Security of RSA:

If Eve can factor large numbers very quickly and consistently, then Eve can break RSA.

Proof: Eve can simply factor $n = pq$.

(Eve knows: (n, e) public key. c the cipher text)

$c = m^e \pmod n$

Eve can compute the decryption exponent

$$d \equiv e^{-1} \pmod{\phi(n)} = e^{-1} \pmod{(p-1)(q-1)}.$$

Eve can recover m by computing $c^d \pmod n$.

Ideally, we want to claim:

"If Eve can break RSA consistently, then Eve can factor large numbers consistently."

(This is an open question.)

RSA Challenge: (Chapter 6.5 of the textbook.)

Claim: If Eve has access to both $n = pq$ and $\phi(n)$ then Eve can factor n.

(A more complicated argument shows that if Eve knows d, then she can factor n.)

Proof: Eve knows n, Eve knows $\phi(n)$ $\Longrightarrow$ $\begin{cases} p \cdot q = n \\ p + q = n - \phi(n) + 1. \end{cases}$

Eve can solve the quadratic equation

$$x^2 - (n - \phi(n) + 1)x + n = 0.$$

The two roots of this equation are p and q.

* : We do not know how to factor large numbers quickly.

(Chapter 6.2 of textbook covers attacks on RSA.)

e.g. if p is too close to q, then RSA is not secure.

if e is too small, then RSA is not secure.

Timing attacks.

Primality Testing

Lemma: Let n be an integer.

If $\exists x, y$ s.t $x^2 \equiv y^2 \pmod n$ and $x \not\equiv \pm y \pmod n$

Then n is not a prime,

Moreover $\gcd(x-y, n)$ is a non-trivial factor of n.

Proof: $x^2 - y^2 \equiv (x+y)(x-y) \equiv 0 \pmod n$. Let $d = \gcd(x-y, n)$.

If $d = n$, then $x \equiv y \pmod n$. ✗

If $d = 1$, then $(x+y)(x-y) \equiv 0 \pmod n \Longrightarrow x \equiv -y \pmod n$. ✗

Otherwise d is a non-trivial factor of n.

Example: $12^2 \equiv 2^2 \pmod{35}$. but $12 \not\equiv \pm 2 \pmod{35}$.

$\gcd(12-2, 35) = 5$ is a factor of 35.

Example: In RSA, $n = pq$.

- Eve can test if $n+1, n+4, n+9, \ldots$ are perfect squares.
  If Eve succeeds, this allows her to factor n.
- This is because (w.l.o.g assume both p and q are odd.)

$$p \cdot q + \left(\frac{|p-q|}{2}\right)^2 = \left(\frac{p+q}{2}\right)^2. \iff 4pq + (p-q)^2 = (p+q)^2$$

  So Eve only need to try $\frac{|p-q|}{2}$ steps.
- Therefore, it is important to pick p, q where $|p-q|$ is not too small.