HackerFrogs Afterschool Cryptography Basics 5

Class:
Cryptography

Workshop Number:
AS-CRY-05

Document Version:
1.75

Special Requirements:
Registered account at picoctf.org

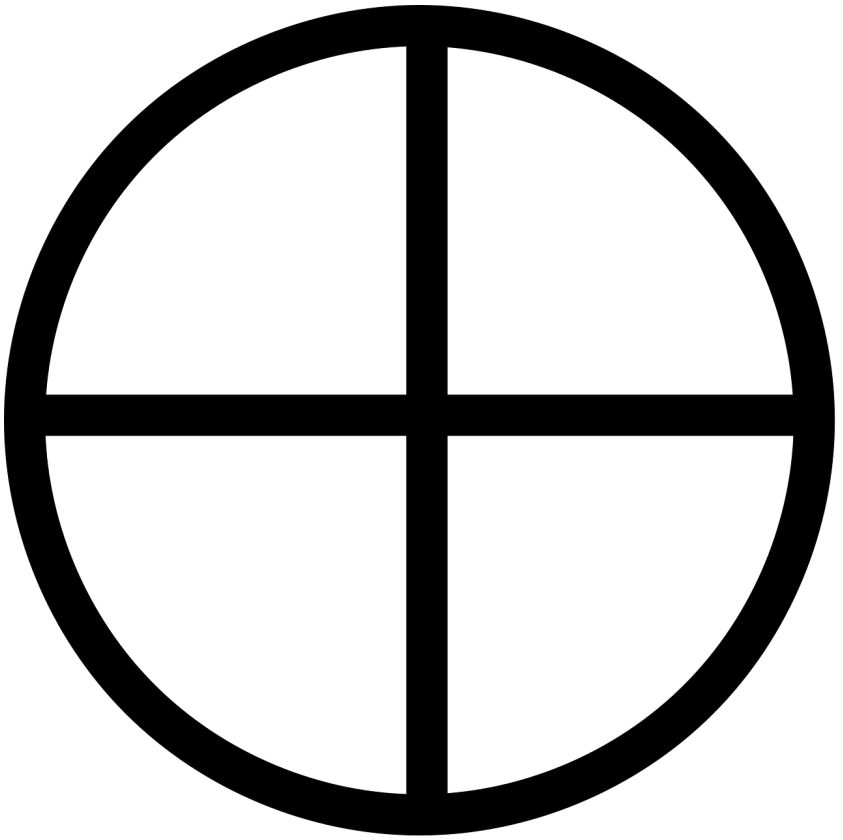
Welcome to HackerFrogs Afterschool!

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

In the last session we learned about the following cryptography concepts

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

This Session's Topics

- Warmup Exercise

- Solving XOR with Partial Info

- The OTP Cipher

Warmup Exercise

Let's reacquaint ourselves with the XOR operation by solving the following challenge over at ctfLearn.com:

https://ctflearn.com/challenge/158

Solving XOR with Partial Data

```
Plaintext  (A) = secret
Key        (B) = 7K#FPZ
Ciphertext (C) = D.@45.
```

Suppose we have a 3 values in a CTF challenge, A, the plaintext, B, the key, and C, the the ciphertext

Solving XOR with Partial Data

```
Plaintext  (A) = secret
Key        (B) = 7K#FPZ
Ciphertext (C) = D.@45.
```

So if we have C, and we can guess at the part of the value of A, then we could get partial insight to the value of B, especially if the length of B is shorter than A

Solving XOR with Partial Data

```
Plaintext  (A) = secret
Key        (B) = 7K#FPZ
Ciphertext (C) = D.@45.
```

So if we have C, and we can guess at the part of the value of A, then we could get partial insight to the value of B, especially if the length of B is shorter than A

CryptoHack – Either you know it, XOR you don't

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/xorkey1/

The OTP Cipher

```
Plaintext  (A) = secret
Key        (B) = hacker
Ciphertext (C) = pwatay
```

The OTP cipher is an encryption technique that requires a plaintext and secret key

The OTP Cipher

```
Plaintext  (A) = secret
Key        (B) = hacker
Ciphertext (C) = pwatay
```

Encryption requires each letter of the plaintext to be combined with its corresponding secret key letter through modular addition

The OTP Cipher

```
Plaintext  (A) = secret
Key        (B) = hacker
Ciphertext (C) = pwatay
```

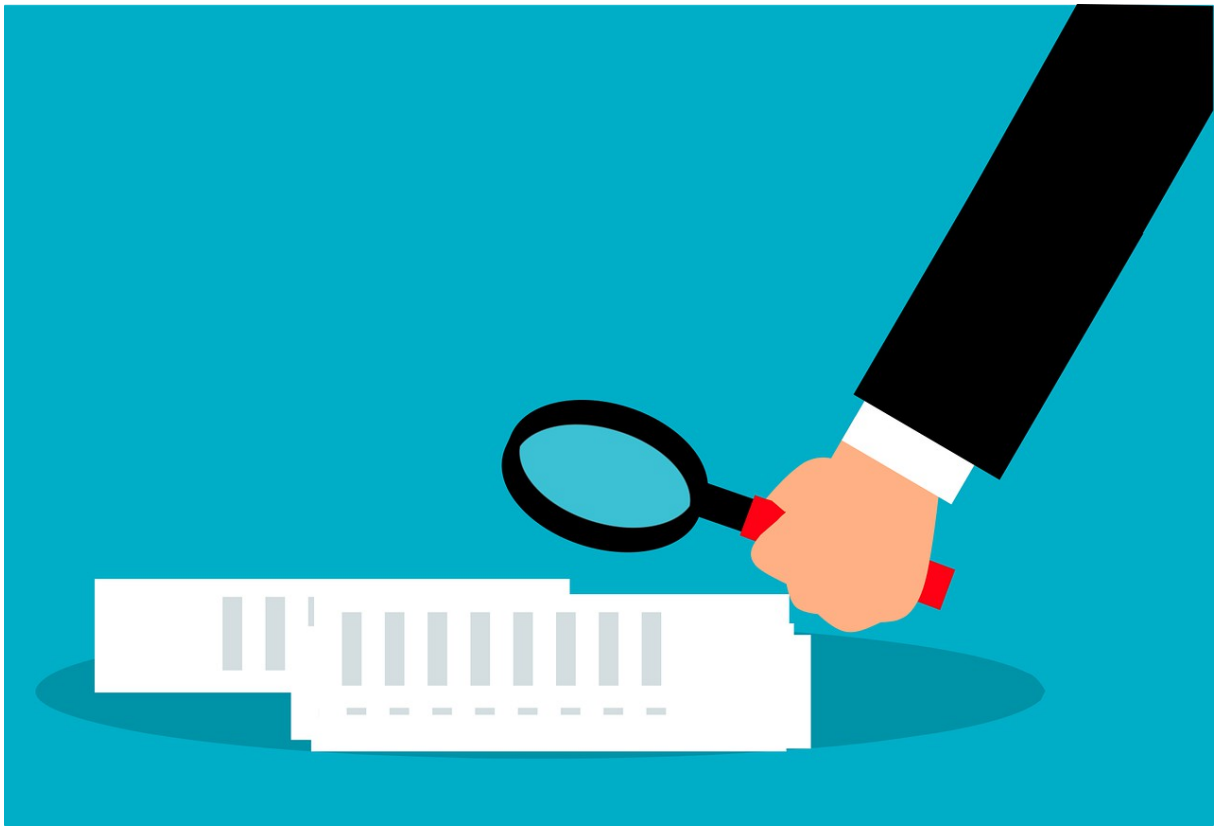
OTP cipher has some similar rules to the XOR operation, since A ^ B = C, and C ^ B = A, etc...

PicoCTF – Easy1

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

https://play.picoctf.org/practice/challenge/43?category=2&page=1&search=eas

Summary



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

Solving XOR with Partial Data

```
Plaintext  (A) = secret
Key        (B) = 7K#FPZ
Ciphertext (C) = D.@45.
```

So if we have C, and we can guess at the part of the value of A, then we could get partial insight to the value of B, especially if the length of B is shorter than A

The OTP Cipher

```
Plaintext  (A) = secret
Key        (B) = hacker
Ciphertext (C) = pwatay
```

OTP cipher has some similar rules to the XOR operation, since A ^ B = C, and C ^ B = A, etc...

What's Next?

In the next HackerFrogs Afterschool Cryptography workshop, we'll do an overview of a very well-known modern cryptography system: RSA

Until Next Time, HackerFrogs!