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 multi, relatively prime w/ n

$\parallel$

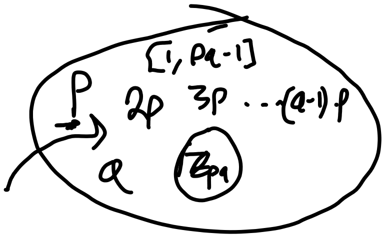
$\rightsquigarrow \varphi(n)$ # of numbers relatively to n.

Euler's Totient

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

What's $\varphi(pq) =$

not more than $pq-1$



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

At least $p \; \underbrace{\varphi(p)}_{p-1} + \underbrace{\varphi(q)}_{q-1}$

$$|\mathbb{Z}_{pq}^{\times}| = pq-1 - \overset{\#\text{ w/ } p \text{ as a factor}}{\left(q-1 \right)} - \overset{\#\text{ } q \text{ as a factor}}{\left(p-1 \right)}$$

- double count? none. ✓
- 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 as a common factor to n,
  i.e $p \mid X$ or $q \mid X$..... $\gcd(X, n) \Rightarrow p$ 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.

$$\underset{\text{asymptotic}}{\pi(n) \sim} \frac{n}{\log n} \qquad \lim_{n \to \infty} \frac{\pi(n) \log n}{n} = 1$$

- Chebyshev $\pi(n) \geq \dfrac{n}{\log_e n} \geq \dfrac{n}{\log_2 n}$

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

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

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

$1/\lambda$ is big 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

$n = p \cdot q$ public modulus

$\varphi(n) = (p-1)(q-1)$

e, d are chosen so that $e \cdot d = 1 \mod \varphi(n)$

pub exponent, secret exponent.

e is typically fixed $e = 3$.

d found by inverse mod $\varphi(n)$

Enc(pk, m):

$$c := m^e \mod n$$

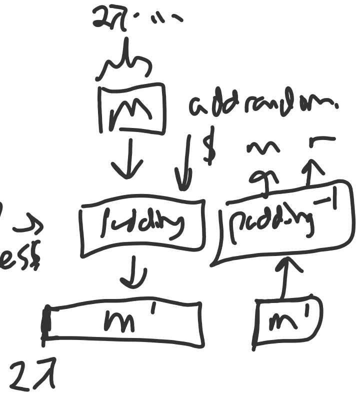
$sk = (p, q, d)$

$pk = (n, e)$

Padding:

RSA-OAEP →

- randomness
- increases size of m.



Dec(sk, c):

$$m' := c^d$$

Correctness:

$$m' = (m^e)^d \mod n$$

$$= m^{e \cdot d} \mod n$$

$$= m^{|\mathbb{Z}_n| \cdot k + 1} \mod n$$

$$= m^1$$

Security relies on RSA assumption.

RSA hard ⇒ factoring is hard.

* RSA-UFO

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

$n = 7 \cdot 5,$

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

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

RSA Signatures:

Sign(sk, m):
sk: d, e, p, q, n

$\sigma := m^d \bmod n.$

Verify($\underline{\sigma}$, m, pk):
pk: n, e

check $m \overset{?}{=} \sigma^e \bmod n$

CRT representation

- Speedup in RSA operations $\underline{4x}$
- Fault attacks.

$$\begin{tikzcd} X & X \arrow[d, Rightarrow] \\ (a,b) \arrow[u, Rightarrow] & \overset{x\%p}{a} \quad \overset{x\%q}{b} \end{tikzcd}$$

$X \% p$

Theorem:

Given primes p, q,
and $a < p$, $b < q$,
we can find a unique $X < pq$

$X \equiv a \pmod p$ $\qquad x = a + pk$

$X \equiv b \pmod q$ $\qquad X = b + qj$ for some

$X \equiv (a \mod p)$

Proof: Specifically:

let $\underline{p^{-1}}$ be the inverse of p in $\mathbb{Z}_q^{\times}$

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

Same for $\underline{q^{-1}}$ $(q \cdot q^{-1}) \equiv 1 \mod p.$

Let $X := a \cdot q \cdot q^{-1} + b \cdot p \cdot p^{-1} \mod pq$

Show $X \equiv a \mod p.$

$$x = aq\underline{q^{-1}} + bpp^{-1}$$

$$+\underline{p}(bp^{-1}) =$$

$$= a(q q^{-1}) \mod p.$$

$$= a \mod p.$$

Same for $X \equiv b \mod q.$

Claim: CRT representation preserves multiplication.

Multiply using CRT. $X \cdot Y \mod pq$

- Convert to CRT

$a = X \mod p.$ $c = Y \mod p$

$b = X \mod q$ $d = Y \mod q.$

$u = (a \cdot c) \mod p$ $v = (b \cdot d) \mod q$

By CRT Solve for z so $z = (a \cdot c) \mod p$

$z = (b \cdot d) \mod q.$

By claim, $z = xy \mod pq$

In RSA:

recall

$$c^{\overset{2\lambda}{\underline{d}}} \mod \overset{}{n} \leftarrow 2\lambda$$

↑ square and add.

2λ iterations of 2λ-bit mults.

mod Multiplying (2λ-bit) $\approx (2\lambda)^2$ operations

$\approx 8\lambda$ op.

Instead:

$u = c \mod p$

$v = c \mod q$ ← ($\underline{d} \mod (\underline{p-1})$)

bit flip → $\boxed{a} = u^{d_p} \mod p$ ← λ-bit mod operation (λ^2)

$b = v^{d_q} \mod q$ 2x

Solve $x = a \mod p$

$= b \mod q$

$d_p = d \mod (p-1)$

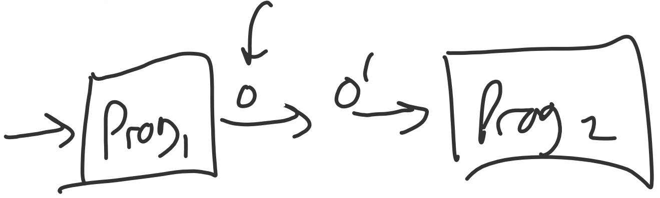
$d_q = d \mod (q-1)$

↑ λ

$2\lambda^3$ 4x better than $8\lambda^3$

Fault attacks

- Some operations are sensitive to mistakes in computing. bit flip



- Personal computers have ECC in ram making this unlikely
- Smart Cards or embedded devices more susceptible
- Space: cosmic rays no filtering
- undervolt overvolt

Suppose a bit flip

Computing $a = u^{dp} \bmod p$ bit flipped value

Only sign any valid
even numbers.

$\sigma = a \bmod p$ $\quad \underline{\sigma'} = \underline{a'} \bmod p$

$= b \bmod q$ $\quad\quad = b \bmod a$

σ correct output
σ' wrong output.

$\underline{(\sigma - \sigma')} = \underline{0 \bmod} \, \underline{q}.$

q divides $(\sigma - \sigma')$

$\underline{\gcd(n, \sigma - \sigma') = q}$ ⇒ recovers entire secret key.