# CO 485 Final Review

Keegan Morrissey

December 12, 2016

# 1 RSA Public Key Encryption

## 1.1 Scheme

- pub key: $(n, e)$, priv key: $d$
- $n = pq, ed \equiv 1 \pmod{\phi}, \phi = (p-1)(q-1)$
- Encr: $c = m^e \mod n$
- Decr: $m = c^d \mod n$

## 1.2 Proof of Correctness

- $m \in [0, n-1], c = m^e \mod n, m' = c^d \mod n$, want $m' = m$
- Case when $m \equiv 0 \pmod{p}$ is easy so consider $m \not\equiv 0 \pmod{p}$
- FlT $\Rightarrow m^{p-1} \equiv 1 \pmod{p}$
- Write $ed = 1 + k(p-1)(q-1), k \in \mathbb{Z}$
- $m' \equiv m^{ed} \equiv m \cdot m^{k(p-1)(q-1)} \equiv m \cdot 1^{k(q-1)} \equiv m \pmod{p}$
- Similarly, $m' \equiv m \pmod{q}$
- CRT $\Rightarrow m' \equiv m \pmod{n}$
- $m', m \in [0, n-1] \Rightarrow m' = m$

## 1.3 Modular Exponentiation

- $a, b, m \in [0, n-1], k = \text{bitlength}(n) = O(\log n)$
- Modular $+, -$: $O(k)$, Modular $\cdot$, inverse: $O(k^2)$

- Modular Exponentiation: $O(k^3)$ using repeated-square-and-multiply method, to compute $a^m \mod n$:

  $m = \sum_{i=0}^{k-1} m_i 2^i$

  $a^m \equiv a^{\sum_{i=0}^{k-1} m_i 2^i} \equiv \prod_{i=0}^{k-1} a^{m_i 2^i} \equiv \prod_{i=0, m_i=1}^{k-1} a^{2^i}$

# 2 Elementary Number Theory

## 2.1 Quadratic Residues

### 2.1.1 Definitions

- $\mathbb{Z}_n = \{0, ..., n-1\}, \mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : \gcd(a, n) = 1\}$
- $\phi(1) = 1$; for $n \geq 2$, $\phi(n) = |\mathbb{Z}_n^*|$
- $n$ prime $\Rightarrow \phi(n) = n - 1$, $\gcd(m, n) = 1 \Rightarrow \phi(mn) = \phi(m)\phi(n)$
- Langrange's Thm: $a \in \mathbb{Z}_n^* \Rightarrow a^{\phi(n)} \equiv 1 \pmod{n}$
- $\text{ord}(a)$ is the smallest $t$ such that $a^t \equiv 1 \pmod{n}$
- $a^s \equiv 1 \pmod{n} \iff \text{ord}(a)|s$, $a^x \equiv a^y \pmod{n} \iff x \equiv y \pmod{\text{ord}(a)}$
- A generator has order $p - 1$. There are exactly $\phi(p-1)$ generators of $\mathbb{Z}_p^*$.
- $\alpha$ is a generator of $\mathbb{Z}_p^* \Rightarrow \mathbb{Z}_p^* = \{a^i \pmod{p} : 0 \leq i \leq p-2\}$
- $QR_n = \{a \in \mathbb{Z}_n^* : a \text{ has a square root in } \mathbb{Z}_n^*\}$, $\overline{QR_n} = \{a \in \mathbb{Z}_n^* : a \text{ has no square root in } \mathbb{Z}_n^*\}$
- Thm: $p \geq 3$ is prime, $a = \alpha^k \mod p$, $a \in QR_p \iff k$ is even.
- Cor: $p \geq 3$ is prime, then $|QR_p| = |\overline{QR_p}| = \frac{p-1}{2}$

### 2.1.2 Legendre and Jacobi Symbols

- $p$: odd prime, $\left(\frac{a}{p}\right) = 0 : p|a, 1 : a \mod p \in QR_p, -1 : a \mod p \in \overline{QR_p}$
- Euler's Thm: $\left(\frac{a}{p}\right) = a^{(p-1)/2} \mod p$
- $n = p_1^{e_1} \cdot ... \cdot p_k^{e_k} \in \mathbb{Z}$, $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdot ... \cdot \left(\frac{a}{p_k}\right)^{e_k}$
- $\left(\frac{a}{n}\right) = 0 \iff \gcd(a, n) \neq 1$

- Properties:

  $\left(\frac{ab}{n}\right)\left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$

  $a \equiv b \pmod{n} \Rightarrow \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$

  $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$

  $\left(\frac{1}{n}\right) = 1$

  $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$

  $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$

  $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) \cdot (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}}$

- **Caution:** $n$ not prime, then $\left(\frac{a}{n}\right)$ does not imply that $a \in QR_n$, but $a \in QR_n \Rightarrow \left(\frac{a}{n}\right) = 1$

- Application: Coin flipping over the phone

## 2.2 PRIMES

- Prime number Thm: $\pi(x)$: # of primes in $[2, x]$; $\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$

- For $x \geq 17$, $\frac{1.26x}{\ln x} > \pi(x) > \frac{x}{\ln x}$

- Thus, we don't have to test many numbers for primality before we find a prime

### 2.2.1 Complexity Class

- PRIMES $\in$ NP $\cap$ CO-NP

  CO-NP Cert: a proper divisor of $n$

  NP Cert: $\alpha \in \mathbb{Z}_n^*$ with order $n-1$ and $n-1 = \prod_{i=1}^{t} p_i^{e_i}$, recursive certificates that each $p_i$ is prime.

### 2.2.2 Trial Division

### 2.2.3 Fermat's Test

- Fermat's Test: $n$ prime and $a \in [1, n-1]$, then $a^{n-1} \equiv 1 \pmod{n}$

  Test with $k$ values for $a$, if it $a^{n-1} \not\equiv 1 \pmod{n}$, (or $a \notin \mathbb{Z}_n^*$) then $n$ is composite, else likely prime

  if there is a Fermat Witness in $\mathbb{Z}_n^*$, then at least half of the elements in $\mathbb{Z}_n^*$ are Fermat Witnesses

  Proof: the set of all Fermat liars for $n$ is a proper subgroup of $\mathbb{Z}_n^*$.

  **Problem:** Carmichael Numbers: $n \geq 3$ with $a^{n-1} \equiv 1 \pmod{n}$ for all $a \in \mathbb{Z}_n^*$

- Thm: Odd, composite $n$ is Carmichael iff $n$ is square-free, prime $p$ divides $n \Rightarrow p-1|n-1$

### 2.2.4 Solovay-Strassen Test

- $n$ odd, prime then $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$ for all $a \in [0, n-1]$

  Repeat this with $k$ values of $a$, if many pass, likely prime.

- If there exists one Euler Witness for $n$ in $\mathbb{Z}_n^*$, then at least half of the elements of $\mathbb{Z}_n^*$ are Euler witnesses for $n$.

  Proof: the set of Euler liars for $n$ is a proper subgroup of $\mathbb{Z}_n^*$.

- Thm: if $n$ is composite, then there exists an Euler witness for $n$ in $\mathbb{Z}_n^*$.

- Proof: if $n$ is square-free, $a$ such that $a \equiv b \pmod{n}$ and $a \equiv 1 \pmod{n}$ is an Euler witness for $n$ in $\mathbb{Z}_n^*$.

- if $n$ is not square-free, $a = 1 + (n/p)$ is an Euler witness for $n$ in $\mathbb{Z}_n^*$.

- In each case, compute $\left(\frac{a}{n}\right)$, and since $\left(\frac{a}{n}\right) \neq 0$, then $a \in \mathbb{Z}_n^*$. Then compute $a^{\frac{n-1}{2}} \bmod n$ and show that this is not equal to $\left(\frac{a}{n}\right)$.

We thus conclude that both deciding whether a number is prime and generating primes are both easy tasks.

## 2.3 Factoring Integers

- COMPUTE-$d$: given $(n, e)$, compute $d$.

- FACTOR-$n$: given $(n, e)$, compute $p, q$

- Thm: FACTOR-$n \equiv_P$ COMPUTE-$d$

- COMPUTE-$d \leq_P$ FACTOR-$n$: obvious

- FACTOR-$n \leq_P$ COMPUTE-$d$: (case: $e < \sqrt{n}$)

  Claim: $\tilde{k} = (ed-1)/n$, $k = (ed-1)/phi$, then $0 < k - \tilde{k} < 6$

  use oracle to compute $d$

  compute $\tilde{k}$, then find $k$, then find $\phi$, then find $p + q$

  Solve with quad eqn: $(x-p)(x-q) = x^2 - (p+q)x + pq = 0$ for $p$ or $q$.

# 3 RSA Signature Scheme

## 3.1 Scheme

## 3.2 Chosen Message Attack

## 3.3 Security Argument

# 4 Discrete Log Problem

## 4.1 Definition

## 4.2 Known Algorithms

## 4.3 Diffie-Hellman

## 4.4 Schnor Signature Schemes

# 5 Elliptic Curves

## 5.1 Definition

## 5.2 Basic ECDH

## 5.3 EC Dual Random Bit Generators

## 5.4 Pairings

## 5.5 Weil Pairing