RSA cryptography

**Sender**

```
msg
k, m
ensure 0 \leq msg < m
hope [msg]_m is a unit
\checkmark c := [msg^k]_m
```

**Network (attacker)**

```
\text{public key: } k, m
\longleftarrow
\text{cyphertext: } c
```

**Recipient**

```
\checkmark
choose p and q, large primes
compute m := pq
compute \varphi(m) = (p - 1)(q - 1)
choose a unit [k]_{\varphi(m)}
compute [k]^{-1}_{\varphi(m)} using \varphi(m)
```

```
c^{[k]^{-1}_{\varphi(m)}} = [msg][k][k]^{-1} = [msg]_m
```
Fast exponentiation

For large $a^k$, write $k$ as a sum of powers of 2:

$$a^k = (a \cdot a) (a \cdot a) \cdots (a \cdot a) \text{ k times}$$

For example:

$$3^{23} = \left(3^{16} \cdot 3^4 \cdot 3^2 \cdot 3^4\right)_{10} = \left(3^{16} \cdot 3^4 \cdot 3^2 \cdot 3^4\right)_{10}$$

$$23 = 1 + 2 + 4 + 16$$

$$[3^{23}]_{10} = [3^{16}]_{10} \cdot [3^4]_{10} \cdot [3^2]_{10} \cdot [3^4]_{10} = [1] \cdot [1] \cdot [9] \cdot [3]$$

$$2^{3^2} = 2^{9} = 2^6 \cdot 2^3$$

$$3^8 = 3^4 \cdot 3^4 = [1] \cdot [1] = [2]$$

$$3^{16} = 3^8 \cdot 3^8 = [1] \cdot [1] = [2]$$

$$23 = 1 \cdot 16 + 1 \cdot 4 + 1 \cdot 2 + 1 \cdot 1$$

$$0^8 + (10111)_2$$
Selecting large primes

Fact: There are lots of prime numbers; they are well spread out.

To find a large prime:
- Choose a large odd number.
- Check to see if prime.
- If not, add 2, check again, repeat.
- Probabilistic test (beyond scope of course).

To choose \([k \alpha_{\text{mod}} (a \text{ unit})]\):
- Try \(k = 7\), compute \(\gcd(k, q(n))\).
- If \(1\): done
- Otherwise, try a different prime (e.g., 17).
Factoring is (probably) hard

To factor $m$,
check $2 | m$ ?
check $3 | m$ ?
check $5 | m$
check $7 | m$
check $11 | m$

try all primes $\leq \sqrt{m}$

out at least one factor $\leq \sqrt{m}$

if $m$ has 1000 (1k) digits

then $\sqrt{m}$ has 500 digits ($k/2$)

try $\sim 10^{500}$ #s.

grows exponentially in # digits of $m$... Too hard!