Western Governors University (WGU) ITAS 2142 D830 Introduction to Cryptography Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

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. Which attack uses the birthday paradox to maximize hash collisions?

- **A. Collision attack**
- **B. Known-plaintext attack**
- **C. Brute-force attack**
- **D. Birthday attack**

2. Which defines asymmetric encryption?

- **A. Relies on a shared secret key**
- **B. Encrypts with a single public key only**
- **C. Uses a public/private key pair**
- **D. Is faster than symmetric encryption**

3. What is a cryptosystem?

- **A. A single encryption algorithm**
- **B. A hardware device for encrypting data**
- **C. A synonym for a hash function**
- **D. A combination of cryptographic algorithms and protocols**

4. A cipher that replaces plaintext symbols with other symbols.

- **A. Substitution Cipher**
- **B. Transposition Cipher**
- **C. Caesar Cipher**
- **D. Polyalphabetic Cipher**

5. Which statement best reflects the security goal of TLS 1.3?

- **A. TLS 1.3 uses no symmetric encryption**
- **B. A server private key compromise does not reveal past session plaintext**
- **C. TLS 1.3 eliminates all public-key operations**
- **D. TLS 1.3 requires full chain revocation checks on every handshake**

6. Which construct is a Message Authentication Code used to verify data integrity and authenticity with a secret key?

A. MAC (Message Authentication Code)

B. Digital Signature

C. Nonce

D. Initialization Vector (IV)

7. Which statement best describes AEAD modes like GCM?

A. They provide confidentiality and integrity for the ciphertext and associated data

B. They provide only confidentiality

C. They provide only integrity

D. They provide key management

8. What is the main purpose of triple-DES (3DES)?

A. Increase effective key length and security against brute-force

B. Faster than DES

C. Provide hashing

D. Provide authenticated encryption

9. Which term is described as the process of converting plaintext into ciphertext?

A. Cipher

B. Plaintext

C. Ciphertext

D. Key

10. Which mode turns a block cipher into a stream cipher?

A. AES

B. CBC Mode

C. CFB Mode

D. ECB Mode

Answers

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

Explanations

1. Which attack uses the birthday paradox to maximize hash collisions?

A. Collision attack

B. Known-plaintext attack

C. Brute-force attack

D. Birthday attack

The idea being tested is how the birthday paradox informs when hash collisions become likely. A cryptographic hash maps many possible inputs to a fixed-size output, so collisions—two different inputs producing the same hash—are inevitable. The birthday paradox shows that with a hash of n bits, you don't need to try 2^n inputs to expect a collision; you expect one after roughly 2^(n/2) attempts. This is the essence of a birthday attack: an approach that deliberately generates many inputs to force a collision in the hash output, exploiting that probability threshold. That makes it the best answer because it directly ties the collision goal to the statistical phenomenon described by the birthday paradox. Other terms describe different ideas: a collision attack is a broad term for finding any two inputs with the same hash, a brute-force attack blindly exhausts possibilities, and a known-plaintext attack uses known plaintext-ciphertext pairs to infer secrets. None of those specifically hinge on the birthday paradox to maximize collisions the way the birthday attack does.

2. Which defines asymmetric encryption?

A. Relies on a shared secret key

B. Encrypts with a single public key only

C. Uses a public/private key pair

D. Is faster than symmetric encryption

Asymmetric encryption relies on a public/private key pair. The public key can be shared openly so others can encrypt data or verify a signature, while the private key stays with the owner to decrypt or sign. This setup removes the need for a shared secret between parties, which is what symmetric encryption requires. The other statements don't define asymmetric encryption: using a shared secret key describes symmetric approaches; encrypting with a public key alone omits the essential role of the private key for decryption or signing; and being faster than symmetric encryption is not a defining trait—asymmetric methods are typically slower and are often used to securely exchange keys that symmetric encryption then uses for fast data protection.

3. What is a cryptosystem?

A. A single encryption algorithm

B. A hardware device for encrypting data

C. A synonym for a hash function

D. A combination of cryptographic algorithms and protocols

A cryptosystem is an integrated setup of cryptographic algorithms and protocols that work together to provide security services such as confidentiality, integrity, and authenticity. It isn't just one encryption algorithm; it's the complete framework that includes encryption and decryption methods, key management, digital signatures, hash or MAC functions, and the procedures and rules (protocols) that govern how these pieces are used in real communication—such as how keys are exchanged, how sessions are established, and how data is protected during transfer. This is why the correct description emphasizes a combination of algorithms and protocols. A single algorithm by itself can't handle all aspects like key management and secure interaction between parties. A hardware device might implement parts of a cryptosystem, but a cryptosystem refers to the full system, not just a device. A hash function alone isn't a cryptosystem either, since it's only a primitive used for integrity checks, not the entire secure framework.

4. A cipher that replaces plaintext symbols with other symbols.

A. Substitution Cipher

B. Transposition Cipher

C. Caesar Cipher

D. Polyalphabetic Cipher

Substitution is about replacing each plaintext symbol with a different symbol to produce ciphertext. In a substitution cipher, there is a fixed mapping from plaintext characters to ciphertext characters, so every symbol in the message is replaced by one other symbol, keeping the length the same. This contrasts with a transposition cipher, which reorders the same symbols without changing them. A Caesar cipher is a specific substitution that shifts every letter by a fixed amount, while a polyalphabetic cipher uses multiple substitution alphabets to vary the mapping. So describing a cipher that replaces plaintext symbols with other symbols points to substitution cipher as the correct idea.

5. Which statement best reflects the security goal of TLS 1.3?

A. TLS 1.3 uses no symmetric encryption

B. A server private key compromise does not reveal past session plaintext

C. TLS 1.3 eliminates all public-key operations

D. TLS 1.3 requires full chain revocation checks on every handshake

Forward secrecy is the security goal shown here. It means that if the server's private key is compromised after a session has ended, that compromise cannot expose the plaintext of what was previously exchanged. TLS 1.3 achieves this by using ephemeral Diffie-Hellman (ECDHE) for each connection to derive fresh session keys. The keys that protect the session data are created during the handshake and then discarded, so the long-term private key isn't needed to decrypt past traffic. The server's private key is only used to authenticate the handshake, not to decrypt the data from prior sessions. That's why a later private-key compromise doesn't reveal past communications. The other statements don't reflect this security property: symmetric encryption is used after the handshake; public-key operations are still used during the handshake for authentication; and requiring full chain revocation checks on every handshake isn't the defining goal of TLS 1.3.

6. Which construct is a Message Authentication Code used to verify data integrity and authenticity with a secret key?

A. MAC (Message Authentication Code)

B. Digital Signature

C. Nonce

D. Initialization Vector (IV)

A Message Authentication Code uses a secret key to verify data integrity and authenticity by producing a short tag from the message and the shared key. The recipient, who also knows the secret key, recomputes the MAC on the received data and checks the tag; if they match, the data hasn't been altered and likely came from someone who possesses the key. This relies on a shared secret, so verification is limited to trusted parties who know the key. This is different from a digital signature, which uses public/private keys and allows anyone with the public key to verify the signature, providing non-repudiation. Nonces prevent replay, and initialization vectors randomize encryption; neither serves as a secret-key-based integrity/authenticity tag.

7. Which statement best describes AEAD modes like GCM?

A. They provide confidentiality and integrity for the ciphertext and associated data

B. They provide only confidentiality

C. They provide only integrity

D. They provide key management

AEAD modes like GCM combine encryption with authentication, giving both secrecy for the message and a way to verify that the message and any related data haven't been tampered with. The ciphertext remains confidential, and an authentication tag ensures integrity for the ciphertext as well as for any associated data that's processed together with it. That combination—confidentiality plus integrity for both the encrypted data and the associated data—best fits what AEAD modes provide. They don't merely offer confidentiality, nor only integrity, and key management is a separate concern from the mode itself.

8. What is the main purpose of triple-DES (3DES)?

A. Increase effective key length and security against brute-force

B. Faster than DES

C. Provide hashing

D. Provide authenticated encryption

Triple-DES aims to boost the strength of DES by running the algorithm three times with up to three keys, dramatically increasing the key length and making brute-force attacks far more difficult. DES uses a 56-bit key, which can be cracked with enough power; by encrypting with K1, decrypting with K2, and encrypting with K3, the effective key material becomes up to 168 bits, greatly enlarging the key space. This substantial increase in key length is the main benefit, trading off speed for security since 3DES must perform three DES operations for each block, making it much slower than DES. It does not provide hashing or built-in authentication; additional mechanisms would be needed for integrity or authenticity.

9. Which term is described as the process of converting plaintext into ciphertext?

A. Cipher

B. Plaintext

C. Ciphertext

D. Key

When you convert readable data into coded data, you're performing encryption. The tool that carries out that transformation is called a cipher—the algorithm or method that defines how plaintext becomes ciphertext. So, in this context, the term that describes the mechanism used to turn plaintext into ciphertext is cipher. The other terms refer to what you start with (plaintext) and what you end up with (ciphertext), or the secret parameter that guides the transformation (the key). Thus, cipher is the best fit for describing the process in this question.

10. Which mode turns a block cipher into a stream cipher?

A. AES

B. CBC Mode

C. CFB Mode

D. ECB Mode

Cipher Feedback mode uses the block cipher to generate a keystream and XORs that keystream with the plaintext, effectively turning the block cipher into a stream cipher. It does this by maintaining a shifting register that starts with an initialization vector. You encrypt the contents of that register with the block cipher to produce a keystream block, take the leftmost s bits of that keystream, and XOR them with the next s bits of plaintext to produce ciphertext. The register is then updated by shifting in the produced ciphertext, and the process repeats for the next segment. Because you can operate on small segments (bits or bytes) rather than fixed blocks, the cipher behaves like a stream cipher and doesn't require padding. Other modes operate on whole blocks and don't provide this continuous keystream generation with feedback, so they don't turn the block cipher into a stream cipher.

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!