

$$N = pq$$

$$N = pq$$

Factoring is slow. Greatest common divisor is *fast*.

Can we find a number K where $\gcd(N, K) = p$, given only N ?

$$x^2 \equiv y^2 \pmod{N}$$

$$x^2 \equiv y^2 \pmod{N}$$

We're going to ban trivial solutions where $x = 0$, $y = 0$, or $x = \pm y$.

$$x^2 \equiv y^2 \pmod{N}$$

$$x^2 - y^2 \equiv 0 \pmod{N}$$

Congruence to 0 implies that N *divides* the difference of x and y squared ($x^2 - y^2$), meaning the difference is a multiple of N .

$$N \mid (x^2 - y^2)$$

$$x^2 - y^2 \equiv 0 \pmod{N}$$

$$(x - y)(x + y) \equiv 0 \pmod{N}$$

We know $N \nmid (x - y)$ and $N \nmid (x + y)$ because we banned $x \equiv \pm y \pmod{N}$.

$$N \mid (x - y)(x + y)$$

$$\gcd(N, x - y)$$

N only has two prime factors, p and q . Neither $x - y$ nor $x + y$ can have **both** p and q as factors because $N \nmid (x - y)$ and $N \nmid (x + y)$. So one of p or q divides $x - y$ and the other divides $x + y$.

Let's pretend I can take discrete logs mod N quickly.
Can I turn this into factors?

$$a^r \equiv 1 \pmod{N}$$

Select a random $1 < a < N$. Solve for r using our magical discrete log solver.

r is the order of a .

$$a^r \equiv 1 \pmod{N}$$

$$a^r - 1 \equiv 0 \pmod{N}$$

Look familiar?

$$a^r - 1 \equiv 0 \pmod{N}$$

$$(a^{r/2} - 1)(a^{r/2} + 1) \equiv 0 \pmod{N}$$

If r isn't even, then pick a different a .

$$\gcd(a^{r/2} - 1, N)$$

Once again, we separated p and q into a difference of two squares and gcd reveals the factor.