CS 594 – Advanced Crypto (Spring 2026)

Alex Block

Lecture 1

January 12, 2026

What is this Course?

What is this Course?

- "Advanced" Cryptography
  - Really more "Intro to Crypto II"

What is this Course?

- "Advanced" Cryptography
  - Really more "Intro to Crypto II"
- Goal: cover more than the "basics" of Crypto

What is this Course?

- "Advanced" Cryptography
  - Really more "Intro to Crypto II"

- Goal: cover more than the "basics" of Crypto
  - Classic ciphers, perfect secrecy
  - Modern crypto definitions (PPT adversaries)
  - PRGs, PRFs, PRPs
  - MACs
  - OWFs, Random Oracles, Hash Functions
  - PKE (RSA, ElGamal), Key Agreement, Digital Signatures

What is this Course?

- "Advanced" Cryptography
  - Really more "Intro to Crypto II"
- Goal: cover more than the "basics" of Crypto
  - Classic ciphers, perfect secrecy
  - Modern crypto definitions (PPT adversaries)
  - PRGs, PRFs, PRPs
  - MACs
  - OWFs, Random Oracles, Hash Functions
  - PKE (RSA, ElGamal), Key Agreement, Digital Signatures
- Above is only one part of the field; Crypto is massive!

What is this Course?

Tentative list of topics:

- Asymptotic vs. Concrete Security
- Idealized Models
- Secret Sharing
- Zero-knowledge Proofs
- Secure Multi-party Computation
- Indistinguishability Obfuscation
- Memory-hard Functions
- Post-quantum Crypto

Syllabus

https://www.cs.uic.edu/~block/courses/cs594-spring2026/

Math Review: Notation

Math Review: Notation

- $\mathbb{N} := \{0, 1, 2, 3, \dots\}$; $\mathbb{Z} := \{0, \pm 1, \pm 2, \pm 3, \dots\}$, $\mathbb{Z}^+ := \{1, 2, 3, \dots\}$, $\mathbb{Q} := \{$ all rational numbers $\}$; $\mathbb{R} := \{$all real numbers$\}$; $\mathbb{R}_{\geqslant 0} := \{x \in \mathbb{R} \colon x \geqslant 0\}$

Math Review: Notation

- $\mathbb{N} := \{0, 1, 2, 3, \dots\}$; $\mathbb{Z} := \{0, \pm 1, \pm 2, \pm 3, \dots\}$, $\mathbb{Z}^+ := \{1, 2, 3, \dots\}$, $\mathbb{Q} := \{$ all rational numbers $\}$; $\mathbb{R} := \{$all real numbers$\}$; $\mathbb{R}_{\geqslant 0} := \{x \in \mathbb{R} \colon x \geqslant 0\}$

- For any $n \in \mathbb{Z}^+$, $[n] := \{1, \dots, n\}$

Math Review: Notation

- $\mathbb{N} := \{0, 1, 2, 3, \dots\}$; $\mathbb{Z} := \{0, \pm 1, \pm 2, \pm 3, \dots\}$, $\mathbb{Z}^+ := \{1, 2, 3, \dots\}$, $\mathbb{Q} := \{$ all rational numbers $\}$; $\mathbb{R} := \{$all real numbers$\}$; $\mathbb{R}_{\geqslant 0} := \{x \in \mathbb{R} \colon x \geqslant 0\}$
- For any $n \in \mathbb{Z}^+$, $[n] := \{1, \dots, n\}$
- For any vector/string x, x_i is the i^{th} symbol of the string
  - i.e., $x = (x_1, \dots, x_n)$ for a vector of length $n \in \mathbb{Z}^+$

Math Review: Notation

- $\mathbb{N} := \{0, 1, 2, 3, \dots\}$; $\mathbb{Z} := \{0, \pm 1, \pm 2, \pm 3, \dots\}$, $\mathbb{Z}^+ := \{1, 2, 3, \dots\}$, $\mathbb{Q} := \{$ all rational numbers $\}$; $\mathbb{R} := \{$all real numbers$\}$; $\mathbb{R}_{\geqslant 0} := \{x \in \mathbb{R} \colon x \geqslant 0\}$
- For any $n \in \mathbb{Z}^+$, $[n] := \{1, \dots, n\}$
- For any vector/string x, x_i is the i^{th} symbol of the string
  - i.e., $x = (x_1, \dots, x_n)$ for a vector of length $n \in \mathbb{Z}^+$
- More notation will be added as we progress in the course; please ask questions if things are not clear!

Math Review: Strings

Math Review: Strings

Definition 1 (Strings)

We let $\{0,1\}^n$ denote the set of n-bit *binary strings* (i.e., 0/1 vectors of length n). We let $x \in \{0,1\}^n$ to denote a binary *string* of length n. For any string y, we let $|y|$ denote the *length of* y.

We'll also consider strings over arbitrary alphabets (i.e., sets) S; e.g., $x \in S^n$ is a string of length n such that $x_i \in S$ for all $i \in \{1, \ldots, n\}$.

For any two strings X, Y, we let $X \| Y$ denote their concatenation.

Math Review: Strings

Definition 1 (Strings)

We let $\{0,1\}^n$ denote the set of n-bit *binary strings* (i.e., 0/1 vectors of length n). We let $x \in \{0,1\}^n$ to denote a binary *string* of length n. For any string y, we let $|y|$ denote the *length of* y.

We'll also consider strings over arbitrary alphabets (i.e., sets) S; e.g., $x \in S^n$ is a string of length n such that $x_i \in S$ for all $i \in \{1,\ldots,n\}$.

For any two strings X, Y, we let $X \| Y$ denote their concatenation.

- For any $n \in \mathbb{Z}^+$,

$$0^n := (0,\ldots,0) \in \{0,1\}^n \qquad 1^n := (1,\ldots,1) \in \{0,1\}^n$$

Math Review: Strings

Definition 1 (Strings)

We let $\{0,1\}^n$ denote the set of n-bit *binary strings* (i.e., 0/1 vectors of length n). We let $x \in \{0,1\}^n$ to denote a binary *string* of length n. For any string y, we let $|y|$ denote the *length of* y.

We'll also consider strings over arbitrary alphabets (i.e., sets) S; e.g., $x \in S^n$ is a string of length n such that $x_i \in S$ for all $i \in \{1,\ldots,n\}$.

For any two strings X, Y, we let $X \| Y$ denote their concatenation.

- For any $n \in \mathbb{Z}^+$,

$$0^n := (0,\ldots,0) \in \{0,1\}^n \qquad 1^n := (1,\ldots,1) \in \{0,1\}^n$$

- $\oplus$ will be pointwise XOR or addition mod 2

Math Review: Strings

Definition 1 (Strings)

We let $\{0,1\}^n$ denote the set of n-bit *binary strings* (i.e., 0/1 vectors of length n). We let $x \in \{0,1\}^n$ to denote a binary *string* of length n. For any string y, we let $|y|$ denote the *length of* y.

We'll also consider strings over arbitrary alphabets (i.e., sets) S; e.g., $x \in S^n$ is a string of length n such that $x_i \in S$ for all $i \in \{1,\ldots,n\}$.

For any two strings X, Y, we let $X \| Y$ denote their concatenation.

- For any $n \in \mathbb{Z}^+$,

$$0^n := (0,\ldots,0) \in \{0,1\}^n \qquad 1^n := (1,\ldots,1) \in \{0,1\}^n$$

- $\oplus$ will be pointwise XOR or addition mod 2
  - $(0,1) \oplus (1,1) = (1,0)$
  - $(0,1) \oplus (1,1) = (1,2) \mod 2 = (1,0)$

Math Review: Asymptotic Notations

Let $f(n), g(n) : \mathbb{N} \to \mathbb{R}_{\geqslant 0}$ be two functions.

Math Review: Asymptotic Notations

Let $f(n), g(n) \colon \mathbb{N} \to \mathbb{R}_{\geqslant 0}$ be two functions.

- $f(n) = O(g(n))$ if there exists $c, n' > 0$ such that for all $n \geqslant n'$, we have $f(n) \leqslant c \cdot g(n)$.

Math Review: Asymptotic Notations

Let $f(n), g(n) \colon \mathbb{N} \to \mathbb{R}_{\geqslant 0}$ be two functions.

- $f(n) = O(g(n))$ if there exists $c, n' > 0$ such that for all $n \geqslant n'$, we have $f(n) \leqslant c \cdot g(n)$.

- $f(n) = \Omega(g(n))$ if there exists $c, n' > 0$ such that for all $n \geqslant n'$, we have $f(n) \geqslant c \cdot g(n)$.

Math Review: Asymptotic Notations

Let $f(n), g(n) \colon \mathbb{N} \to \mathbb{R}_{\geqslant 0}$ be two functions.

- $f(n) = O(g(n))$ if there exists $c, n' > 0$ such that for all $n \geqslant n'$, we have $f(n) \leqslant c \cdot g(n)$.
- $f(n) = \Omega(g(n))$ if there exists $c, n' > 0$ such that for all $n \geqslant n'$, we have $f(n) \geqslant c \cdot g(n)$.
- $f(n) = \Theta(g(n))$ if $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$.

Math Review: Asymptotic Notations

Let $f(n), g(n) \colon \mathbb{N} \to \mathbb{R}_{\geqslant 0}$ be two functions.

- $f(n) = o(g(n))$ if $\lim_{n\to\infty} f(n)/g(n) = 0$; or, for every $c > 0$ there exists $n' > 0$ such that for all $n \geqslant n'$, $f(n) \leqslant c \cdot g(n)$.

Math Review: Asymptotic Notations

Let $f(n), g(n) \colon \mathbb{N} \to \mathbb{R}_{\geqslant 0}$ be two functions.

- $f(n) = o(g(n))$ if $\lim_{n\to\infty} f(n)/g(n) = 0$; or, for every $c > 0$ there exists $n' > 0$ such that for all $n \geqslant n'$, $f(n) \leqslant c \cdot g(n)$.

- $f(n) = \omega(g(n))$ if $\lim_{n\to\infty} f(n)/g(n) = \infty$; or, for every $c > 0$ there exists $n' > 0$ such that for all $n \geqslant n'$, $f(n) \geqslant c \cdot g(n)$.

Math Review: Asymptotic Notations

Let $f(n), g(n) \colon \mathbb{N} \to \mathbb{R}_{\geqslant 0}$ be two functions.

- $f(n) = o(g(n))$ if $\lim_{n\to\infty} f(n)/g(n) = 0$; or, for every $c > 0$ there exists $n' > 0$ such that for all $n \geqslant n'$, $f(n) \leqslant c \cdot g(n)$.

- $f(n) = \omega(g(n))$ if $\lim_{n\to\infty} f(n)/g(n) = \infty$; or, for every $c > 0$ there exists $n' > 0$ such that for all $n \geqslant n'$, $f(n) \geqslant c \cdot g(n)$.

Definition 2 (Negligible Function)

Let $f(n) \colon \mathbb{N} \to \mathbb{R}_{\geqslant 0}$. We say that f is *negligible* if for every constant $c > 0$, we have

$$f(n) = o(1/n^c).$$

Ex: 2^{-n}, $\sqrt{2^{-n}} = 2^{-\frac{n}{2}}$

$q(n)$: polynomial

$q(n)/2^n$

Math Review: Exponents and Logarithms

Greatest Resource Ever for this: ChiliMath

$b^x \cdot b^y = b^{x+y}$	$\log_b(x \cdot y) = \log_b(x) + \log_b(y)$
$b^x / b^y = b^{x-y}$	$\log_b(x/y) = \log_b(x) - \log_b(y)$
$(b^x)^k = b^{x \cdot k}$	$k \cdot \log_b(x) = \log_b(x^k)$
$b^0 = 1,\ b^1 = b$	$\log_b(1) = 0,\ \log_b(b) = 1$
$b^{-x} = 1/b^x$	$-\log_b(x) = \log_b(1/x)$
$b^{\log_b(k)} = k$	$\log_b(b^k) = k$
$(ab)^x = a^x b^x$	$\log_b(x) = \log_c(x)/\log_c(b)$

change of base

- b is called the *base*
- $x, y, k \in \mathbb{R}$
- for logarithms, the following must hold:
  - $b > 0$ and $b \neq 1$
  - $x, y > 0$

Math Review: Exponents and Logarithms

- $\log := \log_2$ will always denote the binary logarithm (used extensively in this course)

Math Review: Exponents and Logarithms

- $\log := \log_2$ will always denote the binary logarithm (used extensively in this course)
- $\ln := \log_e$ will always denote the natural logarithm

Math Review: Exponents and Logarithms

- $\log := \log_2$ will always denote the binary logarithm (used extensively in this course)
- $\ln := \log_e$ will always denote the natural logarithm
- Assumption: the base of a logarithm is *always constant*

Math Review: Exponents and Logarithms

- $\log := \log_2$ will always denote the binary logarithm (used extensively in this course)
- $\ln := \log_e$ will always denote the natural logarithm
- Assumption: the base of a logarithm is *always constant*
  - Gives us $\log_b(n) = \Theta(\log_c(n))$ for all constants b, c

Math Review: Exponents and Logarithms

- $\log := \log_2$ will always denote the binary logarithm (used extensively in this course)
- $\ln := \log_e$ will always denote the natural logarithm
- Assumption: the base of a logarithm is *always constant*
  - Gives us $\log_b(n) = \Theta(\log_c(n))$ for all constants b, c
  - In other words, doesn't really matter which logarithm base we choose!

Math Review: Number Theory

Math Review: Number Theory

- For $m, n \in \mathbb{Z}$, we say that m *divides* n, denoted as $m|n$, if there exists $k \in \mathbb{Z}$ such that $n = k \cdot m$; otherwise, we write $m \nmid n$

Math Review: Number Theory

- For $m, n \in \mathbb{Z}$, we say that m *divides* n, denoted as $m|n$, if there exists $k \in \mathbb{Z}$ such that $n = k \cdot m$; otherwise, we write $m \nmid n$
  - If $d|n$ and $d|m$, then d is a *common divisor* of m and n.

Math Review: Number Theory

- For $m, n \in \mathbb{Z}$, we say that m *divides* n, denoted as $m|n$, if there exists $k \in \mathbb{Z}$ such that $n = k \cdot m$; otherwise, we write $m \nmid n$
  - If $d|n$ and $d|m$, then d is a *common divisor* of m and n.
  - We let $\gcd(m, n) = \gcd(n, m) = \max_{d \in \mathbb{N}}\{d|n \text{ and } d|m\}$ denote the *greatest common divisor*

Math Review: Number Theory

- For $m, n \in \mathbb{Z}$, we say that m *divides* n, denoted as $m|n$, if there exists $k \in \mathbb{Z}$ such that $n = k \cdot m$; otherwise, we write $m \nmid n$
  - If $d|n$ and $d|m$, then d is a *common divisor* of m and n.
  - We let $\gcd(m, n) = \gcd(n, m) = \max_{d \in \mathbb{N}}\{d|n \text{ and } d|m\}$ denote the *greatest common divisor*
  - m and n are *relatively prime* if $\gcd(m, n) = 1$

Math Review: Number Theory

- For $m, n \in \mathbb{Z}$, we say that m *divides* n, denoted as $m|n$, if there exists $k \in \mathbb{Z}$ such that $n = k \cdot m$; otherwise, we write $m \nmid n$
  - If $d|n$ and $d|m$, then d is a *common divisor* of m and n.
  - We let $\gcd(m, n) = \gcd(n, m) = \max_{d \in \mathbb{N}}\{d|n \text{ and } d|m\}$ denote the *greatest common divisor*
  - m and n are *relatively prime* if $\gcd(m, n) = 1$

- For $n \in \mathbb{Z}^+$ and $m \in \mathbb{Z}$, $m \bmod n$ or $m \,\%\, n$ denotes m *modulo* n

Math Review: Number Theory

- For $m, n \in \mathbb{Z}$, we say that m *divides* n, denoted as $m|n$, if there exists $k \in \mathbb{Z}$ such that $n = k \cdot m$; otherwise, we write $m \nmid n$
  - If $d|n$ and $d|m$, then d is a *common divisor* of m and n.
  - We let $\gcd(m, n) = \gcd(n, m) = \max_{d \in \mathbb{N}}\{d|n \text{ and } d|m\}$ denote the *greatest common divisor*
  - m and n are *relatively prime* if $\gcd(m, n) = 1$

- For $n \in \mathbb{Z}^+$ and $m \in \mathbb{Z}$, $m \bmod n$ or $m \,\%\, n$ denotes m *modulo* n
  - I.e., $m \bmod n = r$, where r is the unique integer in $\{0, 1, \ldots, n-1\}$ such that $n|(m - r)$

Math Review: Number Theory

- For $m, n \in \mathbb{Z}$, we say that m *divides* n, denoted as $m|n$, if there exists $k \in \mathbb{Z}$ such that $n = k \cdot m$; otherwise, we write $m \nmid n$
  - If $d|n$ and $d|m$, then d is a *common divisor* of m and n.
  - We let $\gcd(m, n) = \gcd(n, m) = \max_{d \in \mathbb{N}}\{d|n \text{ and } d|m\}$ denote the *greatest common divisor*
  - m and n are *relatively prime* if $\gcd(m, n) = 1$

- For $n \in \mathbb{Z}^+$ and $m \in \mathbb{Z}$, $m \bmod n$ or $m \,\%\, n$ denotes m *modulo* n
  - I.e., $m \bmod n = r$, where r is the unique integer in $\{0, 1, \ldots, n-1\}$ such that $n|(m - r)$
  - Equivalence: $n|m \iff m \bmod n \equiv 0 \iff n|\gcd(m, n)$

Math Review: Number Theory

- For $m, n \in \mathbb{Z}$, we say that m *divides* n, denoted as $m|n$, if there exists $k \in \mathbb{Z}$ such that $n = k \cdot m$; otherwise, we write $m \nmid n$
  - If $d|n$ and $d|m$, then d is a *common divisor* of m and n.
  - We let $\gcd(m, n) = \gcd(n, m) = \max_{d \in \mathbb{N}}\{d|n \text{ and } d|m\}$ denote the *greatest common divisor*
  - m and n are *relatively prime* if $\gcd(m, n) = 1$

- For $n \in \mathbb{Z}^+$ and $m \in \mathbb{Z}$, $m \bmod n$ or $m \,\%\, n$ denotes m *modulo* n
  - I.e., $m \bmod n = r$, where r is the unique integer in $\{0, 1, \ldots, n-1\}$ such that $n|(m - r)$
  - Equivalence: $n|m \iff m \bmod n \equiv 0 \iff n|\gcd(m, n)$

- For $n \in \mathbb{Z}^+$, we let $\mathbb{Z}_n := \{x \bmod n : x \in \mathbb{Z}\}$

Math Review: Number Theory

- For $m, n \in \mathbb{Z}$, we say that m *divides* n, denoted as $m|n$, if there exists $k \in \mathbb{Z}$ such that $n = k \cdot m$; otherwise, we write $m \nmid n$
  - If $d|n$ and $d|m$, then d is a *common divisor* of m and n.
  - We let $\gcd(m, n) = \gcd(n, m) = \max_{d \in \mathbb{N}}\{d|n \text{ and } d|m\}$ denote the *greatest common divisor*
  - m and n are *relatively prime* if $\gcd(m, n) = 1$

- For $n \in \mathbb{Z}^+$ and $m \in \mathbb{Z}$, $m \bmod n$ or $m \,\%\, n$ denotes m *modulo* n
  - I.e., $m \bmod n = r$, where r is the unique integer in $\{0, 1, \ldots, n-1\}$ such that $n|(m - r)$
  - Equivalence: $n|m \iff m \bmod n \equiv 0 \iff n|\gcd(m, n)$

- For $n \in \mathbb{Z}^+$, we let $\mathbb{Z}_n := \{x \bmod n : x \in \mathbb{Z}\}$
  - Abusing notation, $\mathbb{Z}_n \equiv \{0, 1, \ldots, n-1\}$, where all operations are performed modulo n

Math Review: Group Theory

Math Review: Group Theory

Definition 3 (Groups)

A set $\mathbb{G}$ and an operator $\odot$ is called a *group*, denoted as $(\mathbb{G}, \odot)$, if it satisfies the following

Math Review: Group Theory

Definition 3 (Groups)

A set $\mathbb{G}$ and an operator $\odot$ is called a *group*, denoted as $(\mathbb{G}, \odot)$, if it satisfies the following

- **Closure**: for any $a, b \in \mathbb{G}$, $a \odot b \in \mathbb{G}$

Math Review: Group Theory

Definition 3 (Groups)

A set $\mathbb{G}$ and an operator $\odot$ is called a *group*, denoted as $(\mathbb{G}, \odot)$, if it satisfies the following

- **Closure**: for any $a, b \in \mathbb{G}$, $a \odot b \in \mathbb{G}$
- **Identity**: there exists a special element $1 \in \mathbb{G}$ such that $1 \odot a = a \odot 1 = a$ for all $a \in \mathbb{G}$

Math Review: Group Theory

Definition 3 (Groups)

A set $\mathbb{G}$ and an operator $\odot$ is called a *group*, denoted as $(\mathbb{G}, \odot)$, if it satisfies the following

- **Closure**: for any $a, b \in \mathbb{G}$, $a \odot b \in \mathbb{G}$
- **Identity**: there exists a special element $1 \in \mathbb{G}$ such that $1 \odot a = a \odot 1 = a$ for all $a \in \mathbb{G}$
- **Associativity**: for any $a, b, c \in \mathbb{G}$, $(a \odot b) \odot c = a \odot (b \odot c)$

Math Review: Group Theory

Definition 3 (Groups)

A set $\mathbb{G}$ and an operator $\odot$ is called a *group*, denoted as $(\mathbb{G}, \odot)$, if it satisfies the following

- **Closure**: for any $a, b \in \mathbb{G}$, $a \odot b \in \mathbb{G}$
- **Identity**: there exists a special element $1 \in \mathbb{G}$ such that $1 \odot a = a \odot 1 = a$ for all $a \in \mathbb{G}$
- **Associativity**: for any $a, b, c \in \mathbb{G}$, $(a \odot b) \odot c = a \odot (b \odot c)$
- **Inverses**: for any $a \in \mathbb{G}$, there exists an element $a^{-1} \in \mathbb{G}$ such that $a \odot a^{-1} = 1$

Math Review: Group Theory

Definition 3 (Groups)

A set $\mathbb{G}$ and an operator $\odot$ is called a *group*, denoted as $(\mathbb{G}, \odot)$, if it satisfies the following

- **Closure**: for any $a, b \in \mathbb{G}$, $a \odot b \in \mathbb{G}$
- **Identity**: there exists a special element $1 \in \mathbb{G}$ such that $1 \odot a = a \odot 1 = a$ for all $a \in \mathbb{G}$
- **Associativity**: for any $a, b, c \in \mathbb{G}$, $(a \odot b) \odot c = a \odot (b \odot c)$
- **Inverses**: for any $a \in \mathbb{G}$, there exists an element $a^{-1} \in \mathbb{G}$ such that $a \odot a^{-1} = 1$

The *order* of the group is its cardinality $|\mathbb{G}|$. A group is *finite* if the order is finite.

Math Review: Group Theory

- In this course, all groups we see will be finite unless otherwise stated

Math Review: Group Theory

- In this course, all groups we see will be finite unless otherwise stated
- We will also only see *additive* or *multiplicative* groups, where these groups (respectively) have operators $+$ and $\cdot$

Math Review: Group Theory

- In this course, all groups we see will be finite unless otherwise stated
- We will also only see *additive* or *multiplicative* groups, where these groups (respectively) have operators $+$ and $\cdot$
  - In additive groups, we let 0 denote the identity, and 1 for multiplicative groups

Math Review: Group Theory

- In this course, all groups we see will be finite unless otherwise stated
- We will also only see *additive* or *multiplicative* groups, where these groups (respectively) have operators $+$ and $\cdot$
  - In additive groups, we let 0 denote the identity, and 1 for multiplicative groups

Definition 4 (Abelian and Cyclic Groups)

A group $(\mathbb{G}, \odot)$ is *Abelian* if $\odot$ is a commutative operator: $a \odot b = b \odot a$ for all $a, b \in \mathbb{G}$. A group $(\mathbb{G}, \odot)$ is *cyclic* if it is Abelian and there exists a *generator* $g \in \mathbb{G}$ such that $\mathbb{G} = \{g^0, g^1, g^2, \dots\}$, where $g^i := \underbrace{g \odot g \odot \cdots \odot g}_{i \text{ times}}$, with $g^0 := 1$.

Math Review: Group Theory

- In this course, all groups we see will be finite unless otherwise stated
- We will also only see *additive* or *multiplicative* groups, where these groups (respectively) have operators $+$ and $\cdot$
  - In additive groups, we let 0 denote the identity, and 1 for multiplicative groups

Definition 4 (Abelian and Cyclic Groups)

A group $(\mathbb{G}, \odot)$ is *Abelian* if $\odot$ is a commutative operator: $a \odot b = b \odot a$ for all $a, b \in \mathbb{G}$. A group $(\mathbb{G}, \odot)$ is *cyclic* if it is Abelian and there exists a *generator* $g \in \mathbb{G}$ such that $\mathbb{G} = \{g^0, g^1, g^2, \dots\}$, where $g^i := \underbrace{g \odot g \odot \cdots \odot g}_{i \text{ times}}$, with $g^0 := 1$.

- In additive groups, we write $i \cdot g = \underbrace{g + g + \cdots + g}_{i \text{ times}}$, and

  multiplicative groups, we write $g^i = \underbrace{g \cdot g \cdot \cdots \cdot g}_{i \text{ times}}$

Math Review: Group Theory Examples

- $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, and $(\mathbb{Z}, +)$ are additive groups

Math Review: Group Theory Examples

- $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, and $(\mathbb{Z}, +)$ are additive groups
- $(\mathbb{R}^*, \cdot)$, $(\mathbb{Q}^*, \cdot)$ are multiplicative groups
  without 0

Math Review: Group Theory Examples

- $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, and $(\mathbb{Z}, +)$ are additive groups
- $(\mathbb{R}^*, \cdot)$, $(\mathbb{Q}^*, \cdot)$ are multiplicative groups
  - $(\mathbb{Z}^*, \cdot)$ is NOT a multiplicative group

Math Review: Group Theory Examples

- $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, and $(\mathbb{Z}, +)$ are additive groups
- $(\mathbb{R}, \cdot)$, $(\mathbb{Q}, \cdot)$ are multiplicative groups
  - $(\mathbb{Z}, \cdot)$ is NOT a multiplicative group

- For any $n \in \mathbb{Z}^+$, $(\mathbb{Z}_n, +)$ is an additive group under addition modulo n

Math Review: Group Theory Examples

- $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, and $(\mathbb{Z}, +)$ are additive groups
- $(\mathbb{R}, \cdot)$, $(\mathbb{Q}, \cdot)$ are multiplicative groups
  - $(\mathbb{Z}, \cdot)$ is NOT a multiplicative group

- For any $n \in \mathbb{Z}^+$, $(\mathbb{Z}_n, +)$ is an additive group under addition modulo n
- For any prime number p, the set $\mathbb{Z}_p^* := \{1, 2, \ldots, p-1\}$ is a multiplicative group under multiplication modulo p

Math Review: Finite Fields

Definition 5 (Finite Fields)

A set $\mathbb{F}$ is a *finite field* if $(\mathbb{F}, +)$ is an additive cyclic group and $(\mathbb{F}^*, \cdot)$ is a multiplicative cyclic group, and $|\mathbb{F}|$ is finite.

Math Review: Finite Fields

Definition 5 (Finite Fields)

A set $\mathbb{F}$ is a *finite field* if $(\mathbb{F}, +)$ is an additive cyclic group and $(\mathbb{F}^*, \cdot)$ is a multiplicative cyclic group, and $|\mathbb{F}|$ is finite.

Fact

For any finite field $\mathbb{F}$, $|\mathbb{F}| = p^m$ for prime p and $m \in \mathbb{Z}^+$.

Math Review: Finite Fields

Definition 5 (Finite Fields)

A set $\mathbb{F}$ is a *finite field* if $(\mathbb{F}, +)$ is an additive cyclic group and $(\mathbb{F}^*, \cdot)$ is a multiplicative cyclic group, and $|\mathbb{F}|$ is finite.

Fact

For any finite field $\mathbb{F}$, $|\mathbb{F}| = p^m$ for prime p and $m \in \mathbb{Z}^+$.

Examples

Math Review: Finite Fields

Definition 5 (Finite Fields)

A set $\mathbb{F}$ is a *finite field* if $(\mathbb{F}, +)$ is an additive cyclic group and $(\mathbb{F}^*, \cdot)$ is a multiplicative cyclic group, and $|\mathbb{F}|$ is finite.

Fact

For any finite field $\mathbb{F}$, $|\mathbb{F}| = p^m$ for prime p and $m \in \mathbb{Z}^+$.

Examples

- $\mathbb{F} = \mathbb{Z}_p$ is a finite field for any prime p (under addition and multiplication modulo p)

Math Review: Finite Fields

Definition 5 (Finite Fields)

A set $\mathbb{F}$ is a *finite field* if $(\mathbb{F}, +)$ is an additive cyclic group and $(\mathbb{F}^*, \cdot)$ is a multiplicative cyclic group, and $|\mathbb{F}|$ is finite.

Fact

For any finite field $\mathbb{F}$, $|\mathbb{F}| = p^m$ for prime p and $m \in \mathbb{Z}^+$.

Examples

- $\mathbb{F} = \mathbb{Z}_p$ is a finite field for any prime p (under addition and multiplication modulo p)
- $\{0, 1\} \equiv \mathbb{Z}_2$ is a finite field under XOR and AND (multiplication)

Math Review: Finite Fields

Definition 5 (Finite Fields)

A set $\mathbb{F}$ is a *finite field* if $(\mathbb{F}, +)$ is an additive cyclic group and $(\mathbb{F}^*, \cdot)$ is a multiplicative cyclic group, and $|\mathbb{F}|$ is finite.

Fact

For any finite field $\mathbb{F}$, $|\mathbb{F}| = p^m$ for prime p and $m \in \mathbb{Z}^+$.

Examples

- $\mathbb{F} = \mathbb{Z}_p$ is a finite field for any prime p (under addition and multiplication modulo p)
- $\{0, 1\} \equiv \mathbb{Z}_2$ is a finite field under XOR and AND (multiplication)
- $\mathbb{F}_{2^n} \cong \mathbb{Z}_2[X]/(P(X))$ is a finite field under multiplication and addition modulo irreducible (mod 2) polynomial $P(X)$ of degree n

Math Review: Finite Fields

Definition 5 (Finite Fields)

A set $\mathbb{F}$ is a *finite field* if $(\mathbb{F}, +)$ is an additive cyclic group and $(\mathbb{F}^*, \cdot)$ is a multiplicative cyclic group, and $|\mathbb{F}|$ is finite.

Fact

For any finite field $\mathbb{F}$, $|\mathbb{F}| = p^m$ for prime p and $m \in \mathbb{Z}^+$.

Examples

- $\mathbb{F} = \mathbb{Z}_p$ is a finite field for any prime p (under addition and multiplication modulo p)
- $\{0, 1\} \equiv \mathbb{Z}_2$ is a finite field under XOR and AND (multiplication)
- $\mathbb{F}_{2^n} \cong \mathbb{Z}_2[X]/(P(X))$ is a finite field under multiplication and addition modulo irreducible (mod 2) polynomial $P(X)$ of degree n
  - $\mathbb{F}_{2^n} \cong \mathbb{Z}_2[X]/(1 + X + X^n)$ as an example

Math Review: Linear Algebra

Math Review: Linear Algebra

- A *matrix* is a 2D grid of scalar values (e.g., $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}_n$, etc.). An $m \times n$ matrix has m rows and n columns. For a set of scalars S, we let $S^{m \times n}$ denote the set of all $m \times n$ matrices with scalars in S, and let $\mathbf{M} \in S^{m \times n}$ denote one such matrix.

Math Review: Linear Algebra

- A *matrix* is a 2D grid of scalar values (e.g., $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}_n$, etc.). An $m \times n$ matrix has m rows and n columns. For a set of scalars S, we let $S^{m \times n}$ denote the set of all $m \times n$ matrices with scalars in S, and let $\mathbf{M} \in S^{m \times n}$ denote one such matrix.
  - All sets of scalars S we consider in this class will be (finite) fields, unless otherwise stated

Math Review: Linear Algebra

- A *matrix* is a 2D grid of scalar values (e.g., $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}_n$, etc.). An $m \times n$ matrix has m rows and n columns. For a set of scalars S, we let $S^{m \times n}$ denote the set of all $m \times n$ matrices with scalars in S, and let $\mathbf{M} \in S^{m \times n}$ denote one such matrix.
  - All sets of scalars S we consider in this class will be (finite) fields, unless otherwise stated

- For two matrices $\mathbf{A} \in \mathbb{F}^{m \times n}$ and $\mathbf{B} \in \mathbb{F}^{n \times k}$, their product is $\mathbf{C} = \mathbf{A} \cdot \mathbf{B} \in \mathbb{F}^{m \times k}$.

Math Review: Linear Algebra

- A *matrix* is a 2D grid of scalar values (e.g., $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}_n$, etc.). An $m \times n$ matrix has m rows and n columns. For a set of scalars S, we let $S^{m \times n}$ denote the set of all $m \times n$ matrices with scalars in S, and let $\mathbf{M} \in S^{m \times n}$ denote one such matrix.
  - All sets of scalars S we consider in this class will be (finite) fields, unless otherwise stated

- For two matrices $\mathbf{A} \in \mathbb{F}^{m \times n}$ and $\mathbf{B} \in \mathbb{F}^{n \times k}$, their product is $\mathbf{C} = \mathbf{A} \cdot \mathbf{B} \in \mathbb{F}^{m \times k}$.

- The *transpose* of a matrix $\mathbf{A} \in \mathbb{F}^{m \times n}$ is denoted as $\mathbf{A}^\top \in \mathbb{F}^{n \times m}$ such that the i^{th} row of $\mathbf{A}$ is the i^{th} column of $\mathbf{A}^\top$.

Math Review: Linear Algebra

- A *matrix* is a 2D grid of scalar values (e.g., $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}_n$, etc.). An $m \times n$ matrix has m rows and n columns. For a set of scalars S, we let $S^{m \times n}$ denote the set of all $m \times n$ matrices with scalars in S, and let $\mathbf{M} \in S^{m \times n}$ denote one such matrix.
  - All sets of scalars S we consider in this class will be (finite) fields, unless otherwise stated

- For two matrices $\mathbf{A} \in \mathbb{F}^{m \times n}$ and $\mathbf{B} \in \mathbb{F}^{n \times k}$, their product is $\mathbf{C} = \mathbf{A} \cdot \mathbf{B} \in \mathbb{F}^{m \times k}$.

- The *transpose* of a matrix $\mathbf{A} \in \mathbb{F}^{m \times n}$ is denoted as $\mathbf{A}^\top \in \mathbb{F}^{n \times m}$ such that the i^{th} row of $\mathbf{A}$ is the i^{th} column of $\mathbf{A}^\top$.
  - For matrices $\mathbf{A}, \mathbf{B}$, we have $(\mathbf{AB})^\top = \mathbf{B}^\top \cdot \mathbf{A}^\top$ and $(\mathbf{A}^\top)^\top = \mathbf{A}$.

Math Review: Linear Algebra

- A *vector* $\vec{x}$ of length n is a $1 \times n$ matrix (i.e., a row vector, or equivalently a string).

Math Review: Linear Algebra

- A *vector* $\vec{x}$ of length n is a $1 \times n$ matrix (i.e., a row vector, or equivalently a string).
  - We let $\langle \vec{x}, \vec{y} \rangle := \sum_i x_i \cdot y_i$ denote the *inner product* for two vectors $\vec{x}, \vec{y} \in \mathbb{F}^n$.

$\vec{x} \cdot \vec{y}$

$\vec{x} \cdot (\vec{y})^T$

F-mult

F-add

Math Review: Linear Algebra

- A *vector* $\vec{x}$ of length n is a $1 \times n$ matrix (i.e., a row vector, or equivalently a string).
  - We let $\langle \vec{x}, \vec{y} \rangle := \sum_i x_i \cdot y_i$ denote the *inner product* for two vectors $\vec{x}, \vec{y} \in \mathbb{F}^n$.

- For any (finite) field $\mathbb{F}$, $(\mathbb{F}^n, +)$ is a *vector space* of dimension n, where $+$ is pointwise addition over $\mathbb{F}$.

Math Review: Probability

Math Review: Probability

- For a finite set S, we let $x \xleftarrow{\$} S$ denote the process of sampling an element of S uniformly at random.

Math Review: Probability

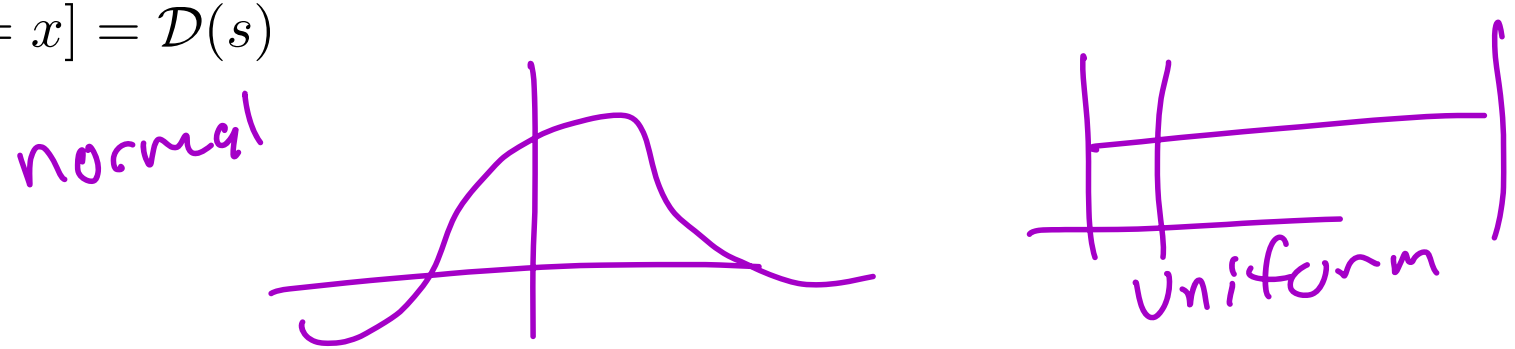
- For a finite set S, we let $x \xleftarrow{\$} S$ denote the process of sampling an element of S uniformly at random.
  - For any $s \in S$, $\Pr_{x \xleftarrow{\$} S}[x = s] = 1/|S|$.

Math Review: Probability

- For a finite set S, we let $x \xleftarrow{\$} S$ denote the process of sampling an element of S uniformly at random.
  - For any $s \in S$, $\Pr_{x \xleftarrow{\$} S}[x = s] = 1/|S|$.
- A *distribution* $\mathcal{D}$ over a finite set S is a function $\mathcal{D} \colon S \to [0, 1]$ such that $\sum_{s \in S} \mathcal{D}(s) = 1$.

Math Review: Probability

- For a finite set S, we let $x \xleftarrow{\$} S$ denote the process of sampling an element of S uniformly at random.
  - For any $s \in S$, $\Pr_{x \xleftarrow{\$} S}[x = s] = 1/|S|$.
- A *distribution* $\mathcal{D}$ over a finite set S is a function $\mathcal{D}\colon S \to [0, 1]$ such that $\sum_{s \in S} \mathcal{D}(s) = 1$.
  - We let $x \leftarrow \mathcal{D}$ denote the random process of sampling an element of S according to the distribution $\mathcal{D}$; that is, for any $s \in S$: $\Pr_{x \leftarrow \mathcal{D}}[s = x] = \mathcal{D}(s)$



Math Review: Probability

- For a finite set S, we let $x \xleftarrow{\$} S$ denote the process of sampling an element of S uniformly at random.
  - For any $s \in S$, $\Pr_{x \xleftarrow{\$} S}[x = s] = 1/|S|$.
- A *distribution* $\mathcal{D}$ over a finite set S is a function $\mathcal{D} \colon S \to [0, 1]$ such that $\sum_{s \in S} \mathcal{D}(s) = 1$.
  - We let $x \leftarrow \mathcal{D}$ denote the random process of sampling an element of S according to the distribution $\mathcal{D}$; that is, for any $s \in S$: $\Pr_{x \leftarrow \mathcal{D}}[s = x] = \mathcal{D}(s)$
  - $\mathcal{D}$ is *uniform* if $\mathcal{D}(s) = 1/|S|$ for all $s \in S$.

Math Review: Probability

- For a finite set S, we let $x \xleftarrow{\$} S$ denote the process of sampling an element of S uniformly at random.
  - For any $s \in S$, $\Pr_{x \xleftarrow{\$} S}[x = s] = 1/|S|$.
- A *distribution* $\mathcal{D}$ over a finite set S is a function $\mathcal{D}\colon S \to [0,1]$ such that $\sum_{s \in S} \mathcal{D}(s) = 1$.
  - We let $x \leftarrow \mathcal{D}$ denote the random process of sampling an element of S according to the distribution $\mathcal{D}$; that is, for any $s \in S$: $\Pr_{x \leftarrow \mathcal{D}}[s = x] = \mathcal{D}(s)$
  - $\mathcal{D}$ is *uniform* if $\mathcal{D}(s) = 1/|S|$ for all $s \in S$.
- Given a finite set S with distribution $\mathcal{D}$, an *event* E is simply any subset of S: $E \subseteq S$

Math Review: Probability

- For a finite set S, we let $x \xleftarrow{\$} S$ denote the process of sampling an element of S uniformly at random.
  - For any $s \in S$, $\Pr_{x \xleftarrow{\$} S}[x = s] = 1/|S|$.
- A *distribution* $\mathcal{D}$ over a finite set S is a function $\mathcal{D}\colon S \to [0,1]$ such that $\sum_{s \in S} \mathcal{D}(s) = 1$.
  - We let $x \leftarrow \mathcal{D}$ denote the random process of sampling an element of S according to the distribution $\mathcal{D}$; that is, for any $s \in S$: $\Pr_{x \leftarrow \mathcal{D}}[s = x] = \mathcal{D}(s)$
  - $\mathcal{D}$ is *uniform* if $\mathcal{D}(s) = 1/|S|$ for all $s \in S$.
- Given a finite set S with distribution $\mathcal{D}$, an *event* E is simply any subset of S: $E \subseteq S$
  - Note that $\Pr[E] := \sum_{e \in E} \Pr_{s \leftarrow \mathcal{D}}[e = s]$

Math Review: Probability

Fix a distribution $\mathcal{D}$ over a finite set S.

- For any two events $E_1, E_2 \subseteq S$

Math Review: Probability

Fix a distribution $\mathcal{D}$ over a finite set S.

- For any two events $E_1, E_2 \subseteq S$
  - **NOT**: $\Pr[E_1] = 1 - \Pr[\overline{E}_1] = 1 - \Pr[\neg E_1]$

Math Review: Probability

Fix a distribution $\mathcal{D}$ over a finite set S.

- For any two events $E_1, E_2 \subseteq S$
  - **NOT**: $\Pr[E_1] = 1 - \Pr[\overline{E}_1] = 1 - \Pr[\neg E_1]$
  - **AND**: $\Pr[E_1 \wedge E_2] = \Pr[E_1 \cap E_2] = \Pr[E_1] \cdot \Pr[E_2 | E_1]$

conditional probability

Math Review: Probability

Fix a distribution $\mathcal{D}$ over a finite set S.

- For any two events $E_1, E_2 \subseteq S$
  - **NOT**: $\Pr[E_1] = 1 - \Pr[\overline{E}_1] = 1 - \Pr[\neg E_1]$
  - **AND**: $\Pr[E_1 \wedge E_2] = \Pr[E_1 \cap E_2] = \Pr[E_1] \cdot \Pr[E_2|E_1]$
    - E_1 and E_2 are *independent* if $\Pr[E_1 \wedge E_2] = \Pr[E_1] \cdot \Pr[E_2]$

Math Review: Probability

Fix a distribution $\mathcal{D}$ over a finite set S.

- For any two events $E_1, E_2 \subseteq S$
  - **NOT**: $\Pr[E_1] = 1 - \Pr[\overline{E}_1] = 1 - \Pr[\neg E_1]$
  - **AND**: $\Pr[E_1 \wedge E_2] = \Pr[E_1 \cap E_2] = \Pr[E_1] \cdot \Pr[E_2|E_1]$
    - E_1 and E_2 are *independent* if $\Pr[E_1 \wedge E_2] = \Pr[E_1] \cdot \Pr[E_2]$
  - **OR**: $\Pr[E_1 \vee E_2] = \Pr[E_1 \cup E_2] = \Pr[E_1] + \Pr[E_2] - \Pr[E_1 \wedge E_2]$

Math Review: Probability

Fix a distribution $\mathcal{D}$ over a finite set S.

- For any two events $E_1, E_2 \subseteq S$
  - **NOT**: $\Pr[E_1] = 1 - \Pr[\overline{E}_1] = 1 - \Pr[\neg E_1]$
  - **AND**: $\Pr[E_1 \wedge E_2] = \Pr[E_1 \cap E_2] = \Pr[E_1] \cdot \Pr[E_2 | E_1]$
    - E_1 and E_2 are *independent* if $\Pr[E_1 \wedge E_2] = \Pr[E_1] \cdot \Pr[E_2]$
  - **OR**: $\Pr[E_1 \vee E_2] = \Pr[E_1 \cup E_2] = \Pr[E_1] + \Pr[E_2] - \Pr[E_1 \wedge E_2]$
    - **Union Bound**: $\Pr[E_1 \vee E_2] \leqslant \Pr[E_1] + \Pr[E_2]$

$$\Pr\left[\bigvee_{i=1}^{\infty} E_i\right] \leq \sum_{i=1}^{\infty} \Pr[E_i]$$

Next Time

Concrete Security vs. Asymptotic Security