

Re: $a^{(b^x)} \bmod n$?

Source: <http://sci.tech-archive.net/Archive/sci.math/2005-06/msg04005.html>

- *From:* Gerry Myerson <gerry@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 23 Jun 2005 10:09:52 +1000
-

In article <1119476893.618583.126570@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>, "Pubkeybreaker" <Robert_silverman@xxxxxxxxxxxx> wrote:

> Jean-Claude Arbaut wrote:
>> On 22/06/2005 14:11, fredsaf_20055@xxxxxxxx wrote:
>>
>>> Given positive integers a,b,x,n is it possible to efficiently compute:
>>>
>>> $a^{(b^x)} \bmod n$?
>>>
>>> $\phi(n)$ is unknown and b^x is so large it can't be used directly.
>>>
>>> Or is it known this to be a hard problem?
>>>
>>> Thanks.
>>
>> If b^x is manageable, it's easy by "fast exponentiation".
>>
>> By manageable, I mean up to 10000 figures, for example.
>
> And even if b is unmanageable!!
> Hint: Think "Lagrange's Theorem".
> Further Hint: Think about $b^x \bmod \phi(n)$

How do you think about $b^x \bmod \phi(n)$ when, as OP says above, $\phi(n)$ is unknown? Presumably n is something like an RSA key, and computing $\phi(n)$ is infeasible.

—

Gerry Myerson (gerry@xxxxxxxxxxxxxxxx) (i -> u for email)

.

- *References:*
 - ◆ $a^{(b^x)} \bmod n$?
◇ *From:* fredsaf_20055
 - ◆ Re: $a^{(b^x)} \bmod n$?
◇ *From:* Jean-Claude Arbaut

Re: $a^{(b^x)} \bmod n$?

◆ **Re: $a^{(b^x)} \bmod n$?**

◇ From: Pubkeybreaker

- Prev by Date: **Re: IMPORTANT Re: Zero digits in powers**
- Next by Date: **Re: IMPORTANT Re: Zero digits in powers**
- Previous by thread: **Re: $a^{(b^x)} \bmod n$?**
- Next by thread: **Re: $a^{(b^x)} \bmod n$?**
- Index(es):
 - ◆ **Date**
 - ◆ **Thread**