Number Theory and Cryptography

Yash Sharma[1] BS-MS 3rd Year

[1]Department of Mathematics IISER Bhopal

Introduction

Number theory forms the mathematical foundation of modern cryptography. Concepts like modular arithmetic, prime factorization, and elliptic curves secure data in the digital age.

Preliminaries of Number Theory

- **Greatest Common Divisor :** For integers $a, b \neq 0$, $\gcd(a,b) = \max\{d > 0 : \ d \mid a, \ d \mid b\}$.
- **Euclidean Algorithm :** The Euclidean algorithm computes $\gcd(a,b)$; the extended version finds $x, y \in \mathbb{Z}$ with $ax + by = \gcd(a,b)$, which yields modular inverses when $\gcd(a,b) = 1$.
- **Fundamental Theorem of Arithmetic :** Every integer $n > 1$ factors uniquely as $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}, \quad p_i$ primes.
- **Totient Function :** $\varphi(n) = \#\{1 \leq k \leq n : \gcd(k,n) = 1\}$. It counts the units of $(\mathbb{Z}/n\mathbb{Z})^\times$ and is multiplicative on coprime inputs.

Theorems of Euler and Fermat

- **Euler's Theorem :** If $\gcd(a,n) = 1$ then $a^{\varphi(n)} \equiv 1 \pmod{n}$.
  - It ensures that encrypting and then decrypting a message returns the original via $(m^e)^d \equiv m \pmod{n}, \quad ed \equiv 1 \pmod{\varphi(n)}$, with Euler's theorem providing the mathematical reversibility that enables RSA to work.
- **Fermat's Little Theorem :** For prime $p \nmid a$, $a^{p-1} \equiv 1 \pmod{p}$.
  - It provides modular exponentiation and inversion—essential for encryption, decryption, and key exchange. It ensures predictable modular behavior for secure, reversible transformations in public-key systems like RSA and Diffie–Hellman.

Chinese Remainder Theorem

If $n_1, n_2, \ldots, n_k$ are pairwise coprime, then the system of congruences

$$x \equiv a_1 \pmod{n_1}, \quad x \equiv a_2 \pmod{n_2}, \quad \ldots, \quad x \equiv a_k \pmod{n_k}$$

has a unique solution modulo $N = n_1 n_2 \cdots n_k$. Explicitly,

$$x \equiv \textstyle\sum_{i=1}^{k} a_i N_i M_i \pmod{N},$$

where $N_i = N n_i^{-1}$ and $M_i \equiv N_i^{-1} \pmod{n_i}$.

- **Applications:** The CRT is crucial in RSA decryption, enabling computations modulo the prime factors p and q of $n = pq$ separately and recombining results via CRT, reducing exponentiation time by a factor of 4.

RSA Cryptography

A public-key scheme on the group $(\mathbb{Z}/n\mathbb{Z})^\times$, with $n = pq$ (large primes p, q).

Public key: (n, e). **Private key:** d with $ed \equiv 1 \pmod{\varphi(n)}$.

Encryption: $c \equiv m^e \pmod{n}$. **Decryption:** $m \equiv c^d \pmod{n}$.

- **Security basis:** Computational difficulty of factoring n and inverting modular exponentiation without d.
- **Mathematical core:** Relies on Euler's theorem $m^{\varphi(n)} \equiv 1 \pmod{n}$ for correct decryption.
- **Essence:** Modular exponentiation is a one-way trapdoor function—easy to compute but hard to invert without the secret key.

Diffie-Hellman Key Exchange

A public key exchange over insecure channels. Let $G = \langle g \rangle$ be cyclic of order q.

Alice $\to g^a$, Bob $\to g^b$; both derive g^{ab}.

Security: Rooted in the **Discrete Logarithm Problem (DLP)** — recovering a from g^a is computationally hard.

RSA vs ECC

- **ECC advantages:** Higher security per bit; compact keys and efficient scalar multiplication on $E(\mathbb{F}_q)$ minimize computation, memory, and energy — ideal for constrained systems.
- **RSA advantages:** Based on modular exponentiation in $(\mathbb{Z}/n\mathbb{Z})^\times$; simple arithmetic, long-term standardization, and broad interoperability.
- **Practical considerations:** ECC needs safe curve choice and constant-time arithmetic to avoid side-channel attacks; RSA requires large moduli ($n = pq$) for comparable security, raising computation cost.

Feature	RSA	ECC
Algebraic Base	$(\mathbb{Z}/n\mathbb{Z})^\times$	$E(\mathbb{F}_q)$, elliptic curve group
Security Basis	Integer Factorization	Elliptic Curve Discrete Logarithm (ECDLP)
Key Size	Large (2048–4096 bits)	Compact ($\approx$ 256 bits for equivalent strength)
Efficiency	Classical, slower	Modern, faster, energy-efficient

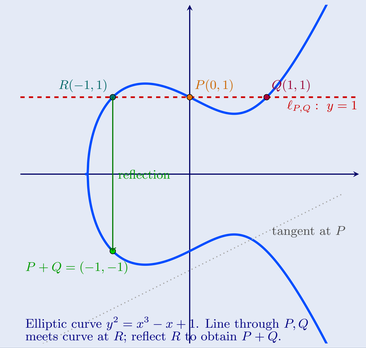
Interpretation: Both use one-way functions, but ECC gains extra security from algebraic geometry.

What Next?

- **Quantum Threat:** Shor's algorithm breaks RSA & ECC.
- **Post-Quantum Shift:** Move to quantum-resistant schemes — Lattice (NTRU, Kyber), Code (McEliece), Hash & Multivariate.
- **Core Idea:** From number/elliptic arithmetic $\to$ lattice geometry & combinatorial hardness.

Introduction to Elliptic Curves

An elliptic curve over a field K is a smooth projective curve of genus one possessing a rational base point O. In affine form (for char $K \neq 2, 3$): $E : y^2 = x^3 + ax + b, \quad \Delta = -16(4a^3 + 27b^2) \neq 0$



Geometric group law: for $P, Q \in E$ the line through P and Q meets E at R', and reflecting R' across the x-axis gives $R = P + Q$. The point at infinity $\mathcal{O}$ is the identity, and the inverse of (x, y) is $(x, -y)$.

Elliptic curves power ECC, pairings, and signatures — secure, and efficient.

Group Law on Elliptic Curves

The set $E(K)$ of K-rational points is an abelian group: for $P, Q \in E(K)$ the line through P, Q meets E at R, and

$$P + Q = -R$$

(the reflection of R across the x-axis). This defines a complete algebraic group law, so E is a group variety; the tangent case $P = Q$ yields the duplication formula.

Mordell's Theorem: $E(K) \cong E(K)_{\text{tors}} \oplus \mathbb{Z}^r$,

Elliptic Curve Cryptography

ECC is built upon the arithmetic of elliptic curves over finite fields $\mathbb{F}_q$. Its **security** relies on the **Elliptic Curve Discrete Logarithm Problem (ECDLP)** — given points $P, Q \in E(\mathbb{F}_q)$, find k such that $Q = kP$.
The difficulty of solving ECDLP underpins asymmetric cryptographic schemes like **ECDH** (key exchange) and **ECDSA** (digital signatures). ECC achieves **RSA-equivalent security** with **exponentially smaller key sizes**, due to the rich structure of $E(\mathbb{F}_q)$.

References

- S. Rubinstein-Salzedo, *Cryptography: The Mathematics of Secret Information*, Springer, 2018.
- J. H. Silverman & J. Tate, *Rational Points on Elliptic Curves*, Springer, 1992.