Cryptography Basics - Comprehensive Exam Questions

Table of Contents

Multiple Choice Questions (MCQs)

Basic Concepts

1. In symmetric-key cryptography, the relationship between encryption key (ke) and decryption key (kd) is: a) ke ≠ kd b) ke = kd c) ke > kd d) ke and kd are unrelated

2. Which of the following is NOT a primary goal of cryptography? a) Confidentiality b) Integrity c) Authenticity d) Compression

3. The avalanche effect in block ciphers means: a) Small changes in key cause small changes in ciphertext b) Large changes in plaintext cause small changes in ciphertext c) Small changes in plaintext or key cause significant changes in ciphertext d) The cipher becomes more secure over time

4. Stream ciphers operate on: a) Fixed-size blocks of data b) Single bits or bytes at a time c) Entire messages at once d) Variable-length blocks

RSA Cryptosystem

5. In RSA, if p = 7 and q = 11, what is the value of n? a) 18 b) 77 c) 60 d) 154

6. In RSA key generation, φ(n) represents: a) The number of prime factors of n b) The number of positive integers less than n that are relatively prime to n c) The square root of n d) The logarithm of n

7. For RSA to work correctly, the public exponent e must satisfy: a) e > n b) gcd(e, φ(n)) = 1 c) e is prime d) e < p and e < q

8. In RSA encryption, if the plaintext is X and public key is (e, n), the ciphertext Y is: a) Y = X^d mod n b) Y = X^e mod n c) Y = X + e mod n d) Y = X × e mod n

ElGamal Cryptosystem

9. The ElGamal cryptosystem's security is based on: a) Integer factorization problem b) Discrete logarithm problem c) Prime number generation d) Hash function collisions

*10. In ElGamal, a generator α of Zp means:** a) α^i mod p generates all numbers 1 to p-1 b) α is the largest element in Zp* c) α is always equal to 2 d) α is the smallest prime in Zp*

11. ElGamal encryption produces ciphertext that is: a) The same length as plaintext b) Half the length of plaintext c) Twice the length of plaintext d) Variable length depending on the message

MACs and Digital Signatures

12. The main difference between MAC and digital signature is: a) MAC uses public key, signature uses private key b) MAC provides confidentiality, signature provides integrity c) MAC uses symmetric key, signature uses asymmetric key d) MAC is faster, signature is slower

13. In HMAC, the values ipad and opad are: a) Random numbers b) Fixed padding constants c) Hash function outputs d) Key derivation functions

14. Pre-image resistance in hash functions means: a) Hard to find two inputs with same hash b) Hard to find input given the hash output c) Easy to compute hash from input d) Hash output is always the same size

15. In RSA signature scheme, to sign message m with private key d: a) s = m^e mod n b) s = m^d mod n c) s = m + d mod n d) s = m × d mod n

Hybrid Systems

16. Hybrid cryptosystems combine: a) Two different symmetric algorithms b) Two different asymmetric algorithms c) Symmetric and asymmetric algorithms d) Hash functions and encryption

17. The main advantage of hybrid systems is: a) Stronger security only b) Faster encryption only c) Better key management only d) Speed of symmetric crypto + key management of asymmetric crypto

18. In a typical hybrid system, the asymmetric algorithm is used to: a) Encrypt the entire message b) Encrypt the symmetric key c) Generate hash values d) Verify message integrity

Advanced Concepts

19. OAEP (Optimal Asymmetric Encryption Padding) is used with RSA to: a) Make encryption faster b) Reduce key size c) Improve security against attacks d) Enable digital signatures

20. The one-time pad provides perfect security when: a) The key is longer than the message b) The key is truly random and used only once c) The key is shared securely d) All of the above

---

Short Answer Questions (SAQs)

Basic Concepts

1. Define the three main security goals of cryptography and explain why each is important.

2. Explain the difference between stream ciphers and block ciphers. Give one advantage of each.

3. What is the avalanche effect in cryptography? Why is it desirable?

4. Distinguish between symmetric and asymmetric encryption in terms of keys used and typical applications.

Mathematical Foundations

5. Explain modular arithmetic. Calculate 23 mod 7 and show your work.

6. What is Euler's totient function φ(n)? Calculate φ(15) and explain your method.

7. Explain what it means for two numbers to be relatively prime. Are 15 and 28 relatively prime? Show your work.

RSA Cryptosystem

8. Perform RSA key generation with p = 5 and q = 7. Choose e = 5 and find the corresponding d.

9. Using the keys from question 8, encrypt the message m = 13 and then decrypt the result to verify.

10. Explain why RSA encryption and decryption work mathematically. What theorem makes this possible?

11. Why is "textbook RSA" considered insecure? What is OAEP and how does it address these issues?

ElGamal Cryptosystem

12. Explain the discrete logarithm problem. Why is it considered computationally hard?

13. What is a generator in the context of ElGamal? How do you verify if an element is a generator?

14. Perform ElGamal key generation with p = 11, g = 2, and private key u = 3.

15. Why is ElGamal considered probabilistic while RSA is deterministic? What are the implications?

MACs and Digital Signatures

16. Explain how Message Authentication Codes (MACs) work. What security properties do they provide?

17. What are the five essential properties of cryptographic hash functions? Explain each briefly.

18. Describe the HMAC construction. Why is it preferred over simple H(K||M)?

19. Explain the difference between authentication and non-repudiation. Which cryptographic tools provide each?

20. How does the RSA signature scheme work? Why is "hash-then-sign" used instead of signing the message directly?

Security Analysis

21. Explain two potential security vulnerabilities in stream ciphers.

22. What happens if the same RSA key pair is used for both encryption and digital signatures? Why is this problematic?

23. Describe a scenario where ElGamal would be preferred over RSA.

24. Why is key management challenging in symmetric cryptography? How do asymmetric systems help?

25. Explain the concept of perfect forward secrecy. How does it relate to hybrid systems?

Evaluation, Comparison, and Recommendation Questions

Comprehensive Evaluation Questions

1. Critical Analysis: RSA vs ElGamal Evaluate the RSA and ElGamal cryptosystems across the following dimensions:

- Security assumptions
- Computational efficiency
- Ciphertext expansion
- Randomness requirements
- Suitability for different applications

Based on your analysis, recommend which system would be better for:
a) Encrypting small messages (e.g., credit card numbers)

b) Encrypting large files
c) Implementation in resource-constrained devices

2. Security Architecture Design A company needs to implement a secure communication system with the following requirements:

- 10,000 employees need to communicate securely
- Messages range from short (100 bytes) to large (10 MB)
- System must be scalable and efficient
- Both confidentiality and authenticity are required

Design and justify a cryptographic solution. Address:

- Choice of encryption algorithms (symmetric/asymmetric)
- Key management strategy
- Authentication mechanisms
- Performance considerations
- Security trade-offs

3. Vulnerability Assessment Analyze the following cryptographic implementations and identify potential vulnerabilities:

a) **System A**: Uses RSA with 1024-bit keys, no padding, same key pair for encryption and signing b) **System B**: Uses AES-128 with a fixed key for all communications c) **System C**: Uses HMAC-MD5 for message authentication d) **System D**: Uses ElGamal with small random values for k

For each system, provide:

- Risk assessment (High/Medium/Low)
- Specific vulnerabilities
- Recommended fixes
- Implementation priority

4. Algorithm Selection Framework Create a decision framework for selecting cryptographic algorithms. Your framework should consider:

- Security requirements
- Performance constraints
- Regulatory compliance

- Future-proofing
- Implementation complexity

Apply your framework to recommend solutions for:
a) IoT sensor network
b) Banking transaction system
c) Secure messaging application
d) Digital document signing

Comparative Analysis Questions

5. Stream Ciphers vs Block Ciphers Compare stream ciphers and block ciphers across multiple dimensions:

Aspect	Stream Ciphers	Block Ciphers
Data Processing		
Memory Requirements		
Error Propagation		
Implementation Complexity		
Typical Applications		

Based on your comparison, recommend the appropriate cipher type for:

- Real-time voice communication
- File encryption
- Database encryption
- Network protocol encryption

6. MAC vs Digital Signature Comparison Analyze MACs and Digital Signatures across these criteria:

Security Properties:

- Authentication
- Integrity
- Non-repudiation
- Scalability

Performance:

- Computational overhead

- Key management complexity
- Verification speed

Practical Considerations:

- Infrastructure requirements
- Regulatory acceptance
- Implementation challenges

Recommend the appropriate solution for:
a) Internal company email system
b) Legal document system
c) Financial transaction processing
d) IoT device authentication

Recommendation and Justification Questions

7. Hybrid System Design Design a hybrid cryptographic system for a telemedicine application where:

- Patient data must be highly secure
- Real-time video consultation is required
- System must work on mobile devices
- Regulatory compliance (HIPAA) is mandatory

Your design should address:

- Symmetric algorithm choice and justification
- Asymmetric algorithm choice and justification
- Key exchange mechanism
- Authentication strategy
- Performance optimization
- Compliance considerations

8. Future-Proofing Strategy Quantum computers pose a threat to current cryptographic systems. Develop a migration strategy for an organization currently using:

- RSA-2048 for key exchange
- AES-128 for symmetric encryption
- SHA-256 for hashing

- RSA signatures for authentication

Your strategy should include:

- Risk timeline assessment
- Alternative algorithms evaluation
- Migration phases and priorities
- Cost-benefit analysis
- Backward compatibility considerations

9. Security vs Performance Trade-off An online gaming company needs to implement security for real-time multiplayer games. The system must:

- Prevent cheating (message integrity)
- Protect user accounts (authentication)
- Maintain low latency (<50ms)
- Support 100,000 concurrent users

Analyze the trade-offs and recommend a solution that addresses:

- Encryption algorithm selection
- Key management approach
- Authentication mechanism
- Performance optimization techniques
- Scalability considerations

10. Regulatory Compliance Scenario A multinational corporation needs to implement cryptography that complies with:

- US FIPS 140-2 standards
- EU GDPR requirements
- Industry-specific regulations (finance/healthcare)
- Export control restrictions

Evaluate and recommend:

- Compliant algorithms and key sizes
- Implementation standards
- Audit and monitoring requirements

- International deployment considerations
- Risk management strategies

Case Study Analysis

11. Cryptographic Failure Analysis Analyze this scenario: *A company implemented a secure messaging system using RSA with 1024-bit keys and no padding. After deployment, they discovered that attackers could decrypt messages by exploiting the deterministic nature of their implementation.*

Address:

- Root cause analysis
- Vulnerability exploitation methods
- Impact assessment
- Remediation strategies
- Prevention measures for future implementations

12. Implementation Challenge You're tasked with securing a legacy system that:

- Currently uses plaintext communication
- Cannot be completely redesigned
- Must maintain backward compatibility
- Has limited computational resources
- Requires immediate security improvement

Develop a phased implementation plan that includes:

- Immediate security enhancements
- Medium-term improvements
- Long-term security architecture
- Risk mitigation during transition
- Success metrics and validation

Answer Key

MCQ Answers

1. b) ke = kd
2. d) Compression

3. c) Small changes in plaintext or key cause significant changes in ciphertext
4. b) Single bits or bytes at a time
5. b) 77
6. b) The number of positive integers less than n that are relatively prime to n
7. b) gcd(e, φ(n)) = 1
8. b) Y = X^e mod n
9. b) Discrete logarithm problem
10. a) α^i mod p generates all numbers 1 to p-1
11. c) Twice the length of plaintext
12. c) MAC uses symmetric key, signature uses asymmetric key
13. b) Fixed padding constants
14. b) Hard to find input given the hash output
15. b) s = m^d mod n
16. c) Symmetric and asymmetric algorithms
17. d) Speed of symmetric crypto + key management of asymmetric crypto
18. b) Encrypt the symmetric key
19. c) Improve security against attacks
20. d) All of the above

SAQ Sample Answers

Question 1: Three main security goals

- **Confidentiality**: Keeping information secret from unauthorized parties. Important for protecting sensitive data like personal information, trade secrets, and classified documents.
- **Integrity**: Ensuring data hasn't been altered or tampered with. Critical for maintaining trust in communications and preventing malicious modifications.
- **Authenticity**: Verifying the identity of the sender and ensuring the message origin is legitimate. Essential for preventing impersonation and ensuring accountability.

Question 5: Modular arithmetic Modular arithmetic involves finding the remainder when one number is divided by another. 23 mod 7 = 2 Calculation: 23 ÷ 7 = 3 remainder 2 Therefore, 23 ≡ 2 (mod 7)

Question 8: RSA key generation Given p = 5, q = 7, e = 5:

- n = p × q = 5 × 7 = 35

- φ(n) = (p-1)(q-1) = 4 × 6 = 24
- Check gcd(5, 24) = 1 ✓
- Find d: 5d ≡ 1 (mod 24)
- d = 5 (since 5 × 5 = 25 ≡ 1 mod 24)
- Public key: (5, 35)
- Private key: (5, 35)

Evaluation Question Guidelines

For the comprehensive evaluation questions, students should demonstrate:

- Deep understanding of cryptographic concepts
- Ability to analyze trade-offs
- Practical implementation considerations
- Security risk assessment
- Clear justification of recommendations
- Consideration of real-world constraints

Grading should focus on:

- Technical accuracy (40%)
- Analysis depth (30%)
- Practical considerations (20%)
- Communication clarity (10%)