Tweet

**Hello peeps,**

Today we will be learning how to solve Cryptography Challenges from Cryptopals. Cryptopals is an online platform which consists of different sets of cryptography challenges. There are people out there who are totally new to programming and cryptography just like me, and these challenges are worth your time for clearing out the basics.

So, I will be giving a walk-through on Cyptopals set 1, challenge 1 which is to convert a given hex string into base64.

In this challenge, a string has been given which should produce an output that should match the one, provided in the challenge. Our task is to write a script to automate the conversion of hex string into base64.

I will be using python for this walk through; however, you can use the programming language of your comfort as the logic will remain the same.

While trying to generate the required output, i will be using two modules:

- Base64
- unhexlify from the module binascii

I used the base64 module to convert the string to base64 and the unhexlify module to get the binary data represented by the hexadecimal string.

So, I convert the  hexadecimal string into binary data which I further encode into base64 value.

Here we go:

```
string =
"49276d206b696c6c696e6720796f757220627261696e206c696b65206120706f69736
f6e6f7573206d757368726f6f6d”
raw = unhexlify(string)
print (raw)
```

The output of the above code should be similar to the below screenshot:

Yes, the output does say something. If you get the above output, it means you are doing it correctly.

Next step is to convert the string into base64.

```
bin_raw = base64.b64encode(raw)
```

```
print bin_raw
```

And you get the required output:

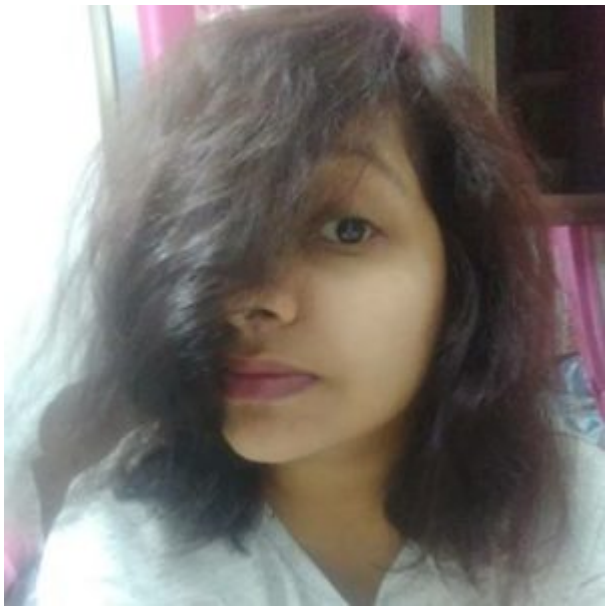
Sounds easy, right?

Yes, it is! 

The first challenge is quite simple to do but as it keeps going, the challenge becomes more tricky and interesting.

Cryptography deals with such encoding and decoding and it is important for us to understand how a simple piece of string is getting converted. Later, we will come to know how it is being used entirely.

In the upcoming days, i intend to write walkthroughs and my leanings on Cryptography. Until then, happy decoding!!!



cryptfreak

I am currently improving my skills in Application and mobile-based security. My area of research includes **Blockchain**, specially **Ethereum based Smart Contracts**. But

**Cryptography** and **Mathematics** have always been my first love. I am highly passionate about information security and I deeply involve myself into the logic behind. **I prefer Decoding things than Breaking them**