Subscribe to RSS feed

Search Search

More Smoked Leet Chicken

We pwn CTFs

- Home
- rfCTF 2011
- Hack.lu 2010 CTF write-ups
- Leet More 2010 write-ups

« Olympic CTF Sochi 2014 Registration is Open

Codegate 2014 Quals — Minibomb (pwn 400) »

Feb
09

Olympic CTF 2014 GuessGame (300)

- Writeups

by hellman

> Be careful, it's cheating!
> nc 109.233.61.11 3126

Summary: discrete logarithm with group oracle

This challenge was in FigureCrypting category in Olympic CTF 2014. At first, there was some proof of work required (I've stolen this idea from some GitS ctf):

```
$ nc -n 109.233.61.11 3126
Proof of work, please
Prefix is (hexed) 25cbcf3a964c3fc5
sha1 prefix (hexed) must be 000000
input (hexed):
```

Puzzle can be solved with this C script.

```
...
Let's play a guess game:
  How many 'tinsels' are there in 'therese'?
You can use [mix a b] or [inv a] commands 251 times.
Use [guess x] to submit your guess
  Good luck!
```

The idea behind the challenge is simple discrete logarithm, while the group is given as an oracle. The elements are encoded as random words, and a player have access to a group operation and an element inverse operation. In this setting the lower bound for discrete logarithm is asymptotically equal to **sqrt(p)** operations (p is order of the group and is a prime), because you can't exploit encoding properties of the elements like in index calculus method (as there are no properties at all).

Since the group size couldn't be too large, players could simply guess the answer. So the server was 'cheating': it moved the secret while the group rules were not broken.

The intended way to solve this was to use Baby Step Giant Step algorithm (which is based just on the meet-in-the-middle technique). First, we need to estimate the group order. One can make a dozen of random guesses and see that the order should be just a bit larger than 30000. One can guess that it's 31337 (and confirm with a bunch of mix operations) or make a table of first 100 elements and then try to compute powers in range(30000, 35000, 100) until one matches (you can use fast exponentiation here for power).

For classic BSGS you need `2 * sqrt(31337) = 2 * 177 = 354` operations, but only 251 requests are allowed. Easy to notice that **inverse** oracle doesn't count:

```
mix jefferson jefferson
bessemer (250 questions left)
inv bessemer
sally (250 questions left)
inv sally
bessemer (250 questions left)
mix sally bessemer
postcards (249 questions left)
```

So in the first step of BSGS we can make table of the same size with twice fewer operations — just inverse each element of the table. But `177/2 + 177 = 265` is still too much! Can we use the same trick for the second step of BSGS? No, because if some element falls in our table, it's inverse falls too! (that's how our table is constructed). E.g. you gain no profit of computing inverses in the second stage.

So what do we have? We need to minimize `x + y` (x — number of operations in the first stage, y — number of operations in the second stage), while we need to cover the whole group: `(2x + 2)y >= 31337` (`2x+2` means that we already know two values — g and inv(g) and we gain two table items for one **mix** request.

Let's check for some good values for x:

```
for x in range(100, 150):
    print x, x + math.ceil(31337 / (2*x + 2))
100 255.0
101 254.0
102 254.0
103 253.0
104 253.0
105 252.0
106 252.0
107 252.0
108 251.0
109 251.0
```

```
110 251.0
111 250.0
112 250.0
113 250.0
114 250.0
115 250.0
116 249.0
117 249.0
118 249.0
119 249.0
120 249.0
121 249.0
122 249.0
123 249.0
124 249.0
125 249.0
126 249.0
127 249.0
128 249.0
129 249.0
130 249.0
131 249.0
132 249.0
133 249.0
134 250.0
135 250.0
136 250.0
137 250.0
138 250.0
139 250.0
140 251.0
141 251.0
142 251.0
143 251.0
144 252.0
145 252.0
146 252.0
147 252.0
148 253.0
149 253.0
```

Seems the minimum is 249 operations (and anything between 116 and 133 works)! But wait, we haven't counted one operation of doubling our "giant step" — we need it because we have larger table). So, we can do it in 250 operations!

Bugs

That was the intended solution, but there was a flaw: when you make a request with a word from dictionary, which was not given to you in current session, it was binded to the first free number: 0, 2, 3, … (1 is given to you already). So you can ask an inverses of words from dictionary and they'll get freezed. Using 31337/2 inverse operations you could guess the number with 0 mix oracles :)

Some teams used this partially: you can make a table of any size without using mix oracles.

I allowed using non-given words because it seems logical — for a group you should be able to pick any random element. But they should really be frozen to random elements, or otherwise picking new word should be counted as oracle request too.

Implementation

A few notes about how it was implemented:

For any group, where we are looking only at powers of some generator, we can switch to the group of indexes (powers of the generator) which is just additive group mod N. So actually “discrete logarithm” can be treated as finding **v/g** in additive group (or even finding **v**, because `g=1`). But since you can’t apply extended gcd as usual (which bases on a properties of element encoding), this is not easier to compute, but is easier to think as.

The game (G, V) contains two tables, matching words with numbers.

The first table hold elements which don’t depend on V (therefore are fixed (frozen) and can’t be moved). This elements could be computed as G + G, G — G, 2G + 4G, etc.

The second table hold elements dependent on V, with coefficients of V: xV + yG –> (x, y), e.g. V + V + G –> (2, 1).

It’s now easy to compute all operations — convert both operands to xV + yG form and compute the result in this form. Then decide where to store the result — in the first table or in the second.

V is binded to some value while the second table is not intersecting the first. When they intersect, new value for V is searched. If player is good enough, there can be no good place for V and then it’s frozen forever.

Sources

server.py
game.py (with solution)

Tags: 2014, BSGS, crypto, ctf, discrete logarithm, guess, interactive, mitm, olympic, oracle, python, sha1, writeup

2 comments

1.

   rockosov **says:**

   February 11, 2014 at 11:37 (UTC 3)

   Reply

   Nice crypto guess task! :)

2.

***bowknotbowknot* says:**

December 17, 2015 at 22:27 (UTC 3)

Reply

moves through); what's more , sits with the outer wall with the rectum.
Disorders of this particular prostate
Amyloid
Normally influencing men who ? re more more mature in age group, Amyloid (known mainly because Corpora amylacea) can be described as dense collecting calcified required protein based matter that collects inside the prostates ducts defining it as difficult to your prostate to liberate fluid.
Effortlessly can moreover mean you can find other underpinning issues while in the prostate region.
Prostatitis
Prostatitis is a lot of inflammation on the prostate, in the future the inflammation helps make the prostate swell in proportions causing the tubes using urine to turn into blocked making it feel like difficult and even painful to be able to urinate, if urination is attainable at most of.
Cancerous prostatic hyperplasia
Almost like Prosta moves through); what's more , sits with the outer wall with the rectum.

Disorders of this particular prostate

Amyloid

Normally influencing men who ? re more more mature in age group, Amyloid (known mainly because Corpora amylacea) can be described as dense collecting calcified required protein based matter that collects inside the prostates ducts defining it as difficult to your prostate to liberate fluid.

Effortlessly can moreover mean you can find other underpinning issues while in the prostate region.

Prostatitis

Prostatitis is a lot of inflammation on the prostate, in the future the inflammation helps make the prostate swell in proportions causing the tubes using urine to turn into blocked making it feel like difficult and even painful to be able to urinate, if urination is attainable at most of.

Cancerous prostatic hyperplasia

Almost like Prostatis, Benign prostatic hyperplasia will be name provided for a condition where prostate will get enlarged, there's nothing caused as a result of inflammation but is a really natural occurrence eventually and mostly affects any older mens population.

Effortlessly can hinder the urinary pontoons or quit urination simply being possible overall.

Prostate cancer

If you want to possess prostate cancer tumor information is crucial to you if you happen to male and over 50.Prostate cancer certainly is the most dangerous of most prostate problems and it's factors behind cancer hitting older guys.Prostate cancer is furthermore a condition that will kill without difficulty; this happens because the malignant cells survive and multiple rampant, moving towards other system of the body just like the bones and additionally nearby internal tissue.

Factors behind symptoms with prostate tumors are which it can damage in the fewer abdominal section during urination, difficulty urinating together with cause less ability to get an lovemaking.There are a great many other symptoms needed for prostate cancer malignancy, but they are simply more slight.

Summary

It happens to be commonly recommended that men in which are more mature in age needs to have regular rectal exams from them doctor so that the prostate will be checked.Beforehand earlier, the prostate sits with outer wall for the rectum.

For people who are smaller in age it can be vital that they're just educated within the affects that prostate is wearing the physique.If we're able to educate younger generation it's going to mean which will greater concentration is presented to finding a remedy and ensure it is easier for the purpose of men to give up suffering alone.

Leave a Reply

Your email address will not be published.

Message:

You may use these HTML tags and attributes: `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <em> <i> <q cite=""> <s> <strike> <strong>`

Name:

Email:

Website:

Submit Comment

Submit Comment

Archives

- March 2017 (3)
- October 2016 (6)
- September 2016 (3)
- May 2016 (5)
- April 2016 (2)
- March 2016 (5)
- September 2015 (2)
- May 2015 (4)
- April 2014 (4)
- March 2014 (1)
- February 2014 (4)
- January 2014 (2)
- December 2013 (1)
- October 2013 (1)
- June 2013 (6)
- April 2013 (1)
- February 2013 (2)
- November 2012 (6)
- October 2012 (7)
- May 2012 (6)
- April 2012 (2)
- March 2012 (4)
- February 2012 (17)
- January 2012 (12)
- December 2011 (6)
- October 2011 (5)
- September 2011 (10)
- August 2011 (8)
- July 2011 (3)
- June 2011 (5)
- April 2011 (10)
- March 2011 (7)
- January 2011 (2)
- December 2010 (1)
- November 2010 (1)
- October 2010 (11)
- September 2010 (11)

Meta

- Register
- Log in

- Entries RSS
- Comments RSS
- WordPress.org

Tags

2010 2011 2012 2013 2014 2016 aes aslr binary bruteforce c++ codegate crt crypto ctf defcon exploit exploitation formatstring gits hack.lu hacklu hash ictf leetmore libnum nuit du hack nx pctf plaid plaidctf ppp python quals reverse reversing rop rsa sage shellcode vm web writeup x64 xor

Valid XHTML 1.0 Strict Valid CSS Level 2.1

More Smoked Leet Chicken uses Graphene theme by Syahir Hakim.