EECS 575: Advanced Cryptography
Fall 2022
Lecture 6

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- More number theory background
- The Rabin collection
- One-wayness of the Rabin collection

Agenda for this lecture

- Announcements
- More number theory background
- The Rabin collection
- One-wayness of the Rabin collection

Announcements

- Homework 2 is out, due 9/30
- My office hours are after class
- Alexandra will be lecturing on Monday morning 9/26

Agenda for this lecture

- Announcements
- More number theory background
- The Rabin collection
- One-wayness of the Rabin collection

Recap from last time

GCD: x, y, $gcd(x, y)$

largest $\in \mathbb{Z}$ that divides both

If $gcd(x, y) = 1$, x, y co-prime

Extended Euclidean Algorithm

$EEA(x, y) := (a, b)$

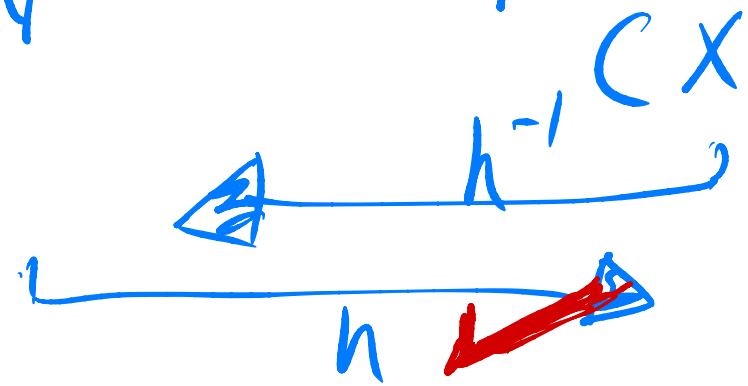
$$ax + by = gcd(x, y)$$

Recap from last time

$(N = pq)$

Chinese Remainder Theorem

$$\mathbb{Z}_N \simeq \mathbb{Z}_p \times \mathbb{Z}_q$$



$$h(x) = (x \bmod p, x \bmod q)$$

$$h(x+y) = h(x) + h(y)$$

$$h(x \cdot y) = h(x) \cdot h(y)$$

$$(x, y) \cdot (a, b) = (ax, by)$$

Chinese Remainder Theorem

Can compute $h^{-1}(x,y) \in \mathbb{Z}_N$

How? CRT Basis $h(c_p) = (1,0)$

$c_q, c_p \in \mathbb{Z}_N$ $\quad h(c_q) = (0,1)$

$h(c_p) = (c_p = 1 \bmod p,\ 0 \bmod q)$

$h^{-1}(x,y) := x c_p + y c_q \in \mathbb{Z}_N$

$h(x c_p + y c_q) = h(x c_p) + h(y c_q)$

$h(x)h(c_p) + h(y)h(c_q)$

$x \bmod p, x \bmod q \cdot (1,0)$

$(x \bmod p, 0) + (0, y \bmod q)$

Chinese Remainder Theorem

How to compute CRT basis c_p, c_q

1. write $ap + bq = 1$

$c_p = bq \in \mathbb{Z}_N$

$c_q = ap \in \mathbb{Z}_N$

$h(c_p x + c_q y) = h(c_p)h(x) + h(c_q)h(y)$

$h(c_p) = h(1 - ap) = bq$

$= (1 \bmod p, \ 1 - ap \bmod q)$

$= (1 \bmod p, \ bq \bmod q)$

$h(c_p) =$

$h(bq) = (bq \bmod p, \ bq \bmod q)$

$1 - ap$

$= (1, \ 0 \bmod q)$

Chinese Remainder Theorem

Number Theory Background

Euler's totient Function

$\varphi(p) = p-1$

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

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

$\varphi(x) = |\{y \in \{1, \ldots, x-1\} \text{ s.t. } \gcd(x,y)=1\}|$

$\mathbb{Z}_x^*$

$y^{-1} \bmod x \qquad yq = 1 \bmod x$

$EEA(x,x) \quad ax + by = 1$

Number Theory Background

$$\mathbb{Z}_N^* = \{x < N \text{ s.t. } gcd(x, N) = 1\}$$

$$\rightarrow QR_N^* = \{x \in \mathbb{Z}_N^* \text{ s.t. } \exists y \text{ s.t. } y^2 = x \bmod N\}$$

$$\mathbb{Z}_p^* = \{1, \ldots, p-1\}$$

$$|QR_p^*| = \frac{p-1}{2} \quad [\text{why?}]$$

$$\mathbb{Z}_N^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_q^*$$

$$QR_N^* \simeq QR_p^* \times QR_q^*$$

$$\mathbb{Z}_N \simeq \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_n^{e_n}}$$

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

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

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

$$q, 2q, \ldots, (p-1)q$$

$$p, 2p, \ldots, (q-1)p$$

Number Theory Background

$\mathbb{Z}_{15}^* \cong \mathbb{Z}_3^* \times \mathbb{Z}_5^*$

$h(7 \cdot 4) = h(7) \cdot h(4)$

$63 \bmod 15 = 3$

$h(3) = 3 \bmod 3,\ 3 \bmod 5$

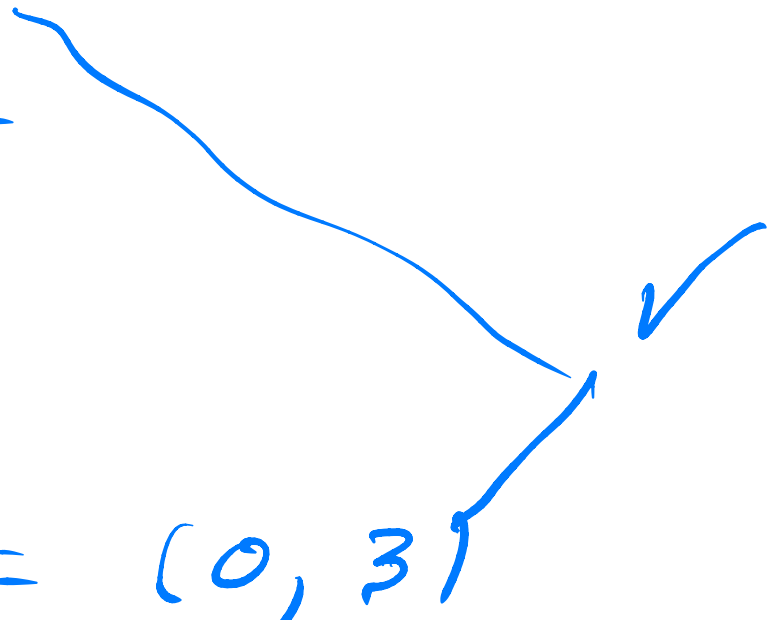
$(0, 3)$

$h(7) = 7 \bmod 3 \quad 7 \bmod 5$

$1 \quad , \quad 2$

$h(4) = 0 \quad , \quad 4$

$h(7)h(4) = (1 \cdot 0, 2 \cdot 4) = (0, 3)$



Number Theory Background

$\mathbb{Z}_{15}^*$

$\{1, 2, 4, 7, 8, 11, 13, 14\}$

$\phi(15) = (3-1)(5-1) = 8$ ✓

$\mathbb{QR}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$

$1 \quad 4 \quad 1 \quad 4 \quad 4 \quad 1 \quad 4 \quad 1$

$|\mathbb{QR}_N^*| = \frac{(p-1)(q-1)}{4} = \frac{p-1}{2} \quad \frac{q-1}{2}$

Number Theory Background

$\Phi R_{15}^{*} = \{1, 2, 4, 7, 8, 11, 13, 14\}$

$1 \quad 4 \quad 1 \quad 4 \quad 4 \quad 1 \quad 4 \quad 1$

$h(7) = 1 \bmod 3, \ 2 \bmod 5$

$h(8) = 2 \bmod 3, \ 3 \bmod 5$

$h(2) = 2 \bmod 3, \ 2 \bmod 5$

$h(13) = 1 \bmod 3, \ 3 \bmod 5$

Number Theory Background

$y \in QR_N^*$ $\quad x \in \mathbb{Z}_N^*$ s.t. $x^2 = y$

$h(x) = \{(x_1, x_2), (-x_1, x_2), (x_1, -x_2), (-x_1, -x_2)\} \in \sqrt{y} \bmod N$

$a + x = 0 \bmod N$

$a + N - a = 0 \bmod N$

$h(x) = (x \bmod p, x \bmod q)$

Agenda for this lecture

- Announcements
- More number theory background
- The Rabin collection
- One-wayness of the Rabin collection

Rabin's collection

OWF collection

$$F = \{F_s : D_s \to R_s\}_{s \in \{0,1\}^*}$$

- Easy to sample F'n
  $s \leftarrow \$(1^n)$
- Easy to sample domain
  $\forall s, \exists$ Samp
  $x \leftarrow Samp(s), x \in D_s$
- Easy to compute
  $\forall s$, det ppt
- Hard to invert
  $\Pr[I(s, f_s(x)) \in f_s^{-1}(f_s(x))]$
  $s \leftarrow \$, x \leftarrow Samp(s)$
  $\leq negl(n)$

Rabin's collection

$f_N(x) = x^2 \bmod N$ $\quad F = \{ f_N \}_{N=pq}$

$f_N : \mathbb{Z}_N^* \to QR_N^*$

- $S()$ samples p, q, outputs N
- $\mathbb{Z}_N^*$ can be sampled
- F_N eff. computed
- Hard to to invert w/r/t S

Agenda for this lecture

- Announcements
- More number theory background
- The Rabin collection
- One-wayness of the Rabin collection

Rabin's collection is one-way

Thm: If factoring is hard w.r.t. $\mathcal{D}$, then Rabin collection is OW (for $\mathcal{S}$)

Proof: Assume $\mathcal{I}$ for Rabin,

$$\Pr_{\substack{N \leftarrow \mathcal{D} \\ x \leftarrow \mathrm{Samp}}}\left[\mathcal{I}(N, f_N(x)) \in F_N^{-1}(f_N(x))\right] \geq 1/p(n)$$

$$\Pr_{\substack{N \leftarrow \mathcal{D} \\ x \leftarrow \mathrm{Samp}}}\left[\mathcal{I}(N, y = x^2 \bmod N) \in \sqrt{y}\right] \geq 1/p(n)$$

Idea: Build F factors N.

$F(N)$:

$x_1 \leftarrow \mathrm{Samp}$

$x_0^2 = y \bmod N$

$x_2 \leftarrow \mathcal{I}(N, y)$

If $x_1 \neq \pm x_2$

  Ret $\gcd(x_1 - x_2, N)$

Else

  Fail

Outputs some $\sqrt{y}$ w.p. $\geq 1/p(n)$

$$x_1^2 = x_2^2 \bmod N$$

$$(x_1 - x_2)(x_1 + x_2) = 0 \bmod N$$

0

Either $(x_1 - x_2)$ or $(x_1 + x_2)$ has gcd $\neq$

Rabin's collection is one-way