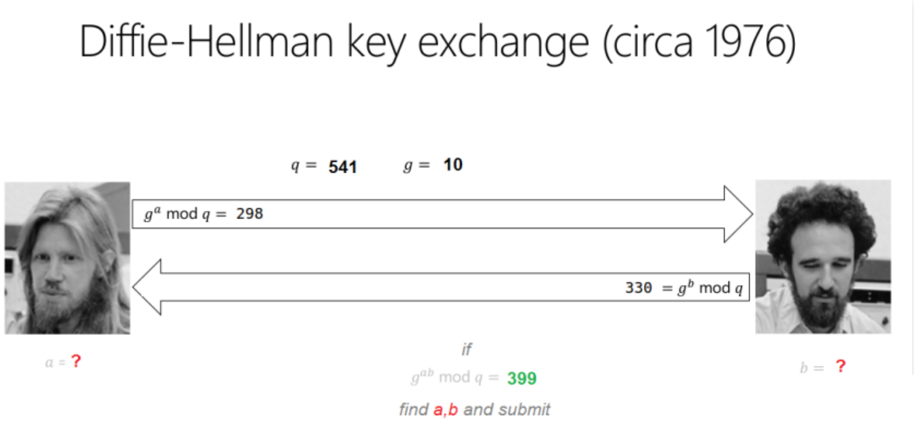
Warren Paulus

Information Security Consultant: Analyzing, Testing and Fixing IT components to increase their security

nullcon HackIM – 2017 – Crypto 2

Here is how to resolve the challenge "***Breaking Bad Key Exchange***" provided, during a CTF, by nullcon HackIM in February 2017:



nullcon HackIM – 2017 – cryptopuzzle2

> *Hint 1 : in the range (1 to g*q), there are couple of pairs yielding common secrete as 399.*
> *Hint 2 : 'a' and 'b' both are less than 1000*
>
> *Flag Format: flag{a,b}*

First, write down the information you got:

> *q=541*
>
> *g=10*
>
> *g^a mod p=298 –> a?*
>
> *g^b mod q=330 –> b ?*

> *g^ab mod q=339 -> a,b?*

It will be interesting to resolve the unknown variables in both equations and get all possible values. To do this, I used the second hint and I wrote a Python script like this:

```
# init
q=541
g=10
res_a=[]
res_b=[]

# get the unknown values a and b
# range(0,1000) because of hint 2
for x in range(0,1000):
 if pow(g,x)%q==298:
  res_a.append(x)
  print "a ="+str(x)
 if pow(g,x)%q==330:
  res_b.append(x)
  print "b ="+str(x)

# check the values found a and b
# with the third equation
for y in res_a:
 for z in res_b:
  if pow(pow(g,y),z)%q==399:
  #if pow(g,(y*z))%q=399:
   print "a = "+str(y)+" b = "+str(z)
```

The result was:

> *a = 170 b = 268*
> *a = 170 b = 808*
> *a = 710 b = 268*
> *a = 710 b = 808*

The flag was ” **flag{170,808}** “. (+ **350 points!**)

Do not hesitate to leave me comments! 🙂

Share this:

Twitter Facebook G+ Google

★ Like

Be the first to like this.

warrenpaulus / February 24, 2017 / CTF, nullcon HackIM - 2017 / crypto, CTF, diffie-hellman, key, modulus, python