

## Question from an intelligent (?) layman

---

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-11/msg01008.html>

---

- *From:* "Al" <[alanpeg@xxxxxxxxxx](mailto:alanpeg@xxxxxxxxxx)>
  - *Date:* 23 Nov 2006 11:54:32 -0800
- 

I understand that one element of cryptography is to publish a large number that is the product of two primes. It is believed impossible to factor that number (call it N). But can't one make a table of products of pimes and just compare the key with values in the table? For example take the primes 2, 3, 5, and 7:

N Primes

-----  
6 2\*3  
10 2\*5  
14 2\*7  
15 3\*5  
21 3\*7  
35 5\*7

Now if  $N = 21$ , one goes to the table and reads off the answer ( $3 \cdot 7$ ). Is this wrong or am I missing something? I will appreciate any comments.

Al Rosenfield  
Columbus OH

.