...s... ...H...e...o...r...!

Tseegscfslh ertmsaei akrrg ueec s Heor!
```

We form the ciphertext by zig-zagging the plaintext across a grid with a specific number of rows (called rails), and this is known as the key

The Rail-Fence Cipher



```
Plaintext Message

The secret message is Hackerfrogs rule!

Ciphertext Message

T … s … e … e … g … s … c … f … s … l ..
.h. .e.r.t.m.s.a.e.i. .a.k.r.r.g. .u.e.
.. e … c …   … s …   … H … e … o … r … !

Tseegscfslh ertmsaei akrrg ueec s Heor!
```

If we have the ciphertext, and we know the number of rails used (the key), we can decrypt the ciphertext

PicoCTF - Rail-Fence

Let's learn more about the Rail-Fence cipher by working through a challenge on PicoCTF. Navigate to the following URL

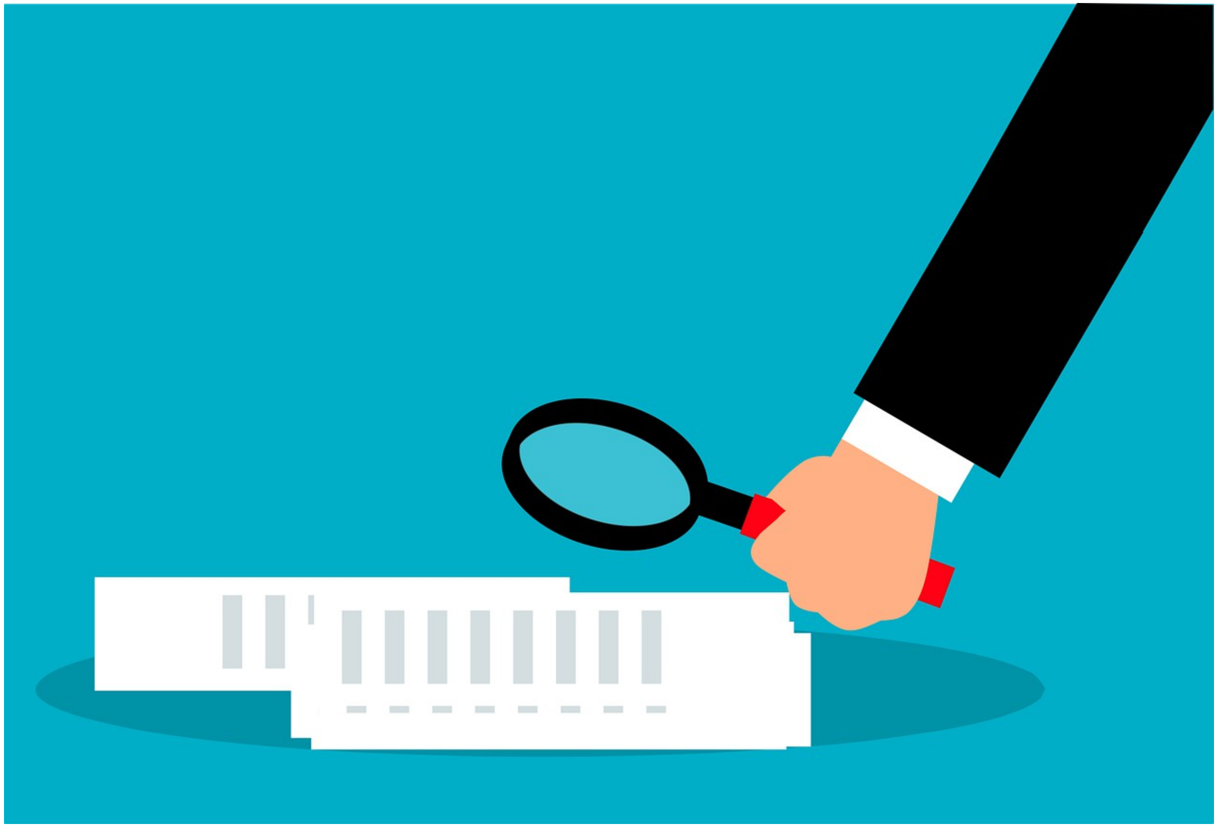
https://play.picoctf.org/practice?category=2&page=1&search=fence

PicoCTF – Transposition Trial

Let's learn more about transposition ciphers by working through a challenge on PicoCTF. Navigate to the following URL

https://play.picoctf.org/practice/challenge/312?category=2&page=1&search=trans

Summary

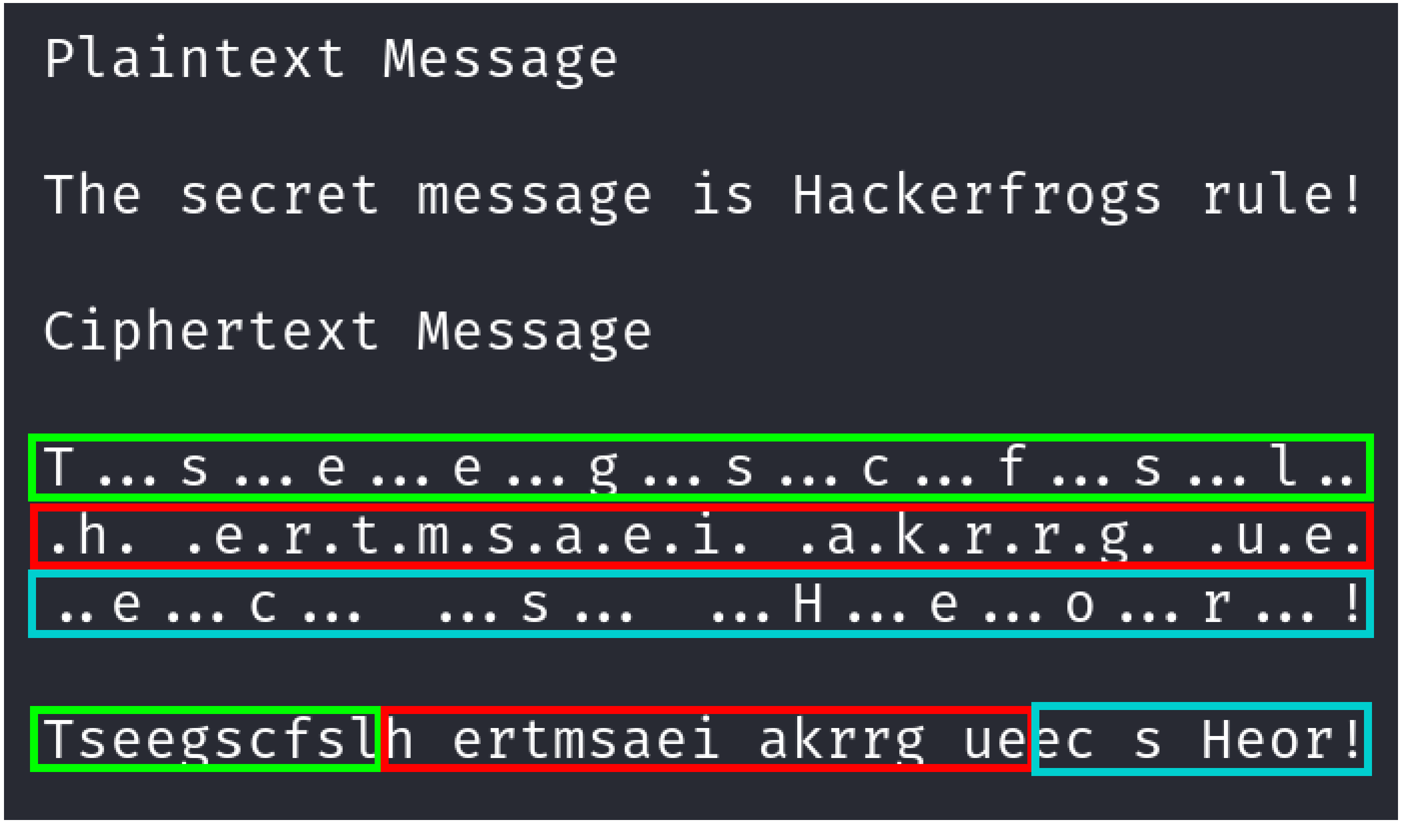


Let's review the cryptography concepts we learned in this workshop:

The Vigenere Cipher

The Vigenere Cipher is a type of symmetrical substitution cipher where each character is substituted according to its relation to a key, which is a word or phrase

The Rail-Fence Cipher

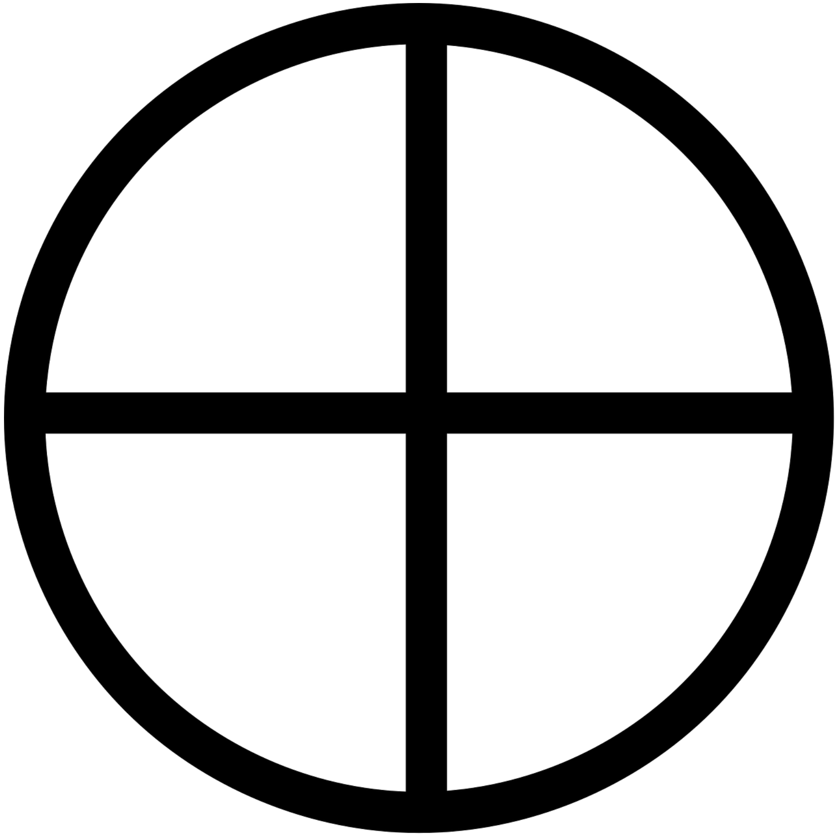


```
Plaintext Message

The secret message is Hackerfrogs rule!

Ciphertext Message

T...s...e...e...g...s...c...f...s...l..
.h. .e.r.t.m.s.a.e.i. .a.k.r.r.g. .u.e.
..e...c... ...s... ...H...e...o...r...!

Tseegscfslh ertmsaei akrrg ueec s Heor!
```

The Rail-Fence cipher is a transposition cipher where the plaintext content remains the same, but it is rearranged according to a specific system

What's Next?

In the next HackerFrogs Afterschool Cryptography workshop, we'll take a look at an important concept for cryptography, the XOR math operation



Until Next Time, HackerFrogs!