

Re: Modulo exponentiation 2 bits at a time.

Source: <http://sci.tech-archive.net/Archive/sci.math/2007-05/msg00111.html>

- *From:* Phil Carmody <thefatphil_demunged@xxxxxxxxxxxx>
 - *Date:* 01 May 2007 20:59:19 +0300
-

fabrice.gautier@xxxxxxxxxx writes:

Hi,

I'm looking for reference on a modulo exponentiation algorithm that use 2 bits of the exponent at each loop instead of the simplest algorithm that just use 1 bit for each loop.

To make things clearer , calculating $q=c^e \pmod m$

The loop in the simplest algo is something like:

```
{
q=q*q (mod m);
if (e[i]) q=q*c (mod m);
}
```

The other algo loop is something like

```
{
```

```
q=q*q;
q=q*q;
if(e[i]e[i+1])
{
```

```
q=q*C[e[i], e[i+1]] ;
```

```
}
```

```
}
```

where C's 4 elements are precalculated.

Re: Modulo exponentiation 2 bits at a time.

Add 'window' to your google search.

If your search doesn't find /HAC/, then repeat until it does.

Phil

—

"Home taping is killing big business profits. We left this side blank so you can help." — Dead Kennedys, written upon the B-side of tapes of /In God We Trust, Inc./.

.