Foundations of Cyber Security 2023

CTF Challenge Proposal (Team: Cryptohackerz)

Members

- [Carina] (https://github.com/carinachu22)
- [Vimal] (https://github.com/usvimal)
- [Siddharth] (https://github.com/mrtlrt)
- [Akash] (https://github.com/akashcx)
- [Yu Jie] (https://github.com/fishorfished)

Context

This CTF challenge adapted the characters from Spy x Family anime. For those who have watched it, this will be fun! For those who didn't, here are some key details of the main characters that will help with the challenges:

1. Anya is a 5 year old little girl who likes to watch a spy tv show, and will sometimes create ciphers.
2. Damian is a boy in the same class as Anya and they are always bickering.
3. Anya's favourite is her fluffy white pet dog called *Bond*.

Introduction

On the last day of school, Damian was mocking Anya for her ugly artwork that she did and Anya got angry. Damian was puzzled why she suddenly teared up and ran away. 2 hours later, Anya came running back to him and thrusted letter into his hands, and ran away again.

Even more confused, Damian opened the letter to reveal some undecipherable words. Damian is asking you for help! Please go to challenge 1 to view the letter and help damian decipher what anya wrote.

Challenge 1

Story:

The letter contains three values on it.

1. Modified plaintext (m')
2. Original cipher (c)
3. Modified cipher (c')

Task:

Find the original plaintext (m)

Given:

1. Modified plaintext (m') = b'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00Find the URL'
2. Original cipher (c) = b'l\xbfm\rl\x9bY\x11\x13\xea\xa9\xff\x83\x81W\x04\xc7T\xb3\xf0\x9740a\x19\xa9x\x8f\xc58O\xcdV1`\xac\xcd6'
3. Modified cipher (c') = b'!\xcb\x19}:\xa1v>c\x8b\xda\x8b\xe6\xe38e\xb50\x9d\x93\xf8\x1b\x7f-N\x9fw\xa2\xc9\x12\x1a\xc8len\x89\xf1\x1d'

Intended Solution:

There are two possible solutions.

The first solution:

1. mask = c XOR c'
2. original plaintext (m) = mask XOR m'

The second solution:

1. k = m' XOR c'
2. original plaintext (m) = c XOR k

Original plaintext (m) = https://pasteboard.co/OLW6IDbNuqR1.png

Challenge 2

Story:

Damian successfully solved the 1st challenge, but he is puzzled by its solution. It seems like the solution for Challenge 1 is linked to Challenge 2. Luckily, Damian knows that Anya cannot spell many things, usually <= 4-lettered words. Damian needs your help for challenge 2! Hint: You can re-read the context portion for hints of the key.

Task:

1. Figure out what kind of cipher it is
2. Find the key
3. Decrypt the ciphertext

Given:

1. Key: Hint from Challenge 1
2. Cipher: V
3. Ciphertext: NCQXMIF GBVT HYDBQFBG DCQT

Intended Solution:

1. Using cipher: V, figure out that it is a Vignere cipher
2. Find the key for the cipher which is Bond. (The name of the dog)
3. Use the key to decrypt the ciphertext

Challenge 3

Story:

Woohoo! Damian has successfully solved the second challenge as well…only to find out there's a third challenge? He finds that the solution from the second challenge is an encrypted message. This has to be the last challenge, hopefully.

Damian realizes that someone who can only spell a handful of words can also only count until 3 digits. And that they wouldn't be proficient with crafting RSA encryption. With this knowledge, can you crack the private key d?

Task:

1. Find the private key d.
2. Using the private key d, find the flag (which is of the format fcs{xxxxxx})

Given:

1. From Challenge 2: n e
2. Encrypted message: AABI BAFI BE ACHC IFH CEBG CIBA CI AHAX HGE BHED IAD AHAX AFHA AFBF AXCE DGB CIBA AXCE CAFD ADA
3. Mapping: A: 1 | B: 2 | C: 3 | D: 4 | E: 5 | F: 6 | G: 7 | H: 8 | I: 9 | X: 0

Intended Solution:

1. Use the mapping and convert the given into numbers.
2. From n use prime factorization to find the primes p and q (Hint: Anya can only count to 3 digits)
3. Using p and q find z and d (private key)
4. Use d to decrypt the message and find the flag.