Cryptography in python

What you will need

- ❏ General understanding of how bytes and bits work in computers
- ❏ Basic knowledge in any programming language
- ❏ A fully working linux virtual machine (preferably kali or parrotOS)
- ❏ A set of python3 libraries to be downloaded
- ❏ Some knowledge in python would help but is not required
- ❏ Stop me and ask questions as soon as you feel lost

Intro to python

- Python is an interpreted programming language used in security, especially in cryptography.
- The ease with which python deals with bytes and encodings makes it perfect for our desired use
- Writing in Python is almost like explaining an algorithm to your friend, it’s almost english

Crypto fundamentals

- bytes data type in python
- The difference between enciphering and encoding of data
- The XOR operation
- Famous XOR implementation
- Block ciphers
- Modes of operations
  - ECB
  - CBC
  - Much more

Bytes

- We can think of bytes as a number system of base 256
-
```
>>> bytes_to_long(b"AB")
16706
>>> (ord("A")*256**1) + (ord("B")*256**0)
16706
>>> _
```
- Why do we need bytes?
  - Ease of conversion from string to numbers in different formats like:
    - Binary
    - Hex
    - Base64

Exercises

- We will walk-through Set1 (exercises 1-8 excluding 6 and 8) of cryptopals
  - https://cryptopals.com/sets/1
- Unbreakable Encryption from MetaCTF 2021
- xorxorxor from HackTheBox
- Welcome Challlenge.py

Recommended Challenges

- “Hex” on Cryptohack
  - https://cryptohack.org/challenges/general/
- “You either know, XOR you don't” on Cryptohack
  - https://cryptohack.org/challenges/general/
- MODES OF OPERATION STARTER
  - http://aes.cryptohack.org/block_cipher_starter/
- Nuclear Sale on HackTheBox
  - https://app.hackthebox.com/challenges/nuclear-sale

Where now?

- Cryptohack for mini courses on different cryptography topics
- Cryptohack for many practice challenges
- Cryptopals for many topic centered sets to practice on
- Ashutosh1206 for references about famous vulnerabilities in cryptosystems
- JacksonInfoSec for implementations of cryptosystems in python
- FilippoValsorda for solving cryptopals on stream
- The Krypton wargame for solving cryptanalytic problems
- HackTheBox for challenging CTF challenges