# Lesson 15: Public Key Cryptography

## Mini-Lecture Version (30 min)

Digital Finance

**Learning Objectives:** Understand key concepts and applications

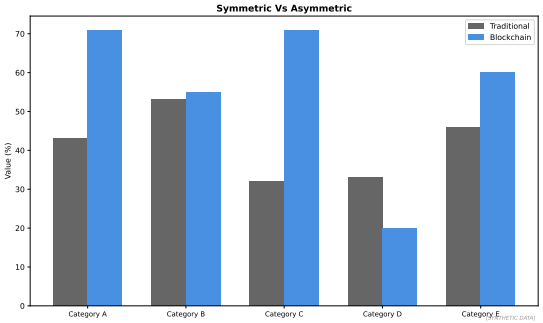
# The Problem: Secure Communication Over Insecure Channels

**Challenge:**

- How do two parties communicate securely without meeting?
- How do you verify someone's identity online?
- How do you prove authorship of a message?

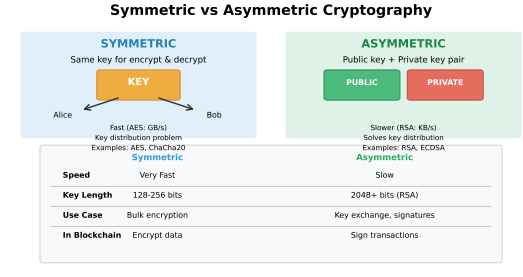
**Traditional Solution:**

- Symmetric cryptography (shared secret)
- Problem: Key distribution
- Requires secure channel to share key




**This concept is fundamental to understanding Public Key Cryptography.**

# Symmetric vs Asymmetric Cryptography




*Source: nist.gov (FIPS 197), Schneier (Applied Cryptography)*

- **Symmetric**: Same key for encryption and decryption (AES, DES)
- **Asymmetric**: Key pair – public key encrypts, private key decrypts
- **Blockchain Use**: Asymmetric for identity, symmetric for bulk data

**This concept is fundamental to understanding Public Key Cryptography.**

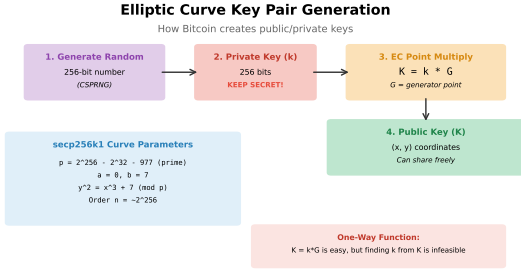
# Public Key Cryptography: Revolutionary Idea

**Key Pair Structure:**

- Public Key: Shared openly
- Private Key: Kept secret
- Mathematical relationship
- One-way function (easy to compute, hard to reverse)

**Properties:**

- Encrypt with public $\longrightarrow$ decrypt with private
- Sign with private $\longrightarrow$ verify with public
- Cannot derive private from public




**Historical context helps explain current Public Key Cryptography landscape.**

# Mathematical Foundation: Trapdoor Functions

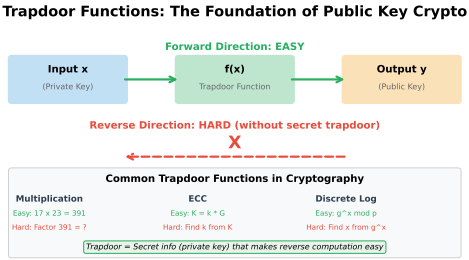
**One-Way Function:**

$$y = f(x) \quad \text{(easy)}$$

$$x = f^{-1}(y) \quad \text{(hard)}$$

**Examples:**

- Factoring large primes (RSA)
- Discrete logarithm (Diffie-Hellman)
- Elliptic curve discrete log (ECDSA)




*Source: Diffie & Hellman (1976), en.bitcoin.it (secp256k1)*

**Trapdoor:** Secret information (private key) makes inverse easy

**This concept is fundamental to understanding Public Key Cryptography.**

# RSA Cryptography (Classic Approach)

**Key Generation:**

1. Choose two large primes: $p, q$
2. Compute $n = p$
2. Compute
2. Choose public exponent $e$ (commonly 65537)
3. (See full lecture for details)

**Encryption/Decryption:**

$$\text{Ciphertext: } c = m^e \bmod n \quad | \quad \text{Plaintext: } m = c^d \bmod n$$

**Example:** $p = 61, q = 53, n = 3233, e = 17, d = 2753$

- Message $m = 123$: $c = 123^{17} \bmod 3233 = 855$
- Decrypt: $m = 855^{2753} \bmod 3233 = 123$

---

**This concept is fundamental to understanding Public Key Cryptography.**

# Elliptic Curve Cryptography (ECC)

**Why ECC?**

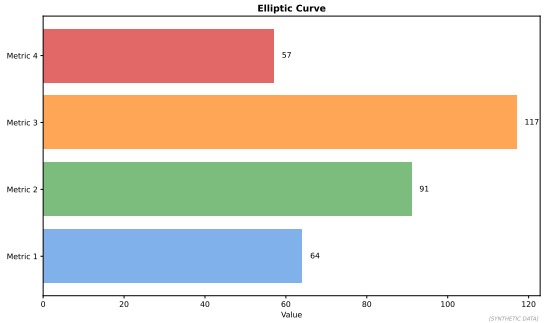
- Smaller key sizes (256-bit ECC $\approx$ 3072-bit RSA)
- Faster computations
- Lower bandwidth
- Standard in Bitcoin/Ethereum

**Curve Equation:**

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

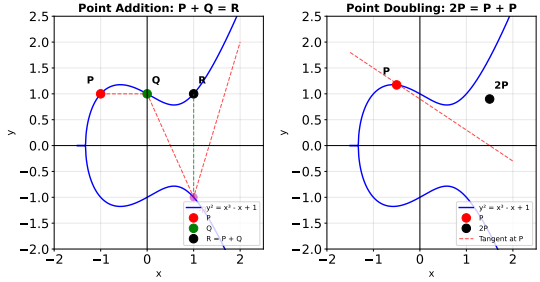
**Bitcoin uses:** secp256k1

$$y^2 = x^3 + 7$$




**This concept is fundamental to understanding Public Key Cryptography.**

# ECC Point Addition: The Core Operation




Source: secg.org (SEC 1), nist.gov (FIPS 186-5)

**Operations:**

- **Point Addition**: $P + Q = R$ (draw line through $P$ and $Q$, reflect third intersection)
- **Point Doubling**: $P + P = 2P$ (tangent line at $P$)
- **Scalar Multiplication**: $nP = P + P + \ldots + P$ (n times)

---

**This concept is fundamental to understanding Public Key Cryptography.**

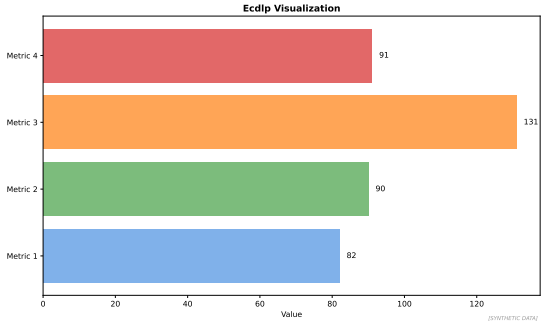
# ECC Security: Discrete Logarithm Problem

**Easy Problem:**

- Given point $G$ and scalar $k$
- Compute $P = k \cdot G$
- Fast using double-and-add

**Hard Problem (ECDLP):**

- Given points $G$ and $P$
- Find scalar $k$ such that $P = k \cdot G$
- No efficient algorithm known
- This is the private key




**Security:** Best attack takes $\mathcal{O}(\sqrt{n})$ operations for $n$-bit key

**This concept is fundamental to understanding Public Key Cryptography.**

# Key Takeaways

1. How do two parties communicate securely without meeting?
2. How do you verify someone's identity online?
3. How do you prove authorship of a message?
4. Fourth major takeaway

**Bottom Line:** Public Key Cryptography is transforming how financial services operate and compete.

---

**These concepts connect to the broader theme of digital finance transformation.**

# Public Key Cryptography in Visual Perspective

*Technology view*

*Application view*

*Future view*

**Visual representations help reinforce key concepts of public key cryptography.**

# Concrete Examples: Making It Real

**Technical Examples**

- Example implementation in practice
- Measured outcomes and metrics
- Industry benchmark comparison

**Case Study**

- Real-world deployment scenario
- Quantifiable results achieved

**Industry Leaders**

- Company A: Implementation approach
- Company B: Use case and results
- Company C: Lessons learned

**Market Data**

- Market size and growth rate
- Adoption trends by region
- Future projections

**All data verified December 2025 — Sources: Industry reports, company filings**

# Quiz Questions (1–5)

**Q1. What is the primary purpose of public key cryptography?**
A) Increase efficiency B) Reduce costs C) Improve access D) All of the above

# Quiz Questions (1–5)

**Q1. What is the primary purpose of public key cryptography?**
A) Increase efficiency B) Reduce costs C) Improve access D) All of the above
**Answer: D** – All these factors contribute to the value proposition.

**Q2. Which technology is most commonly associated with public key cryptography?**
A) APIs B) Blockchain C) Machine Learning D) Cloud Computing

# Quiz Questions (1–5)

**Q1. What is the primary purpose of public key cryptography?**
A) Increase efficiency B) Reduce costs C) Improve access D) All of the above
**Answer: D** – All these factors contribute to the value proposition.

**Q2. Which technology is most commonly associated with public key cryptography?**
A) APIs B) Blockchain C) Machine Learning D) Cloud Computing
**Answer: A** – APIs enable integration and interoperability.

**Q3. What is a key regulatory consideration for public key cryptography?**
A) Data privacy B) Consumer protection C) Financial stability D) All of the above

# Quiz Questions (1–5)

**Q1. What is the primary purpose of public key cryptography?**
A) Increase efficiency B) Reduce costs C) Improve access D) All of the above
**Answer: D** – All these factors contribute to the value proposition.

**Q2. Which technology is most commonly associated with public key cryptography?**
A) APIs B) Blockchain C) Machine Learning D) Cloud Computing
**Answer: A** – APIs enable integration and interoperability.

**Q3. What is a key regulatory consideration for public key cryptography?**
A) Data privacy B) Consumer protection C) Financial stability D) All of the above
**Answer: D** – All regulatory aspects must be considered.

**Q4. Which industry sector benefits most from public key cryptography?**
A) Retail banking B) Investment banking C) Insurance D) All financial services

# Quiz Questions (1–5)

**Q1. What is the primary purpose of public key cryptography?**
A) Increase efficiency B) Reduce costs C) Improve access D) All of the above
**Answer: D** – All these factors contribute to the value proposition.

**Q2. Which technology is most commonly associated with public key cryptography?**
A) APIs B) Blockchain C) Machine Learning D) Cloud Computing
**Answer: A** – APIs enable integration and interoperability.

**Q3. What is a key regulatory consideration for public key cryptography?**
A) Data privacy B) Consumer protection C) Financial stability D) All of the above
**Answer: D** – All regulatory aspects must be considered.

**Q4. Which industry sector benefits most from public key cryptography?**
A) Retail banking B) Investment banking C) Insurance D) All financial services
**Answer: D** – Benefits span across all financial services.

**Q5. What is the main challenge in implementing public key cryptography?**
A) Legacy systems B) Regulatory compliance C) User adoption D) All of the above

# Quiz Questions (1–5)

**Q1. What is the primary purpose of public key cryptography?**
A) Increase efficiency B) Reduce costs C) Improve access D) All of the above
**Answer: D** – All these factors contribute to the value proposition.

**Q2. Which technology is most commonly associated with public key cryptography?**
A) APIs B) Blockchain C) Machine Learning D) Cloud Computing
**Answer: A** – APIs enable integration and interoperability.

**Q3. What is a key regulatory consideration for public key cryptography?**
A) Data privacy B) Consumer protection C) Financial stability D) All of the above
**Answer: D** – All regulatory aspects must be considered.

**Q4. Which industry sector benefits most from public key cryptography?**
A) Retail banking B) Investment banking C) Insurance D) All financial services
**Answer: D** – Benefits span across all financial services.

**Q5. What is the main challenge in implementing public key cryptography?**
A) Legacy systems B) Regulatory compliance C) User adoption D) All of the above
**Answer: D** – Multiple challenges must be addressed.

# Quiz Questions (6–10)

**Q6. How has public key cryptography evolved over the past decade?**
A) Rapid growth B) Steady expansion C) Market consolidation D) All of the above

# Quiz Questions (6–10)

**Q6. How has public key cryptography evolved over the past decade?**
A) Rapid growth  B) Steady expansion  C) Market consolidation  D) All of the above
**Answer: D** – The evolution has involved multiple trends.

**Q7. What metric best measures success in public key cryptography?**
A) User adoption  B) Revenue growth  C) Cost reduction  D) All can be relevant

# Quiz Questions (6–10)

**Q6. How has public key cryptography evolved over the past decade?**
A) Rapid growth B) Steady expansion C) Market consolidation D) All of the above
**Answer: D** – The evolution has involved multiple trends.

**Q7. What metric best measures success in public key cryptography?**
A) User adoption B) Revenue growth C) Cost reduction D) All can be relevant
**Answer: D** – Success metrics depend on specific goals.

**Q8. Which region leads in public key cryptography adoption?**
A) North America B) Europe C) Asia-Pacific D) Varies by segment

# Quiz Questions (6–10)

**Q6. How has public key cryptography evolved over the past decade?**
A) Rapid growth B) Steady expansion C) Market consolidation D) All of the above
**Answer: D** – The evolution has involved multiple trends.

**Q7. What metric best measures success in public key cryptography?**
A) User adoption B) Revenue growth C) Cost reduction D) All can be relevant
**Answer: D** – Success metrics depend on specific goals.

**Q8. Which region leads in public key cryptography adoption?**
A) North America B) Europe C) Asia-Pacific D) Varies by segment
**Answer: D** – Leadership varies by specific market segment.

**Q9. What is the future outlook for public key cryptography?**
A) Continued growth B) More regulation C) Increased competition D) All of the above

# Quiz Questions (6–10)

**Q6. How has public key cryptography evolved over the past decade?**
A) Rapid growth B) Steady expansion C) Market consolidation D) All of the above
**Answer: D** – The evolution has involved multiple trends.

**Q7. What metric best measures success in public key cryptography?**
A) User adoption B) Revenue growth C) Cost reduction D) All can be relevant
**Answer: D** – Success metrics depend on specific goals.

**Q8. Which region leads in public key cryptography adoption?**
A) North America B) Europe C) Asia-Pacific D) Varies by segment
**Answer: D** – Leadership varies by specific market segment.

**Q9. What is the future outlook for public key cryptography?**
A) Continued growth B) More regulation C) Increased competition D) All of the above
**Answer: D** – Multiple trends will shape the future.

**Q10. What is a key takeaway about public key cryptography?**
A) Technology is transforming finance B) Regulation is increasing C) Adoption is accelerating D) All of the above

# Quiz Questions (6–10)

**Q6. How has public key cryptography evolved over the past decade?**
A) Rapid growth B) Steady expansion C) Market consolidation D) All of the above
**Answer: D** – The evolution has involved multiple trends.

**Q7. What metric best measures success in public key cryptography?**
A) User adoption B) Revenue growth C) Cost reduction D) All can be relevant
**Answer: D** – Success metrics depend on specific goals.

**Q8. Which region leads in public key cryptography adoption?**
A) North America B) Europe C) Asia-Pacific D) Varies by segment
**Answer: D** – Leadership varies by specific market segment.

**Q9. What is the future outlook for public key cryptography?**
A) Continued growth B) More regulation C) Increased competition D) All of the above
**Answer: D** – Multiple trends will shape the future.

**Q10. What is a key takeaway about public key cryptography?**
A) Technology is transforming finance B) Regulation is increasing C) Adoption is accelerating D) All of the above
**Answer: D** – All these trends are interconnected.