HackerFrogs Afterschool Cryptography Basics 4

Class:
Cryptography

Workshop Number:
AS-CRY-04

Document Version:
1.75

Special Requirements:
Registered account at picoctf.org

Welcome to HackerFrogs Afterschool!

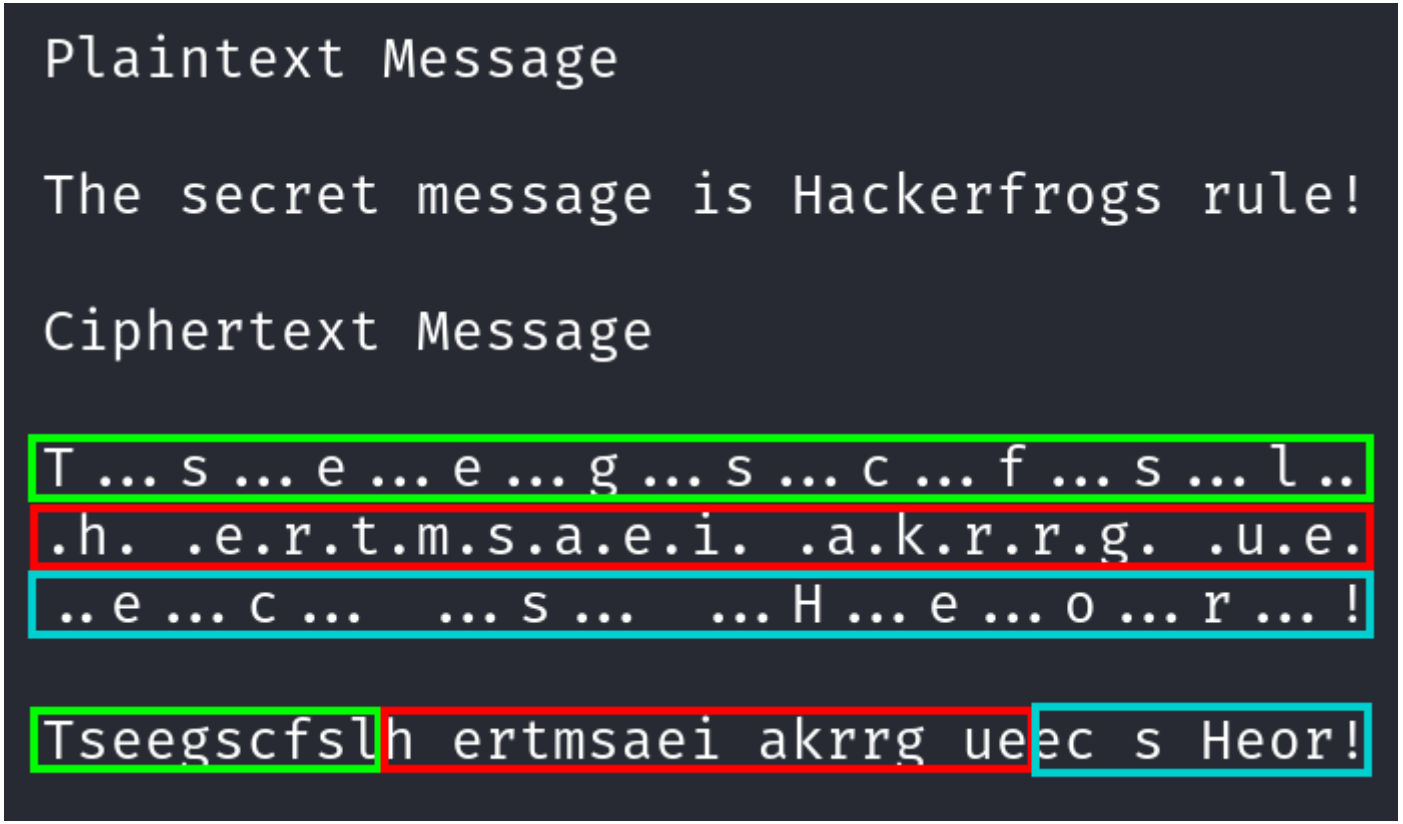
Hey there HackerFrogs! This workshop is the fourth session for cryptography basics

In the last session we learned about the following cryptography concepts

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



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

This Session's Topics

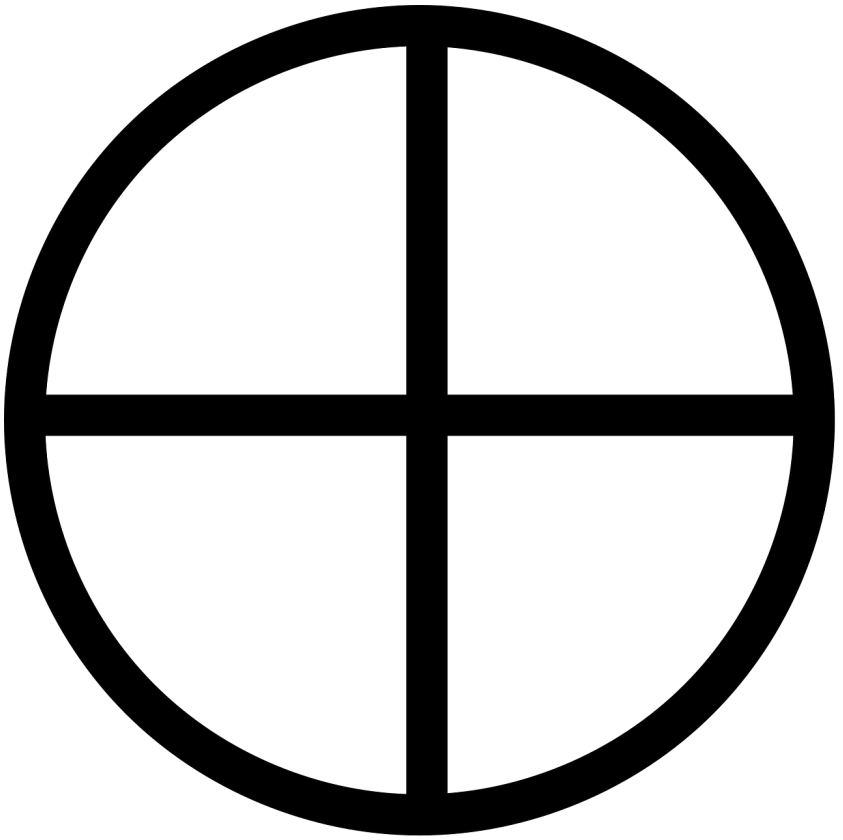
- Intro to the XOR operation

- XOR properties

- Brute forcing XOR

The XOR Operation

XOR is a bitwise operator which can be performed between 2 or more numbers, and returns the number 0 if the bits are the same, and 1 if they are different



The XOR Operation

Hex	Decimal	Binary
0×0A	10	1010

Because XOR is a bitwise operation, non-binary numbers must be converted before XOR can take place

The XOR Operation

Decimal	Binary
10	1010
8	1000
2	0010

Here we see that the result of XOR between the decimal numbers 10 and 8 is 2

The XOR Operation

ASCII	Decimal	Binary
h	102	01101000
F	70	01000110
.	46	00101110

It's possible to perform XOR operations between ASCII characters, since each character can be represented by a binary number

CryptoHack – XOR Starter

Let's learn more about the XOR operation by working through a challenge on CryptoHack. Navigate to the following URL

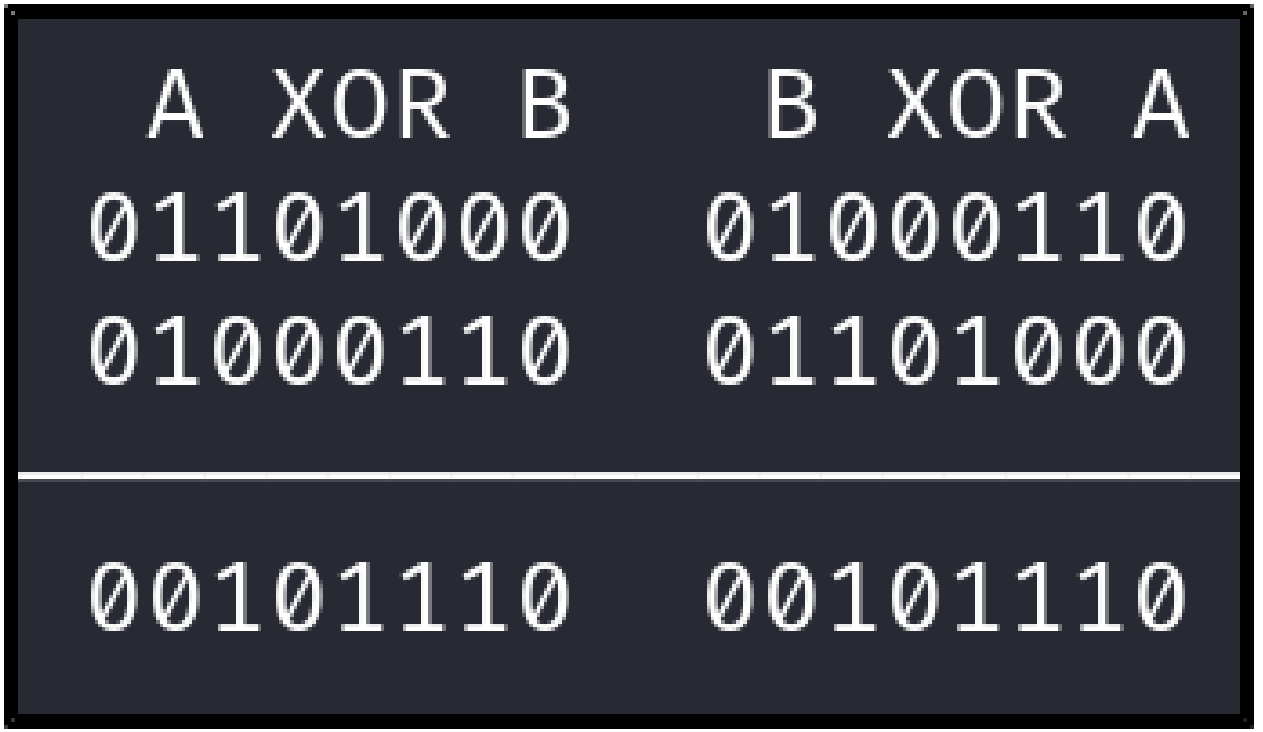
https://cryptohack.org/courses/intro/xor0/

XOR Properties

```
Commutative: A ⊕ B = B ⊕ A
Associative: A ⊕ (B ⊕ C) = (A ⊕ B) ⊕ C
Identity: A ⊕ 0 = A
Self-Inverse: A ⊕ A = 0
```

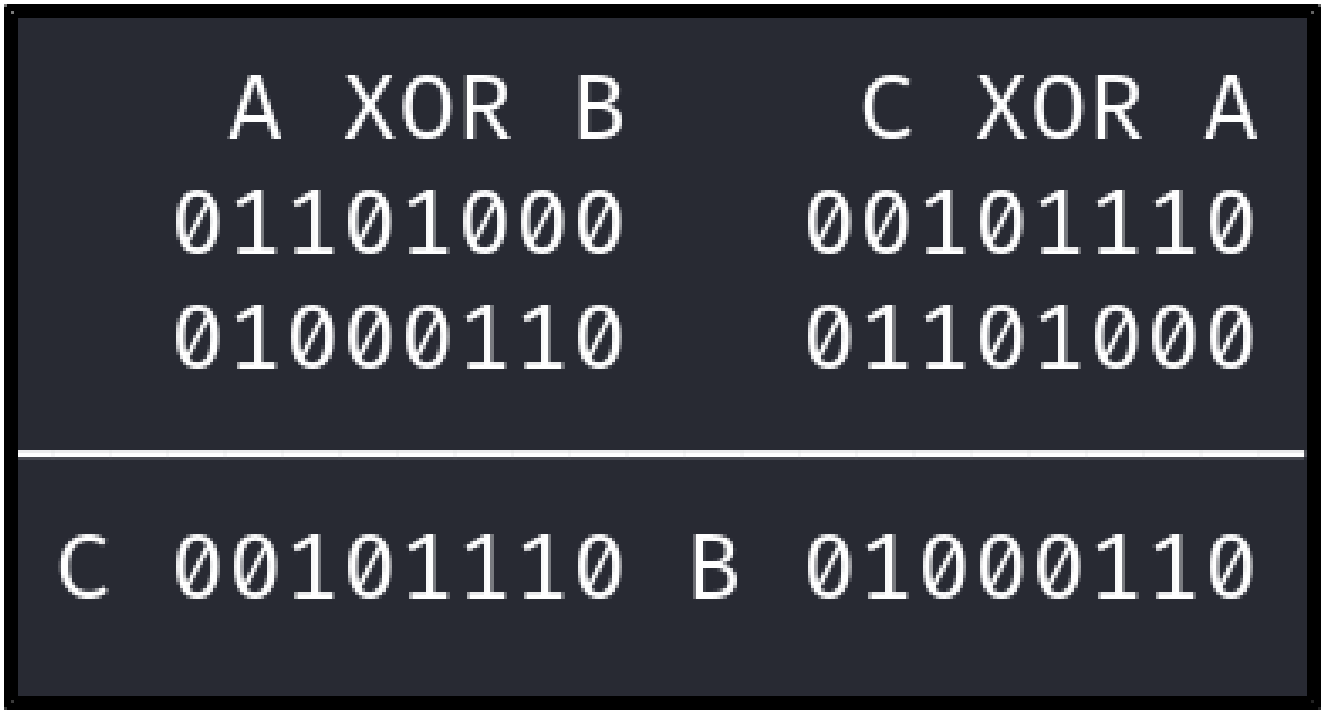
There are several rules that apply to XOR operations, as illustrated above

XOR is Commutative



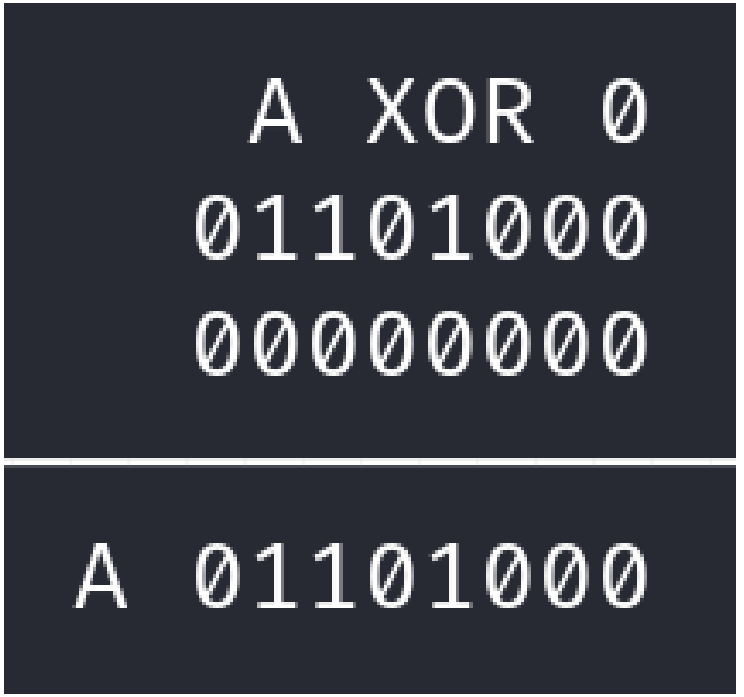
The order in which you XOR numbers does not affect the result. `A ^ B` is the same as `B ^ A`

XOR is Associative



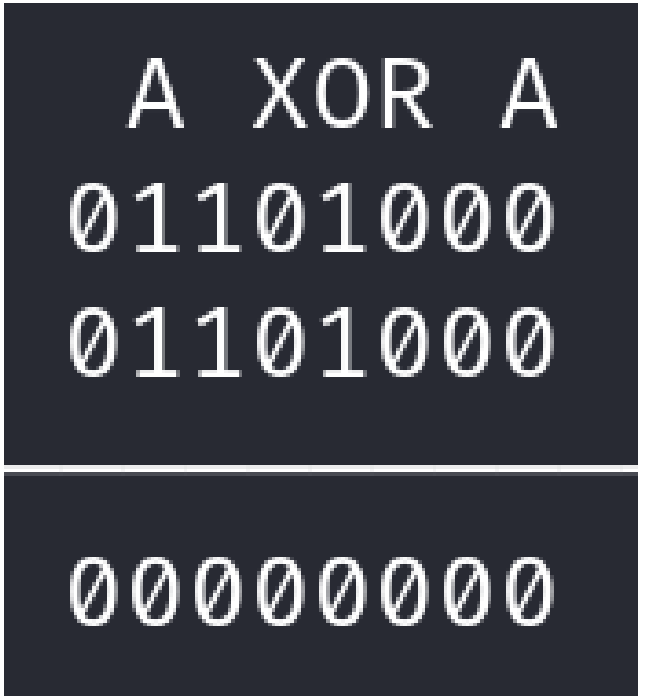
The associative nature of XOR operations means that if we have the XOR result of two numbers, and we know one of the two numbers, we can discover the other number through another XOR

XOR is Identitive (?)



The identitive nature of XOR means that the result of any number XOR zero will be the same number

XOR is Self-Inversive



And finally, the self-inversive nature of XOR means that the result of any number XOR with itself will be zero

A XOR B = C = Cryptography!

```
Plaintext  (A) = secret   s 01110011  e 01100101
Key        (B) = 7K#FPZ   7 00110111  K 01001011
-------------------------------------------------
Ciphertext (C) = D.@45.   D 01000100  . 00101110
```

If we suppose that A is a plaintext string, and B is a key, then the result of A ^ B would be C, which is ciphertext.

A XOR B = C = Cryptography!

```
Plaintext  (A) = secret   s 01110011  e 01100101
Key        (B) = 7K#FPZ   7 00110111  K 01001011
-------------------------------------------------
Ciphertext (C) = D.@45.   D 01000100  . 00101110
```

That means that if we know the ciphertext (c) and the key (B), then we can XOR them together to obtain the plaintext (A)

CryptoHack – XOR Properties

Let's learn more about the XOR operation by working through a challenge on CryptoHack. Navigate to the following URL

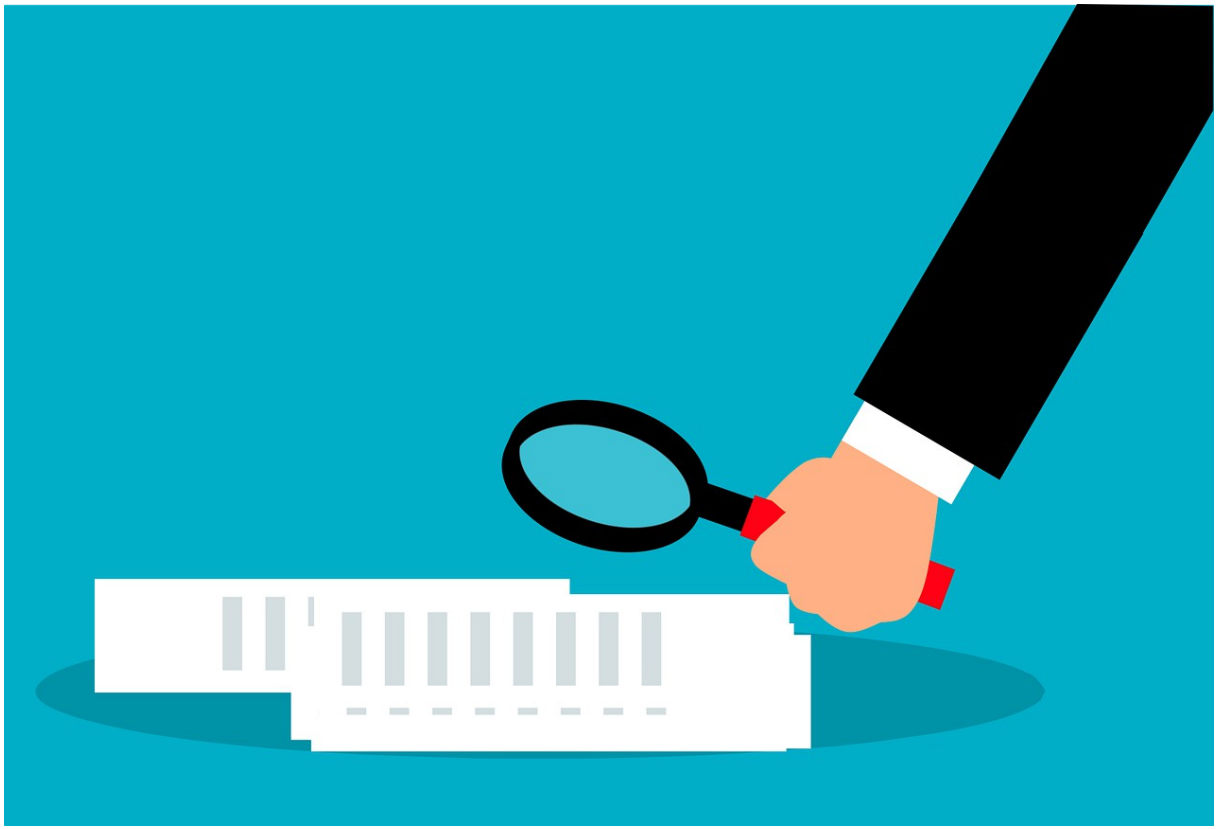
https://cryptohack.org/courses/intro/xorkey0/

CryptoHack – Favourite Byte

Let's learn more about the XOR operation by working through a challenge on CryptoHack. Navigate to the following URL

https://cryptohack.org/courses/intro/xor1/

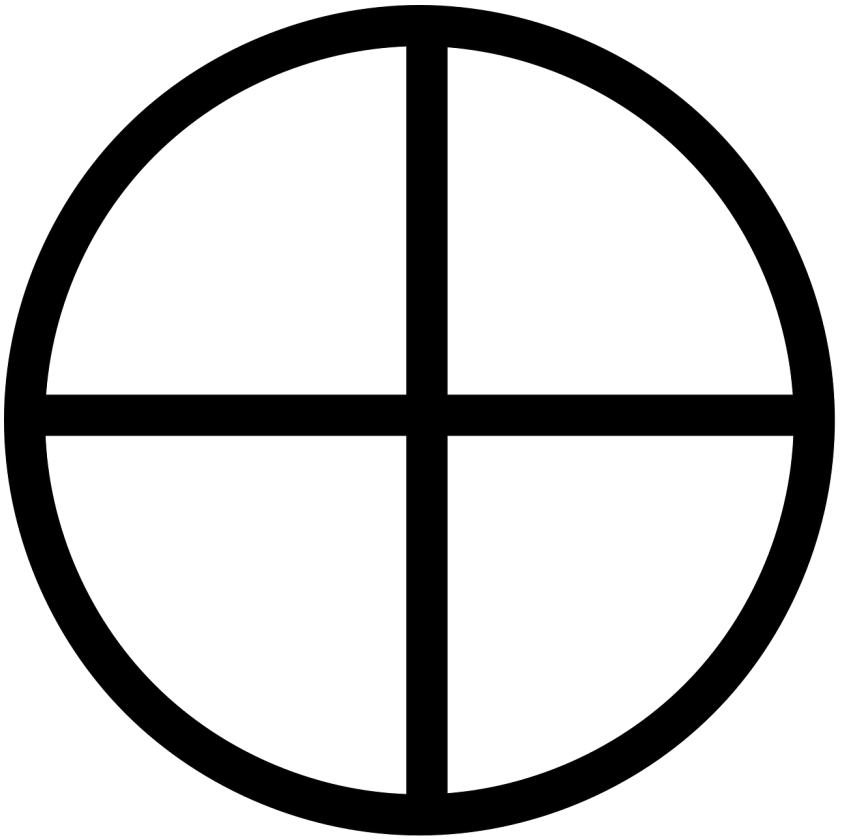
Summary



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

The XOR Operation

XOR is a bitwise operator which can be performed between 2 or more numbers, and returns the number 0 if the bits are the same, and 1 if they are different



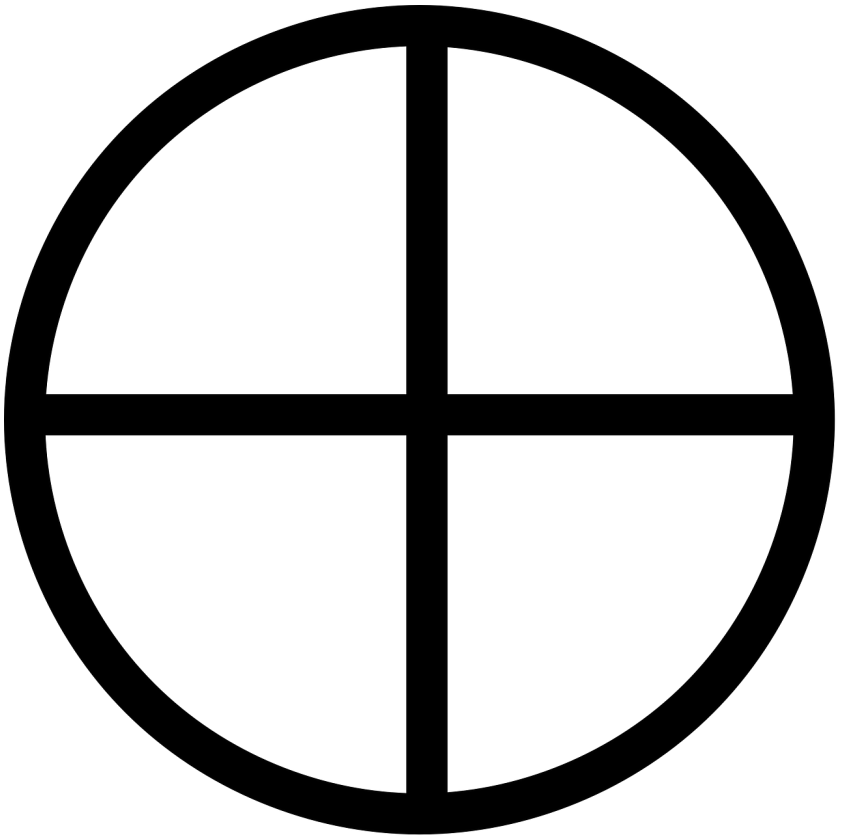
XOR Properties

```
Commutative: A ⊕ B = B ⊕ A
Associative: A ⊕ (B ⊕ C) = (A ⊕ B) ⊕ C
Identity: A ⊕ 0 = A
Self-Inverse: A ⊕ A = 0
```

There are several rules that apply to XOR operations, as illustrated above

What's Next?

In the next HackerFrogs Afterschool Cryptography workshop, we'll take a look at the cryptographic cipher which uses XOR principles, the OTP cipher!



Until Next Time, HackerFrogs!