

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

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2005-06/msg03877.html>

---

- *From:* Jean-Claude Arbaut <[jean-claude.arbaut@xxxxxxxxxxx](mailto:jean-claude.arbaut@xxxxxxxxxxx)>
  - *Date:* Wed, 22 Jun 2005 14:24:24 +0200
- 

On 22/06/2005 14:11, fredsaf\_20055@xxxxxxxxxxx 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.

The trick is writing  $p=b^x$  in binary.

Example:

$p = 3 = 11(2)$ , then  $a^p = a^2 * a$  you

$p = 5 = 101(2)$ , then  $a^p = (a^2)^2 * a$

Full algo:

```
r := 1
m := a mod n
while p > 0
  if p mod 2 = 1 then r := m * r mod n
  m := m * m mod n
  p := p div 2
wend
```

Only need roughly  $O(\lg(p))$  multiplications.

- *Follow-Ups:*
  - ◆ [Re:  \$a^{\(b^x\)} \bmod n\$ ?](#)
    - ◇ *From:* Pubkeybreaker
- *References:*
  - ◆ [a^{\(b^x\)} mod n?](#)
    - ◇ *From:* fredsaf\_20055
- Prev by Date: [Re: Logic in Schools](#)
- Next by Date: [Re: Longest day of year?](#)
- Previous by thread: [a^{\(b^x\)} mod n?](#)
- Next by thread: [Re: a^{\(b^x\)} mod n?](#)
- Index(es):
  - ◆ [Date](#)
  - ◆ [Thread](#)