

# Assignment 1 - TEA Bruteforce Attack in Python 3.9

---

## CPS - 472 Computer & Network Security

Written By: Jacob Scheetz, Spring 2021

### Description

- script that reads in 32 bit unsigned integer plaintext/ciphertext pairs to perform a bruteforce attack on 1 round of the TEA. By using a plaintext/ciphertext pair consisting of 32 bits a piece, we essentially reduce TEA's key space in half. By repeatedly guessing 32 bits of the key, this script deduces the remaining 32 bits of the key left.

### Program Usage:

```
py Scheetz-AS1.py -nameofsampladata
```

### Sample output runs

```
PS C:\Users\Jacob\Desktop\school\spring-2021-classes\cps472-comp-net-sec\Scheetz-AS1> py .\Scheetz-AS1.py .\testrun1.txt
Matching keys have been found and verified!
First Key (k0) is: 999999
Second Key (k1) is: 888888
Runtime of bruteforce was: 1.897001 seconds
```

```
PS C:\Users\Jacob\Desktop\school\spring-2021-classes\cps472-comp-net-sec\Scheetz-AS1> py .\Scheetz-AS1.py .\testrun2.txt
Matching keys have been found and verified!
First Key (k0) is: 656578
Second Key (k1) is: 9999875
Runtime of bruteforce was: 1.251002 seconds
```