

# RSA Key Generation Trouble [Heninger et al./Lenstra et al.]

OpenSSL RSA key generation (abstract):

```
prng.seed(seed)
p = prng.generate_random_prime()
prng.add_randomness(bits)
q = prng.generate_random_prime()
N = p*q
```

Suppose poor entropy at startup:

- Same  $p$  will be generated by multiple devices, but different  $q$
- $N_1, N_2$  : RSA keys from different devices  $\Rightarrow \gcd(N_1, N_2) = p$