QIWI CTF 2016 - Crypto 300_1

Nov 18, 2016 • By thezero
Category: writeups
Tags: crypto qiwictf-2016

Crypto 300_1

Crypto - 300 Points

Alice, Bob, and Cameron want to get shared key by Diffie-Hellman method. Their public keys respectively are g^a mod p, g^b mod p, g^c mod p. Will Alice and Bob be able to get shared key without Cameron's private key? The flag is the first 20 digits of the shared key in decimal form.

```
p:
898615866193008508601970840287040219111417174591316046945431587655694737064279

g: 6;
a: 230;
b: 250;
g^c:
536161780083359874153092408176222547741827701014202262273168815829775962132940
```

Writeup

This is a simple crypto challenge on the Diffie-Hellman key exchange protocol.

In this scenario we have 3 user that need to agree on a shared key and we need to calculate it.

The formula for the shared key is: $g^{abc} \ mod \ p$.

We have Alice and Bob private key (a and b), but we have only Cameron public key $g^c \ mod \ p$

We can't compute directly $(((g)^a)^b)^c \bmod p$ but we can compute the shared key this way: $((g^c)^a)^b \bmod p$

The python-sage script that get the flag

```
#!/usr/bin/env sage -python

p=898615866193008508601970840287040219111417174591316046945431587655694737064

g=6
a=230
b=250
gc=536161780083359874153092408176222547741827701014202262273168815829775962132

gca = (gc**a) % p
gcab = (gca**b) % p

print "flag: ", str(gcab)[:20]
# flag: 38058349620867258480
```