EECS 498/CSE 598: Zero-Knowledge Proofs
Winter 2026
Lecture 2

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Overview of multiprecision arithmetic
- Arithmetic modulo a prime
- Finite fields
- Engineering math libraries for cryptography

Agenda for this lecture

- Announcements
- Overview of multiprecision arithmetic
- Arithmetic modulo a prime
- Finite fields
- Engineering math libraries for cryptography

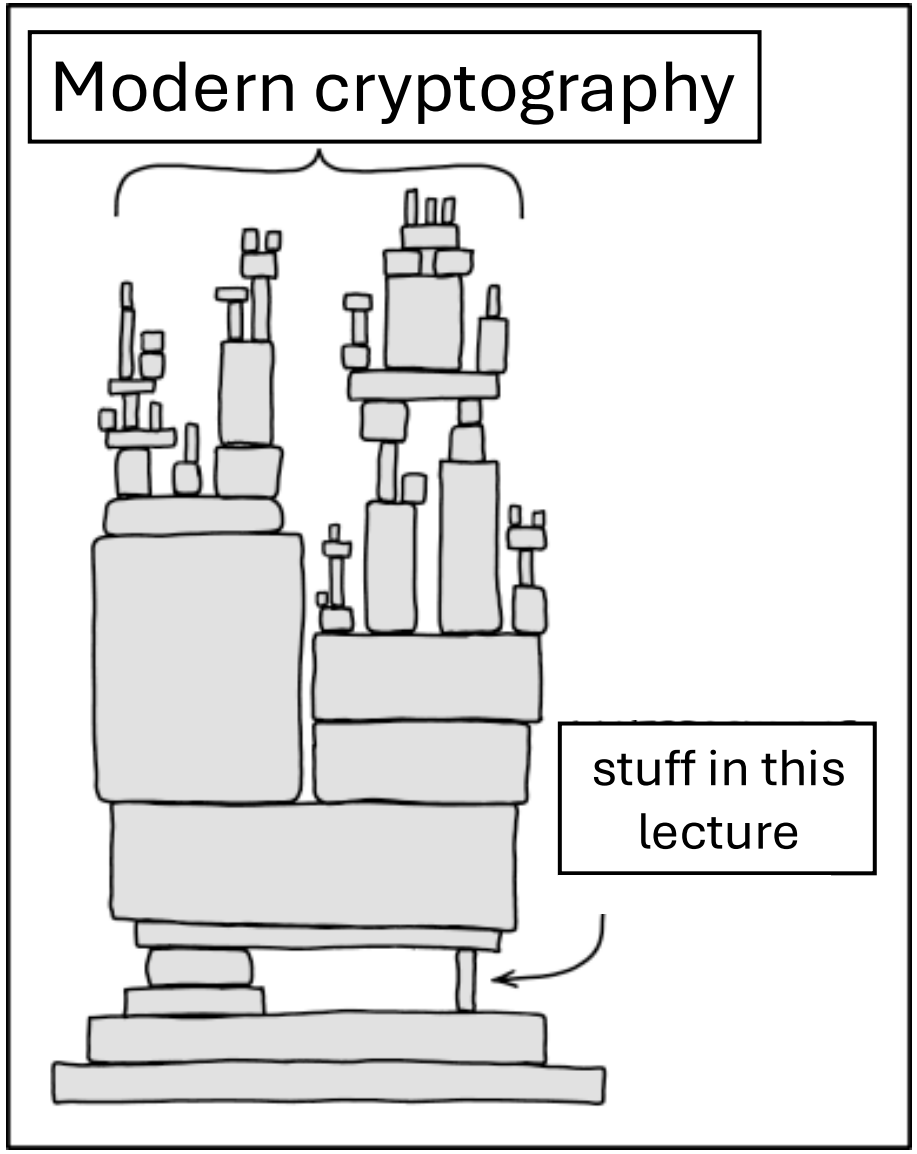
Announcements

- Project 1 is online – start if you haven't yet!
- Autograder is working
- 598 folks stay behind at the end

Guesses for Ella's cat's name?

Agenda for this lecture

- Announcements
- Overview of multiprecision arithmetic
- Arithmetic modulo a prime
- Finite fields
- Engineering math libraries for cryptography



Further background for this lecture: chapters 1-4 of Shoup

“God created the integers”

“…but humans made the mistake of creating computers”

- Computer memory is split into fixed-sized *words*. To do math on big integers, store numbers in multiple words
- Can think of the words as digits in base-B representation. Also called “limbs”:

$$d_0 + d_1 B + d_2 B^2 + \cdots d_{k-1} B^{k-1}$$

Do integer arithmetic limb-wise, using schoolbook algorithms:

$$\begin{array}{r} {\scriptstyle 1}\\ 247 \\ +\,146 \\ \hline 393 \end{array}$$

Long integer division

$67\overline{)1226}$

Fact: $\forall a, b \in \mathbb{Z}$ $\exists$ unique q, r s.t. $a = bq + r$, $0 \leq r < |b|$

Fact: $\forall a, b \in \mathbb{Z}$, $\exists$ unique largest d s.t. d divides a evenly and d divides b evenly

$d \mid a$ and $d \mid b$

d is called "greatest common divisor" of a, b $\quad d = \gcd(a, b)$

Fact: $\forall a, b \in \mathbb{Z}$, $\exists$ unique integers x, y

$ax + by = \gcd(a, b)$

x, y are Bezout coefficients

Euclid's algorithm

If $2^n > a \geq b > 0$, EEA makes at most $2n$ recursive calls $\approx$ quadratic-ish

Algorithm 1 Algorithm ExtendedEuclid(a, b) for computing the greatest common divisor of a and b.

Input: Positive integers $a \geq b > 0$.

Output: $(x, y) \in \mathbb{Z}^2$ such that $ax + by = \gcd(a, b)$.

1: **if** $b \mid a$ **then**
2: **return** $(0, 1)$
3: **else**
4: Let $a = b \cdot q + r$ for $r \in \{1, \ldots, b-1\}$
5: $(x', y') \leftarrow$ ExtendedEuclid(b, r)
6: **return** $(y', x' - q \cdot y')$
7: **end if**

$a \cdot 0 + b \cdot 1 = \gcd(a, b)$

Fact: $\gcd(a,b) = \gcd(b,r)$

Induction:

$bx' + ry' = \gcd(b,r)$

$bx' + (a - bq)y'$

$bx' + ay' - bqy' = ay' + b(x' - qy')$

Live demo!

Agenda for this lecture

- Announcements
- Overview of multiprecision arithmetic
- Arithmetic modulo a prime
- Finite fields
- Engineering math libraries for cryptography

Modular arithmetic

$a \bmod b := $ remainder r of $a \operatorname{div} b$

$\in \{0, \ldots, b-1\}$

$a \equiv b \bmod p \Rightarrow a - b \equiv 0 \bmod p$

$p \mid a - b$

$c \equiv d \bmod p$

$a + c \equiv b + d \bmod p$

Same for mul

Multiplicative inverses:

$a, p \in \mathbb{Z} \quad \exists x \text{ s.t. } ax \equiv 1 \bmod p$ iff $gcd(a, p) = 1$

$ax + py = 1$

$ax = 1 \bmod p$

Modular arithmetic

Fermat: $a^{p-1} \equiv 1 \bmod p$ — p prime

"order" of elt a mod p: smallest x s.t. $a^x \equiv 1 \bmod p$

Fact: $x \mid p-1$

Arithmetic mod p "just works"

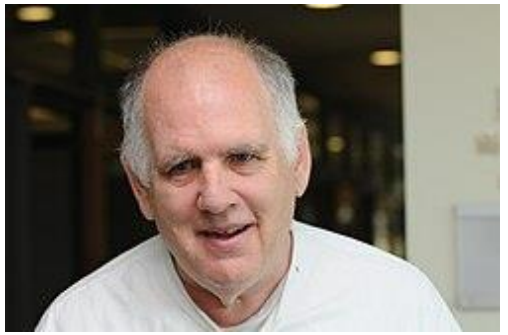
commutativity, distributive

Everything between 1 and $p-1$ have inverses

Solve systems of linear equations

$y^2 = x^3 + ax + b$

Montgomery arithmetic (*)



On Wednesday we'll talk a bit about Montgomery's other big contribution to fast cryptography software, the *Montgomery ladder*

Agenda for this lecture

- Announcements
- Overview of multiprecision arithmetic
- Arithmetic modulo a prime
- Finite fields
- Engineering math libraries for cryptography

Finite fields

$\mathbb{F}_p$

$\{0, \ldots, p-1\}$ $+, \times \bmod p$

↳ Finite field

Fact: All finite fields have size (as sets) a prime power

Factorization of $p-1$ determines possible orders of elts

$a^x \equiv 1 \bmod p$

primitive k-th root of unity mod p

$a^k \equiv 1 \bmod p$

FFT

Agenda for this lecture

- Announcements
- Overview of multiprecision arithmetic
- Arithmetic modulo a prime
- Finite fields
- Engineering math libraries for cryptography

Math libraries for cryptography

On the Importance of Eliminating Errors in Cryptographic Computations*

Dan Boneh
Department of Computer Science, Stanford University,
Stanford, CA 94305-9045, U.S.A.
dabo@cs.stanford.edu

Richard A. DeMillo
Telcordia, 445 South Street,
Morristown, NJ 07960, U.S.A.
rad@telcordia.com

Richard J. Lipton
Princeton University, 35 Olden Street,
Princeton, NJ 08544, U.S.A.
rjl@cs.princeton.edu

Incorrect code or faulty hardware can reveal secrets…

Decoding the PlayStation 3 Hack: Unraveling the ECDSA Random Generator Flaw

Vic Genin Follow 9 min read · Aug 14, 2023

Good randomness is crucial…

Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1

Daniel Bleichenbacher

Bell Laboratories
700 Mountain Ave., Murray Hill, NJ 07974
bleichen@research.bell-labs.com

Errors must be handled correctly…

Remote Timing Attacks are Practical

David Brumley
Stanford University
dbrumley@cs.stanford.edu

Dan Boneh
Stanford University
dabo@cs.stanford.edu

Need to design against *side channel attacks*…