CCYS-001

CERTLABZ CERTIFICATION BOARD

Certified Cryptography Specialist (CCYS)

Exam Objectives CCYS-001

About the exam

Item	Detail
Level	Advanced
Number of questions	120. A performance-based exam: each form can carry up to 5 to 12 performance-based questions alongside the multiple-choice questions.
Delivery model	Computer adaptive in 3 stages of 42, 39, 39 questions. Your score on each stage selects the difficulty of the next, so no two candidates sit the same paper.
Time limit	180 minutes
Scoring	You need a score of 700 out of 900 to pass. Results are reported on a scale of 100 to 900, and 700 corresponds to answering 72% of the exam correctly. Harder questions carry more weight, so a score means the same thing on any route. Multiple-response items and PBQs are scored all or nothing.
Delivery	Online, fully proctored (webcam, microphone and screen).
Prerequisites	No formal prerequisite. Candidates do best with two years in software or security work and 50 to 80 hours of study.
Retakes	No waiting period after a failed first attempt. Candidates pay the exam price each time they attempt the exam. See the CertLabz Certification Retake Policy at certlabz.com/certification-retake-policy.html
Validity	3 years. Renew with 75 CEUs per cycle and the $55 annual continuing-education fee, or by passing the current exam.
Language	English
Exam voucher	$199 for one sitting, valid 12 months. Bundles add the study guide ebook and the All Access plan.

Domain weights

Domain	Questions
D1 Cryptographic Foundations (16%)	19
D2 Symmetric Cryptography and Modes (16%)	19
D3 Asymmetric Cryptography and Key Exchange (17%)	21

D4 PKI, Certificates and Trust (17%)

	21
D5 Protocols and Applied Cryptography (17%)	20
D6 Key Management, Governance and Crypto Agility (17%)	20
Total (100%)	**120**

Objectives by domain

Each objective may appear as knowledge, a scenario to judge, a circuit to trace or assemble, or a number to compute. Each form can carry up to 5 to 12 performance-based questions: drag-and-drop matching, sequencing and table completion, drawn fresh each attempt. The exam does not test any vendor's SDK syntax.

D1 Cryptographic Foundations — 16% — 19 questions

D1.1 Confidentiality, integrity, authenticity, non-repudiation
D1.2 Kerckhoffs's principle and computational security
D1.3 Hash functions, the birthday bound and collision resistance
D1.4 Randomness, nonces and IVs
D1.5 Password hashing with salts and slow KDFs
D1.6 Security strength and why not to roll your own

D2 Symmetric Cryptography and Modes — 16% — 19 questions

D2.1 AES and ChaCha20; retired ciphers
D2.2 ECB, CBC, CTR and why mode matters
D2.3 AEAD: GCM and ChaCha20-Poly1305
D2.4 Nonce reuse, IV predictability and key limits
D2.5 HMAC, KDFs and encrypt-then-MAC
D2.6 Padding oracles and constant-time code

D3 Asymmetric Cryptography and Key Exchange — 17% — 21 questions

D3.1 RSA, elliptic curves and key sizes
D3.2 Diffie-Hellman, ECDHE and forward secrecy
D3.3 Signatures: ECDSA, Ed25519, RSA-PSS and nonce hazards
D3.4 Padding: OAEP versus PKCS#1 v1.5
D3.5 Hybrid encryption and KEMs
D3.6 Post-quantum: ML-KEM, ML-DSA, SLH-DSA and harvest-now-decrypt-later

D4 PKI, Certificates and Trust — 17% — 21 questions

D4.1 X.509, chains and trust anchors
D4.2 CSRs, SANs and name validation
D4.3 Revocation: CRL, OCSP and stapling
D4.4 Offline roots, intermediates and HSMs
D4.5 Certificate Transparency, pinning and short lifetimes
D4.6 ACME automation, code signing and workload identity

D5 Protocols and Applied Cryptography — 17% — 20 questions

D5.1 TLS 1.2 and 1.3 handshake and cipher suites
D5.2 SSH host keys and end-to-end encryption
D5.3 JWTs, webhooks and constant-time comparison
D5.4 Data at rest: disk, envelope and field-level encryption
D5.5 Secrets management, KMS and HSMs
D5.6 Recognizing misuse in real code

D6 Key Management, Governance and Crypto Agility — 17% — 20 questions

D6.1 The key lifecycle and rotation
D6.2 Separation of duties, ceremonies and custody
D6.3 Cryptographic inventory and deprecation
D6.4 FIPS 140-3 and PCI DSS key controls
D6.5 Crypto agility and post-quantum migration planning
D6.6 Key separation, escrow and destruction

Continuing education

Renewal	Requirement
Validity	3 years from the date of issue
CEUs required per cycle	75
Annual CE fee	$55
Alternative to CEUs	Pass the current version of the exam before the expiry date

Qualifying activities

Activity	CEUs
CertLabz labs, PBQs, courses and SkillTracker assessments	1 CEU per hour, up to 25 per cycle
Other industry certifications earned or renewed	10 to 25 each, depending on level
Conferences, webinars and training	1 CEU per hour, up to 20 per cycle
Cryptography, PKI or security engineering work experience	3 per year, up to 9 per cycle
Teaching, mentoring, publishing or open-source contributions	Up to 15 per cycle
College courses in mathematics, security or computing	10 per completed course

CertLabz Certification Retake Policy

- **No waiting period after a failed first attempt:** If you fail your first attempt at any CertLabz certification examination, CertLabz does not require any waiting period between the first and second attempt.
- **Once you pass, you cannot resit the same exam code:** A candidate who has passed an exam and achieved a certification cannot take that exam again under the same exam code without prior consent from CertLabz. You will need to wait until a new series of the exam is published before attempting to recertify by examination.
- **Beta examinations, one attempt only:** A CertLabz beta examination may be taken one time by each candidate.
- **Violations invalidate the attempt:** A test found to be in violation of this policy will be invalidated, and the candidate may be subject to a suspension period. Repeat violators will be permanently banned from the CertLabz Certification Program.
- **Every attempt is paid for:** Candidates must pay the exam price each time they attempt the exam. CertLabz does not offer free retests or discounts on retakes.

Published by the CertLabz Certification Board, a division of CertLabz LLC. Objectives document CCYS-001.
https://certlabz.com/certifications/certified-cryptography-specialist.html