RSA

Wednesday, November 3, 2021 3:58 PM

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

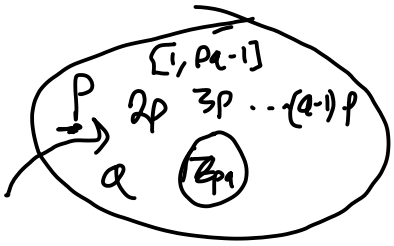
$|\mathbb{Z}_n^\times|$ is group of numbers mod n, under mult, relatively prime w/ n

$\rightsquigarrow \varphi(n)$ # of numbers relatively to n.

Euler's Totient

Suppose $n = pq$, p and q are distinct primes.

Whats $\varphi(pq) =$ not more than $pq-1$



At least $\varphi(p) + \varphi(q)$

$p-1$ $q-1$

w/ common factor to $(p \cdot q)$

w/ p as a factor # q as a factor

$|\mathbb{Z}_{pq}^\times| = pq-1-(q-1)-(p-1)$

- double counting me. ✓
- any others

$= pq-1-q+1-p+1$

$= pq-q-p+1 = (p-1)(q-1)$

$= \varphi(p) \cdot \varphi(q)$

Factoring Assumption:

Given $n = pq$, where

$p \xleftarrow{\$}$ large prime (λ-bit)

$q \xleftarrow{\$}$ large prime

it's hard to find p or q.

- Given a number X that has a common factor to n,
  i.e $p | X$ or $q | X$ ... $\gcd(X, n) \Rightarrow p$ or q.

Facts about finding primes.

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

- Prime Number theorem.

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

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

↑ asymptotic

- Chebyshev $\pi(n) \gg \frac{n}{\log_e n} \gg \frac{n}{\log_2 n}$

- $X \xleftarrow{\$} [2^{\lambda-1}, 2^{\lambda}]$

$\Pr[X \text{ is prime}] \gtrsim 1/\lambda$

$O(2^{\lambda})$ $1/\lambda$

✓ $\frac{2^{\lambda}}{\lambda} - \frac{2^{\lambda-1}}{\lambda-1}$

$1/\lambda$ is Δ is relative to $1/2^{\lambda}$

- Sample(λ):
  $X \xleftarrow{\$} [2^{\lambda-1}, 2^{\lambda}]$
  check if X is prime.
  repeat otherwise.
  Concludes after $O(\lambda)$ trials expectation.

RSA: PKE

Gen():
Sample p, q large primes
$n = pq$ public modulus
$\varphi(n) = (p-1)(q-1)$
e, d are chosen so that $e \cdot d = 1 \bmod \varphi(n)$
e public exponent, d secret exponent.
e is typically fixed $e = 3$.
d found by inverse mod $\varphi(n)$

$sk = (p, q, d)$
$pk = (n, e)$

Enc(pk, m):
$c := m^e \bmod n$

Dec(sk, c):
$m' := c^d$

Correctness:
$$m' = (m^e)^d \bmod n$$
$$= m^{e \cdot d} \bmod n$$
$$= m^{|\mathbb{Z}_n| \cdot k + 1} \bmod n$$
$$= m^1$$

Security relies on RSA assumption.
RSA hard $\Rightarrow$ factoring is hard.

For all $n = pq$, is $p, q > 3$

$e = 3$ feasible:

$n = 7 \cdot 5$,

$\varphi(n) = 6 \cdot 4 = \underline{2^3 \cdot 3}$

3 has no inverse in $\mathbb{Z}_{\varphi(n)}$