Results 1 to 10 of 23

THREAD:
DOES ANYONE KNOW ANY MODULUS ATTACKS IN RSA?

05-07-2011, 04:15 PM #1

trurl_
Registered User

Join Date: Dec 2004
Posts: 133

DOES ANYONE KNOW ANY MODULUS ATTACKS IN RSA?

Another one of my dumb ideas. I am in a cryptography class, just trying to figure out how this one way function works and find if there are any attacks against the modulus. If you know any modulus attacks please share.

This idea isn't tested but I am just trying to learn why these one way functions such as RSA are computational difficult. I now even computers have trouble factoring large digits of 64-digits or more. But maybe RSA weakness is in the modulus operation.

Say we have "P" the product of 2 Prime numbers which are so large they are unknown. Could we take a larger number than P and call this large number "L". We search to find all numbers where P mod L = 0. But we do not have to search all numbers because we know where L = 0 is a multiple of P. So you have P^2 ; P^3 ; P^4...P^n .

Now what? This is where the computer comes in to test the fraction made by

P / larger number

Example
15 is the multiple of the two smallest Prime numbers: 3 and 5.
15 / 30 = ½
15 / 45 = 1/3

15 * 1/3 = 5
We test to see if 5 is Prime then we know 15 = 3 * 5.

This is untested for all numbers and probably doesn't work. It just helps me understand the one way function and public key cryptography. I still need to do more analysis, but this idea may have already been tried before. I am ignorant of the attacks on RSA.

20110506---Bobby Joe Snyder
www.constructorscorner.net

Blog this Post | Edit Post | Reply | Reply With Quote

05-08-2011, 07:48 AM #2

ComicSansMS
Most Horrible Font Ever

Join Date: Jun 2003
Location: Trier, Germany
Posts: 1,328

first of all your thread title is completely misleading. you're talking about the modulo operation (i.e. calculating the remainder of a division) which is something *completely* different than modulus, which is also a term in number theory. please choose your wording more carefully.

second your approach makes absolutely no sense. what you need to find is a factorization. currently you're just accumulating wild numbers. even if your algorithm *did* find a factorization, it would not be more efficient than the widely known exponential-complexity factorization algorithms, as you're just using a simple sieve approach which does not scale here.
actually this is the very essence why rsa works in the first place. if you plan to pass that cryptography class of yours, i'd recommend you take a closer look at the rationale behind this method before moving on

A Pageant of the Bizarre

Blog this Post | Reply | Reply With Quote

05-09-2011, 04:30 PM #3

trurl_
Registered User

Join Date: Dec 2004
Posts: 133

Ok. I am proposing to use only the numbers that are whole to factor. If it does not equal a whole number there is no reason to use it. Would this be any faster than factoring. You would only need to divide once for the decimal numbers and factor only the whole numbers. Is there any advantage to this?

I realize I cannot break a one way function, but can I choose the best chance of a Prime number factor based on whole numbers from the modulus.

I could be putting myself in an endless loop. But I think this is so simple it may be useful.

Here is an updated work I tried to make more clear:

This idea isn't tested but I am just trying to learn why these one way functions such as RSA are computational difficult. I now even computers have trouble factoring large digits of 64-digits or more. But maybe RSA weakness is in the modulus operation.

Say we have "P" the product of 2 Prime numbers which are so large they are unknown. Could we take a larger number than P and call this large number "L". We search to find all numbers where P mod L = 0. But we do not have to search all numbers because we know where L = 0 is a multiple of P. So you have P*2 ; P*3 ; P*4...P*n .

Now what? This is where the computer comes in to test the fraction made by

P / larger number

Example: (This is a simple example to show process. It does not prove anything.)
15 is the multiple of the two smallest Prime numbers: 3 and 5.
15 / 30 = ½
15 / 45 = 1/3

15 * 1/3 = 5

We test to see if 5 is Prime then we know 15 = 3 * 5.

This is untested for all numbers and probably doesn't work. It just helps me understand the one way function and public key cryptography. I still need to do more analysis, but this idea may have already been tried before. I am ignorant of the attacks on RSA.

20110506---Bobby Joe Snyder
www.constructorscorner.net

Also note I realize dividing by a multiple of P is the same as dividing by 1,2,3,4...

However there is an advantage to what I am trying to show. (Even if it is not very clear or easy.)

I am looking for the occurrence when 1/ (L * P) = a whole number.

This helps because the majority of the divisions equal decimal numbers.

Also important is 1 / (P*L). This number approaches zero when L becomes larger. But the advantage is that inverse of the division will equal the number that is its product. Most likely not the Prime numbers' product; However there may be a pattern in how the numbers progress to a number. Similar to how a value is approaches to a value in differential calculus. Also, the Prime multiples cannot be bigger than then 1 / (1/n). This may be nothing new. I am just trying to better understand RSA and its algorithm.

Example:
5 * 17= 85
1 / (85*5) = 425 which is a whole number
85 / 425 = 0.2
0.2 * 85 = 17
85 / 17 = 5

Is this any more clear what I am saying? I have an idea I just can't get it into words.

Blog this Post | Edit Post | Reply | Reply With Quote

trurl_
Registered User

Join Date: Dec 2004
Posts: 133

SIMPLE ARITHMETIC TO CLARIFY THE IDEA.

Here is the idea in simple arithmetic.

1 / (1 / (85 * 2) = 169.99999999999999999999999992 --- not a whole number (decimal number)
1 / (1 / (85 * 3) = 254.99999999999999999999999987 --- decimal
1 / (1 / (85 * 4) = 340.00000000000000000000000041 --- almost not, but still decimal; might have to test by dividing 85 by this number
1 / (1 / (85 * 5) = 424.99999999999999999999999979
Divide 85/524 = .2
.2 * 85 = 17

The product 85 was formed by multiplying 2 Prime numbers: 5 * 17.

1 / (1 / (85 * 6) = 509.99999999999999999999999975 --- must test
85 / 509.99999999999999999999999975 = 0.16666666666666666666666666666675

85 * 0.16666666666666666666666666666675 = 14.16666666 not a whole number

---

It's all about ideas.

constructorscorner.com

Blog this Post | Edit Post | Reply | Reply With Quote

05-10-2011, 11:45 AM #5

ComicSansMS
Most Horrible Font Ever

Join Date: Jun 2003
Location: Trier, Germany
Posts: 1,328

> Originally Posted by **trurl_**
> *1 / (1 / (85 * 2) = 169.99999999999999999999999992 --- not a whole number (decimal number)*
> *1 / (1 / (85 * 3) = 254.99999999999999999999999987 --- decimal*
> *1 / (1 / (85 * 4) = 340.00000000000000000000000041 --- almost not, but still decimal; might have to*

okay, this starts getting bizarre.

1 / (1 / 85*3) = 85*3 which of course is a whole number. obviously you didn't do your homework on floating point representations. read this.

then read my first post again. sieving will *not* help you here! google some basic factorization algorithms if you don't believe me. you will always end up with exponential runtime when using this approach.

A Pageant of the Bizarre

Blog this Post | Reply | Reply With Quote

05-10-2011, 02:09 PM #6

Overmind1984
aka Overkitty

Join Date: Sep 2004
Location: Mesa, Arizona
Posts: 421

> Originally Posted by **ComicSansMS**
> *first of all your thread title is completely misleading. you're talking about the modulo operation (i.e. calculating the remainder of a division) which is something *completely* different than modulus, which is also a term in number theory. please choose your wording more carefully.*

This is just nit picking but modulus and modulo are correct terms for both. Some languages call this operation modulus and some call it modulo. Like wise, modulo is also a term seen regularly in the number theory definition of modulus. So it's not really a fail of usage but a fail of the language itself.

"You don't stop laughing because you grow old. You grow old because you stop laughing."

Blog this Post | Reply | Reply With Quote

05-10-2011, 03:53 PM #7

Join Date: Jun 2003

ComicSansMS
Most Horrible Font Ever

Location: Trier, Germany
Posts: 1,328

> Originally Posted by **Overmind1984**
> *This is just nit picking but modulus and modulo are correct terms for both. Some languages call this operation modulus and some call it modulo. Like wise, modulo is also a term seen regularly in the number theory definition of modulus. So it's not really a fail of usage but a fail of the language itself.*

seems you're right here. in german the distinction between the two is more strict, which is why i got confused initially. thanks for clearing things up

A Pageant of the Bizarre

Blog this Post | Reply | Reply With Quote

05-10-2011, 05:23 PM #8

trurl_
Registered User

Join Date: Dec 2004
Posts: 133

This problem seems like plain stupidity. But it didn't start out that way. I started from the concept and then went to the calculator. Then I used the Windows calculator which gave me those results.

You are right, I goofed. I can factor, but does it offer any advantage of just dividing by 2,3,4,5...n?

Try:

1 / 85 * 3 = 0.035294 removed parenthesis

1 / 0.035294 = 28.3333 = 85 / 3

1 / 85 * 5 = 0.058824

1 / 0.058824 = 17 = 85 / 5

Perhaps it would help to eliminate choices of factors of large numbers or have a pattern in the calculation.

It's all about ideas.

constructorscorner.com

Blog this Post | Edit Post | Reply | Reply With Quote

05-28-2011, 02:56 AM #9

trurl_
Registered User

Join Date: Dec 2004
Posts: 133

The multiple of 2 "unknown" Prime numbers:
85 = 5 * 17

1/(85 * 3) = 1/(0.0039215) = 255

255/(85 / 3) = 255/(28.333333) = 9

Sqrt[9] = 3

1/(85 * 5) = 1/(0.00235) = 425

425/(85 / 5) = 425/(17) = 25

Sqrt[25] = 5

```
17^2 = 289
425 - 289 = 136
136 / 17 = 8

17 / 8 = 2.125
1/2.125 = 0.470588

0.470588 * 136 = 64
Sqrt[64] = 8

8/0.125 = 64

Sqrt[64] = 8
```

These are just some interesting relationships I found in between doing class work. I do not know of any equation that finds whole numbers faster than division.The benefit is to find where the mod equals zero.These relationships can be subtracted to each other and set to zero in an attempt to find some meaningful equation.

www.constructorscorner.net
20110527

It's all about ideas.

constructorscorner.com

Blog this Post | Edit Post | Reply | Reply With Quote

01-27-2012, 12:57 AM #10

trurl_
Registered User

Join Date: Dec 2004
Posts: 133

By now you are tired of my attempts to solve a one way function. It is just something I do when I get bored.

I put a lot of thought into this one. It is not the solution, but a mental exercise. I can think of the trigonometric definition I would use and that is similiar triangles since we know why in terms of x we can set x and y as variables and solve for x. It wouldn't be pretty and we might not be able to solve the polynomial. But instead of factoring you could plug x in and see if it equaled the product of 2 Prime numbers.

Again with such an impossible problem it is more of a mental exercise then a solution.

http://www.constructorscorner.net/id...stitution.html

It's all about ideas.

constructorscorner.com

Blog this Post | Edit Post | Reply | Reply With Quote

+ Reply to Thread

Page 1 of 3 1 2 3 Last

QUICK REPLY

Font Size

Show your signature

Post Quick Reply | Go Advanced | Cancel

« Previous Thread | Next Thread »

TAGS FOR THIS THREAD

None
View Tag Cloud

Add / Edit Tags

POSTING PERMISSIONS

You may post new threads
You may post replies
You may post attachments
You may edit your posts

BB code is On
Smilies are On
[IMG] code is On
[VIDEO] code is On
HTML code is Off

Forum Rules

All times are in GMT 0