Features Business Explore Pricing This repository Search Sign in or Sign up

DogodCTF / ctf-writeups

Watch 1 Star 3 Fork 1

Code Issues 0 Pull requests 0 Projects 0 Pulse Graphs

Branch: master ctf-writeups / volga-ctf-quals-2017 / PyCrypto150 / Create new file Find file History

Felix Hellman Format edit Latest commit `b81fcdc` 7 days ago

..

README.md	Format edit	7 days ago

README.md

Volga CTF Quals 2017 PyCrypto

Category: Crypto, 150 points

> This crypto algorithm uses a huge key and it's implementation is not so trivial to reverse engineer. Isn't it wonderful?

Write-up

We take a peek in encrypt.py -> 160 bit key, 20 bytes.

A team mate noticed that when using a secret of multiple A's, we can see a repetition in the cipher text. Probably Xor Then.

```
$ echo 'flag="AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"' > se
$ ./encrypt.py
$ cat flag.enc
G��%�a�����H�M�MG��%�a�����H�M�MG��%�a�����H�M�MG��%�a�����H�M�MG��%�a�����H�M
```

We toss the provided flag to https://wiremask.eu/tools/xor-cracker/

We know the key is 20 bytes and we get two suggested keys. The unencrypted text becomes the following with the top suggested key.

> key = d1 ff 63 f7 c8 75 d8 c4 1a 84 ca 24 5b 66 0c 1f c6 e2 cc ea

> �ol3$CTF{�@m _is_Pad�Ma:<_Tim s_�@d_Mi$$�mek8 Gil'er1 Vernamewa'ean A�&TeBell La's 1+gine r 2ho, in t91ci inv nt d an ad!it=3e po)ya)phabeti& ...

Not quite right. But we learn some key things. The plaintext after the flag is about Gilbert Vernam, looking at his wikipedia page, we figure out po)ya)phabeti& should be polyalphabetic.

We do some Xor math and calculate the key should be

> key = 94 ff 63 a3 8d 75 d8 c4 1a c1 ca 24 1e 66 0c 1f c6 e2 cc ea

We use this following code to decrypt the text

```
int main()
{
        char key[20] = { 0x94, 0xff, 0x63, 0xa3, 0x8d, 0x75, 0xd8, 0xc4, 0x1a, 0xc1, 0xca, 0x24, 0x1e, 0x66, 0x0c, 0x

         FILE *fileptr;
         char *buffer;
         long filelen;
```

```
         fileptr = fopen("flag.enc", "rb");
         fseek(fileptr, 0, SEEK_END);
         filelen = ftell(fileptr);
         rewind(fileptr);

         buffer = (char *)malloc((filelen+1)*sizeof(char));
         fread(buffer, filelen, 1, fileptr);
         fclose(fileptr);

         int i;
         for(i = 0; i < filelen; i++) {
                 printf("%c", buffer[i] ^ key[i%20]);
         }

         return 0;
 }
```

We now get this plaintext.

> VolgaCTF{N@me_is_Pad_Many_Times_P@d_Mi$$_me?} Gilbert Vernam was an AT&T Bell Labs engineer who, in 1917, invented an additive polyalphabetic ...

Bingo.