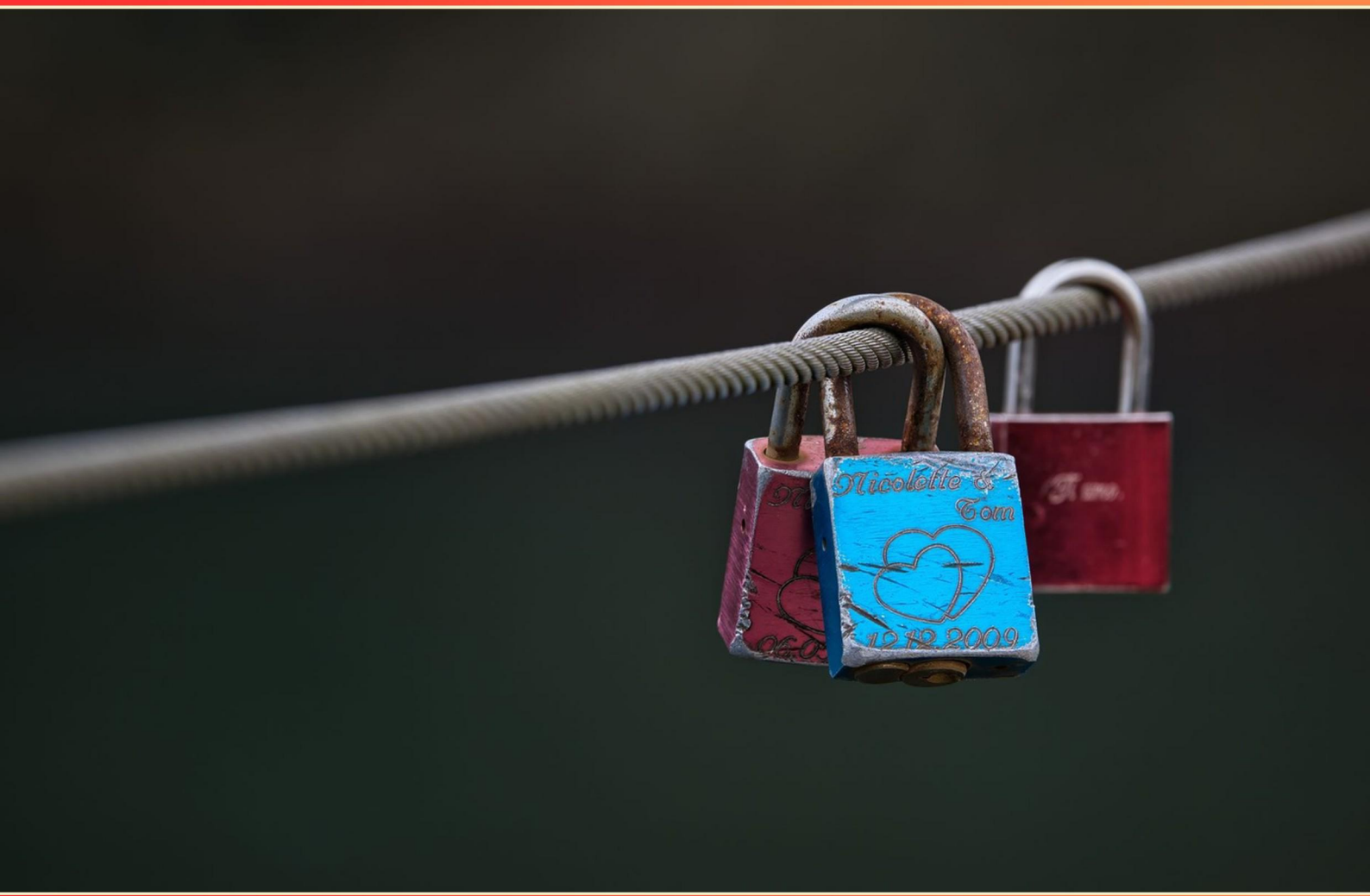
WESTERN GOVERNORS UNIVERSITY (WGU) ITAS 2142 D830 INTRODUCTION TO CRYPTOGRAPHY PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://wgu-itas2142d830.examzify.com

Table of Contents

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- Practice answering questions under realistic conditions,
- Improve accuracy and speed,
- Review explanations to strengthen weak areas, and
- Approach the exam with greater confidence.

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There's no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. What is the primary purpose of salting passwords before hashing?

A. To create a fixed-length output

B. To speed up hashing

C. To prevent rainbow table attacks

D. To ensure integrity and authenticity

2. WPA3-Personal replaces WPA2-PSK with which mechanism?

A. RSA-PSS

B. SAE (Simultaneous Authentication of Equals)

C. DHE-RSA

D. ECDSA-SHA256

3. Which principle states that a cryptosystem should be secure even if the algorithm is public, and only the key must remain secret?

A. Encryption

B. Kerckhoffs's Principle

C. Cipher

D. Plaintext

4. Which statement defines Integrity?

A. Granting permissions after authentication.

B. Verifying identity of a user or system.

C. Ensuring data is not altered without authorization.

D. Ensuring data is only accessible to authorized users.

5. In a proof-of-work blockchain, what is the purpose of a nonce?

A. To serve as a random seed for encryption

B. To act as a number that, when hashed, meets difficulty criteria

C. To identify the miner

D. To encrypt the block contents

6. What term describes a one-way function that can be reversed with secret information?

A. One-Way Function

B. Symmetric Cryptography

C. Substitution Cipher

D. Trapdoor Function

7. CRYSTALS-Kyber is primarily which type of primitive?

A. Key encapsulation mechanism

B. Digital signature

C. Hash function

D. Symmetric cipher

8. Who issues certificates?

A. Public Key Registry

B. Certification Scientist Board

C. Public Auditor

D. Certificate Authority (CA)

9. Which entity verifies identities before certificates are issued?

A. Registration Authority (RA)

B. Certificate Authority (CA)

C. Certificate Revocation List (CRL)

D. Hierarchical Trust Model

10. What does tunnel mode do?

A. Encrypts header only

B. Encrypts entire packet

C. Encrypts payload only

D. Signs packet

Answers

1. C
2. B
3. B
4. C
5. B
6. D
7. A
8. D
9. A
10. B

Explanations

1. What is the primary purpose of salting passwords before hashing?

A. To create a fixed-length output

B. To speed up hashing

C. To prevent rainbow table attacks

D. To ensure integrity and authenticity

Salting passwords before hashing is mainly to defeat rainbow table attacks. Rainbow tables are precomputed lists of password hashes for common passwords, so an attacker can reverse a hash and discover the original password if no salt is used. Introducing a unique, random salt for each password means the value being hashed is different for every user, even if the passwords are the same. This makes precomputed tables useless, because the attacker would have to generate a separate table for every possible salt, which is extremely costly and impractical. The salt is stored with the hash so the system can verify the password during login. The other options don't capture the purpose of salting. Creating a fixed-length output is a property of the hash function itself, not why you add a salt. Salting doesn't inherently speed up hashing; the goal is not speed but security against precomputed attacks. It also isn't about integrity or authenticity, which require mechanisms like MACs or digital signatures.

2. WPA3-Personal replaces WPA2-PSK with which mechanism?

A. RSA-PSS

B. SAE (Simultaneous Authentication of Equals)

C. DHE-RSA

D. ECDSA-SHA256

WPA3-Personal replaces the static pre-shared key with a password-based mutual authentication method that provides stronger protection. This mechanism is SAE, Simultaneous Authentication of Equals, also known as the Dragonfly handshake. In SAE, the client and access point prove knowledge of the shared password through a secure exchange without sending the password itself. Each session derives a fresh, ephemeral shared secret, giving forward secrecy and preventing offline dictionary attacks because an attacker cannot test guesses from captured handshakes without online interaction with the devices. The other options are cryptographic techniques used for signatures or different key-exchange setups in other contexts, not the password-based mutual authentication method used here.

3. Which principle states that a cryptosystem should be secure even if the algorithm is public, and only the key must remain secret?

A. Encryption

B. Kerckhoffs's Principle

C. Cipher

D. Plaintext

Security relies on the key being kept secret, even when everyone knows the method used to encrypt. This idea is Kerckhoffs's Principle: a cryptosystem should remain secure if the algorithm is public and only the key remains secret. By making the algorithm open to analysis, its weaknesses can be found and fixed, while the actual protection comes from the secrecy and strength of the key. For example, RSA relies on a publicly known algorithm, with security resting on the difficulty of factoring large numbers and the secrecy of the private key. The other terms describe parts of the process or data, not the principle about keeping cryptographic security tied to the key rather than the obscurity of the algorithm.

4. Which statement defines Integrity?

A. Granting permissions after authentication.

B. Verifying identity of a user or system.

C. Ensuring data is not altered without authorization.

D. Ensuring data is only accessible to authorized users.

Integrity is about trustworthiness of data: it means information remains accurate and unchanged by unauthorized parties, and any legitimate changes are detectable and authorized. This is achieved with mechanisms like hashes, checksums, digital signatures, message authentication codes, and audit trails, which help ensure that tampering is detectable and prevent improper modifications. Therefore, the statement that describes data not being altered without authorization best captures integrity. The other options describe authentication (verifying identity), authorization (granting permissions), and confidentiality (restricting access), which are different security properties.

5. In a proof-of-work blockchain, what is the purpose of a nonce?

A. To serve as a random seed for encryption

B. To act as a number that, when hashed, meets difficulty criteria

C. To identify the miner

D. To encrypt the block contents

The main idea is that the nonce is the adjustable value miners vary to produce a hash that meets the network's difficulty. In proof-of-work, the block header (which includes things like the previous block hash and the Merkle root) is hashed together with a candidate nonce. Because cryptographic hashes behave like random functions, most nonces won't produce a hash below the difficulty target, but a tiny fraction will. Miners keep trying different nonce values until the hash falls under the required threshold, proving that a certain amount of computational work was done. Once such a nonce is found, the block is considered mined and broadcast. It isn't used as an encryption seed, it doesn't identify the miner, and it doesn't encrypt or alter the block contents. Those roles are separate; the nonce's sole purpose is to enable the proof-of-work condition by providing the variable value that can be hashed to meet the difficulty.

6. What term describes a one-way function that can be reversed with secret information?

A. One-Way Function

B. Symmetric Cryptography

C. Substitution Cipher

D. Trapdoor Function

In cryptography, a trapdoor function is a one-way operation that becomes easy to reverse only when you possess a secret piece of information. The forward calculation is straightforward, but reversing it is hard without the secret. With the trapdoor (the secret), you can invert efficiently. This concept is foundational for public-key systems: anyone can apply the forward operation with a public key, but only the private key holder—the trapdoor—can invert it to recover the original input. This differs from a plain one-way function, which is hard to invert but not designed to be easily invertible with any secret. Symmetric cryptography and simple substitution ciphers rely on shared or fixed keys for both directions and aren't about a hidden trapdoor that makes inversion feasible only for someone who knows it.

7. CRYSTALS-Kyber is primarily which type of primitive?

A. Key encapsulation mechanism

B. Digital signature

C. Hash function

D. Symmetric cipher

This question tests whether you understand that CRYSTALS-Kyber is a post-quantum public-key primitive used to securely establish a symmetric key. It is a key encapsulation mechanism: the sender uses the recipient's public key to encapsulate a random secret into a ciphertext, and the recipient uses their private key to decapsulate and recover the same secret. The shared secret can then be fed into a symmetric cipher to encrypt data. It's not a digital signature, which would provide authentication of origin rather than key exchange; it's not a hash function, which produces fixed-size digests; and it's not a symmetric cipher by itself, which would require a previously shared secret rather than a public-key operation to establish it.

8. Who issues certificates?

A. Public Key Registry

B. Certification Scientist Board

C. Public Auditor

D. Certificate Authority (CA)

Digital certificates are issued by a certificate authority, a trusted entity in a public key infrastructure. The CA verifies the identity of the party requesting a certificate and then issues a digital certificate that binds that identity to a specific public key. The certificate is digitally signed with the CA's private key, allowing anyone who trusts the CA to verify the certificate with the CA's public key. This chain of trust lets others be confident that the public key really belongs to the claimed entity, which is essential for secure communications like TLS/SSL. Other options don't fit because they're not standard issuing authorities in PKI: a public key registry is typically just a directory, not an issuer; a public auditor isn't involved in certificate issuance; and a Certification Scientist Board isn't a recognized authority for issuing certificates.

9. Which entity verifies identities before certificates are issued?

A. Registration Authority (RA)

B. Certificate Authority (CA)

C. Certificate Revocation List (CRL)

D. Hierarchical Trust Model

The key idea is how identity proofing fits into issuing a digital certificate. In a PKI, verifying the applicant's identity happens during enrollment, and this job is handled by the Registration Authority. The RA collects the necessary information, checks documents or credentials, and confirms that the requester meets policy requirements. Once identity verification is completed, the RA forwards the validated request to the Certificate Authority, which then issues and signs the certificate that binds the public key to that verified identity. The Certificate Revocation List is used to check whether a certificate has been revoked, not to verify identities. The hierarchical trust model describes how trust is structured among authorities (root and subordinate CAs) rather than performing identity verification itself. So, the entity responsible for verifying identities before certificates are issued is the Registration Authority.

10. What does tunnel mode do?

A. Encrypts header only

B. Encrypts entire packet

C. Encrypts payload only

D. Signs packet

Tunnel mode secures by wrapping the entire original IP datagram inside an encrypted payload and then placing it inside a new outer IP header. This means both the header of the original packet and its payload are encrypted and protected as it travels, while a new outer header is used for routing. In short, the whole packet goes through confidentiality protection, not just the payload or a signature, which is why tunnel mode encrypts the entire packet.

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://wgu-itas2142d830.examzify.com

We wish you the very best on your exam journey. You've got this!