- Groups of prime order
- Groups of unknown composite order.

\[ \mathbb{Z}_n^x \text{ is group of } \]  
\[ \text{numbers mod } n, \text{ under mult } \]  
\[ \text{relatively prime w/ } n \]  
\[ \sim \varphi(n) \text{ # of numbers relatively to } n. \]

Euler's Totient

Suppose \( n = pq \), \( p \) and \( q \) are distinct primes.

What's \( \varphi(pq) = \) \( \varphi(p) \cdot \varphi(q) \)?

\[ \varphi(p) = \frac{p^1 - 1}{p - 1} \]  
\[ \varphi(q) = \frac{q^1 - 1}{q - 1} \]  
\[ \frac{pq - 1}{pq - 1} - \frac{(q - 1)}{(q - 1)} - \frac{(p - 1)}{(p - 1)} \]  
\[ \frac{pq - 1 - q + 1 - p + 1}{pq - 1} = (p - 1)(q - 1) = \varphi(p) \cdot \varphi(q) \]

**Factoring Assumption:**
Given \( n = pq \), where \( p \) and \( q \) are large primes, it's hard to find \( p \) or \( q \).
- Given a number $X$ that is a common factor of $n$, i.e. $\gcd(x, n) \neq 1 \implies \gcd(x, n) \implies \text{factor of } n$.

**Facts about finding primes:**

- We have algo for checking if a number is prime.
  - AKS deterministic polynomial but bad constants.
  - Miller-Rabin randomized
    $\Rightarrow$ shows a number is prime w/o finding the factors.

**Prime Number Theorem.**

Density: $\pi(n)$ # of primes less than $n$.

$$\pi(n) \sim \frac{n}{\log n} \quad \lim_{n \to \infty} \frac{\pi(n)}{\frac{n}{\log n}} = 1$$

- Asymptotic $\pi(n) \gg \frac{n}{\log n} \gg \frac{n}{\log_2 n}$

- $X \in [2^{a-1}, 2^a]$

$$\Pr[X \text{ is prime}] \geq rac{1}{\sqrt{\pi}} \frac{2^a - 2^{a-1}}{2^a}$$

$$\mathcal{O}(2^a) \frac{1}{\sqrt{\pi}}$$

- Sample $2^a$:

$$x \in [2^{a-1}, 2^a]$$

check if $X$ is prime.

repeat-alternate.

Concludes after $\mathcal{O}(2)$ trials expectation.

RSA: PKC
\[ \text{Gen}(k): \quad \text{Sample } p, q \text{ large primes, public moduli } n = p \cdot q \]

\[ \Phi(n) = \frac{(p-1)(q-1)}{e, d} \quad \text{are chosen so that } e \cdot d = 1 \mod \Phi(n) \]

1st secret exponent. 2nd secret exponent.

\[ e \text{ is typically fixed } e = 3, \quad d \text{ fixed by these mod } \Phi(n) \]

\[ \text{Enc}(pk, m): \quad \sigma_k = (p, q, d) \]

\[ \rho_k = (n, e) \]

\[ c = m^e \mod n \]

\[ \text{Dec}(sk, c): \]

\[ m' = c^d \]

**Correctness:**

\[ m' = (m^e)^d \mod n \]

\[ = m^{e \cdot d} \mod n \]

\[ = m^{\ln m \cdot k + 1} \mod n \]

\[ = m \]

Security relies on RSA assumption.

RSA hard \implies\ Factoring is hard.

\[ \Rightarrow \text{RSA-UFo} \]

\[ \text{For all } n = pq, \text{ is } \phi(n) \text{ feasible?} \]

\[ e = 3 \text{ possible?} \]
\( n \neq 7, \frac{5}{4} \)
\( q(n) = 6 \cdot 4 = 2^3 \cdot 3 \)
\( 3 \) has no residue in \( \mathbb{Z}/q(n) \)

RSA Signatures:

\[ \text{Sign}(s, m): \]
\[ d, e, \beta, \alpha \]
\[ \sigma := m^d \mod n. \]

\[ \text{Verify}(\sigma, m, pk): \]
\[ n, e \]
\[ \text{Check } m = \sigma^e \mod n. \]

---

CRT representation
- Speedup in RSA operations
- Fault attacks.

Theorem:
Given primes \( p, q \)
and \( \alpha < p, \beta < q \),
we can find a unique \( X < pq \)
\[ X \equiv a \pmod{p} \]
\[ X \equiv b \pmod{q} \]

\[ X = a + pk \]
\[ X = b + q \] for some
\[ x \equiv (a \mod p) \]

**Proof:** Specifically:

Let \( p^{-1} \) be the inverse of \( p \) in \( \mathbb{Z}_q^\times \),

\[ (p \cdot p^{-1}) \equiv 1 \mod q \]

Same for \( \bar{q}^{-1} \),

\[ (a \cdot \bar{q}^{-1}) \equiv 1 \mod p. \]

Let \( x \equiv a \cdot \bar{q}^{-1} + b \cdot p \cdot p^{-1} \mod pq \).

Show \( x \equiv a \mod p \).

\[
\begin{align*}
x &= a \cdot \bar{q}^{-1} + b \cdot p \cdot p^{-1} \\
   &= a \cdot \bar{q}^{-1} \mod p.
\end{align*}
\]

Same for \( x \equiv b \mod q \).

**Claim:** CRT representation preserves multiplication.

Multiply using CRT, \( x \cdot y \mod pq \).

- Convert to CRT
  \[
  \begin{align*}
    a &= x \mod p \\
    b &= x \mod q \\
    c &= y \mod p \\
    d &= y \mod q.
  \end{align*}
  \]

- \( U = (a \cdot c) \mod p \)
  \( V = (b \cdot d) \mod q \)

By CRT

Solve for \( z \),

\[ z \equiv (a \cdot c) \mod p \]

\[ z \equiv (b \cdot d) \mod q. \]
By claim, \( Z = XY \mod pq \)

In RSA:

Recall

\[
\begin{align*}
    c & \mod n \leftarrow 2^x \\
    \text{square and add,} \\
    2^x \text{ iterations of } 2^x \text{-bit multis.} \\
    \text{mod Multiplying } (2^x) \times (2^x) \text{ operations}
\end{align*}
\]

Instead:

\[
\begin{align*}
    u &= c \mod p \\
    v &= c \mod q \\
    d_p &= d \mod (p-1) \\
    d_q &= d \mod (q-1) \\
    a &= u^d \mod p \\
    b &= v^d \mod q \\
    x &= a \times b \mod n \\
    2^x &\approx \frac{8}{7} \text{ op.}
\end{align*}
\]

Fault attacks

- Some operations are sensitive to mistakes in computing bit flip

Personal computers have ECC in ROM making this unlikely

- Smart cards or embedded devices more susceptible

- Space, cosmic rays no filtering

- Overvoltage, undervoltage

\[
\begin{align*}
    X &\rightarrow \text{Program 1} \rightarrow 0 \rightarrow \text{Program 2}
\end{align*}
\]
Only sign any valid even numbers.

6 = a \mod p \quad 6' = a' \mod p
= b \mod q \quad = b' \mod q

(6-6') = 0 \mod q.

q divides (6-6')

\gcd(n, 6-6') = q \Rightarrow \text{recovery of secret key.}