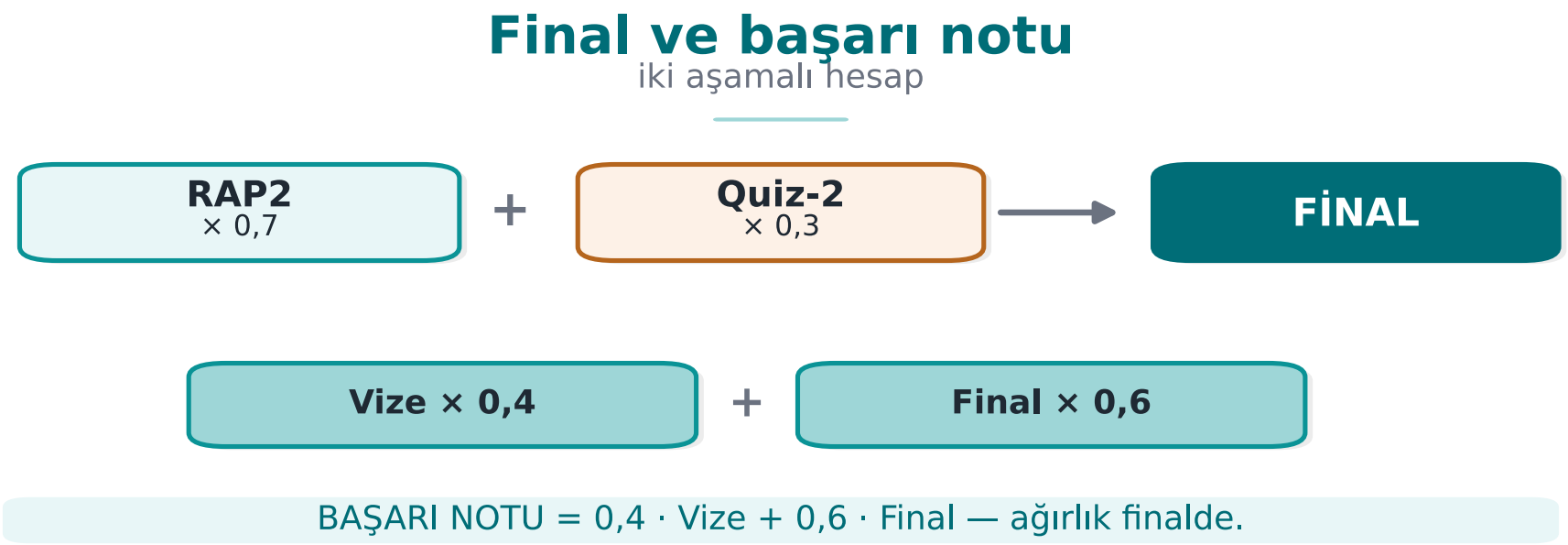
Final Exam Period: Quiz-2

CEN429 Secure Programming — Week 16

Asst. Prof. Dr. Uğur CORUH · 04–17.01.2027

Final and Course Passing Grade — Diagram



Quiz-2: What, When?

- Scope: **weeks 9–14** · **30%** of the final grade
- Date, time, place, duration, format: **announced in class**
- Best preparation: Self-check questions · Week 10 OpenSSL steps · Week 13 compliance matrix

Topic Map

Week	Focus
9	Purpose, cost, and measurement of obfuscation (potency, resilience, cost)
10	Security level · modes and padding · HMAC, EtM, replay · OAEP/PSS, Ed25519/X25519 · signature · DH · PKI, X.509 · CRL/OCSP · PKCS#11
11	White-box/black-box models · white-box's role and limits in layered defence
12	13 steps · requirement template · finding–action · impact analysis · delta assessment
13	Good requirement · compliance matrix · deferred requirements · CC, EAL · FIPS 140-3 · ETSI, EMVCo, PCI, MASVS
14	Purpose of diversification · measuring cost and effectiveness

Quiz-2 Scope — Diagram

Quiz-2 kapsamı (9–14. haftalar)

ortak soru: 'bu koruma neyi korur, neyi korumaz, maliyeti ne?'

Hafta 9	gizleme: beş aile, dört ölçüt, çeşitlendirme
Hafta 10	kip, dolgu, imza, PKI, zincir, iptal
Hafta 11	whitebox: üç model, kodlama, DCA, sınırlar
Hafta 12	değerlendirme süreci, saldırı potansiyeli, CVSS
Hafta 13	iyi gereksinim, izlenebilirlik, CC/FIPS/MASVS
Hafta 14	Tigress, dönüşüm hattı, dayanıklılık ↔ maliyet

Koruma = gecikme; güç katmandan ve ÖLÇÜMDEN gelir.

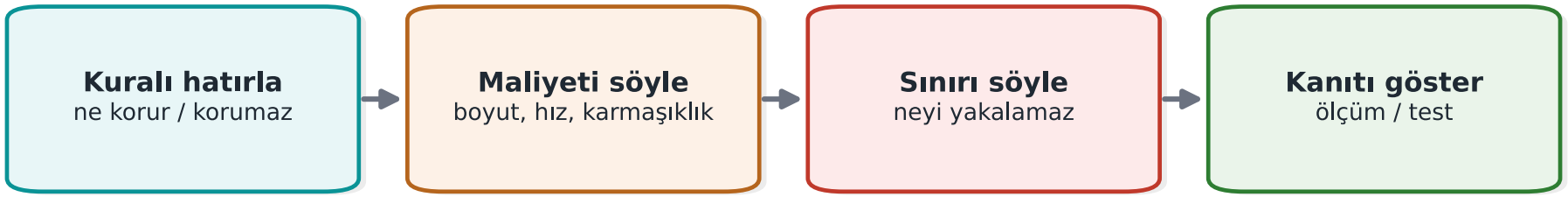
Frequently Confused

A	B	Difference
CBC	GCM	Confidentiality + padding · AEAD, no padding
OAEP	PSS	Encryption · signature
Ed25519	X25519	Signature · key agreement
CN	SAN	Name check → SAN
CRL	OCSP	List · live query
ST	PP	Security target · product class requirement set
EAL	Attack potential	Depth · attacker's resources
Met	Deferred	Product meets it · another party (who, why, how)
Impact analysis	Delta assessment	Documents · re-assesses only what changed

Answer Pattern — Diagram

Quiz-2'de beklenen cevap kalıbı

dört parçayı da söyleyen cevap tam puan alır



Bu kalıp aynı zamanda projenizin S9 ve S16 bölümlerinin yazım biçimidir.

Sample Questions (Week 10)

1. RSA-2048 + AES-256: security level?
2. "Padding invalid" vs. "MAC invalid" as separate messages: risk?
3. Why is `if (EVP_DigestVerify(...))` wrong?
4. Why does `verify` fail without the intermediate certificate?
5. Accepting when OCSP is unreachable: which pattern?
6. What protects against unauthenticated DH?

Sample Questions (Weeks 12–13)

7. Why must the TOE be uniquely defined?
8. Relationship between impact analysis and delta assessment?
9. How is "the application must be secure" fixed?
10. What does "met" without evidence mean?
11. If a library cannot meet the secure-update requirement?
12. Is EAL4+ always more secure than EAL2?
13. Does a FIPS-validated library mean the application is FIPS compliant?

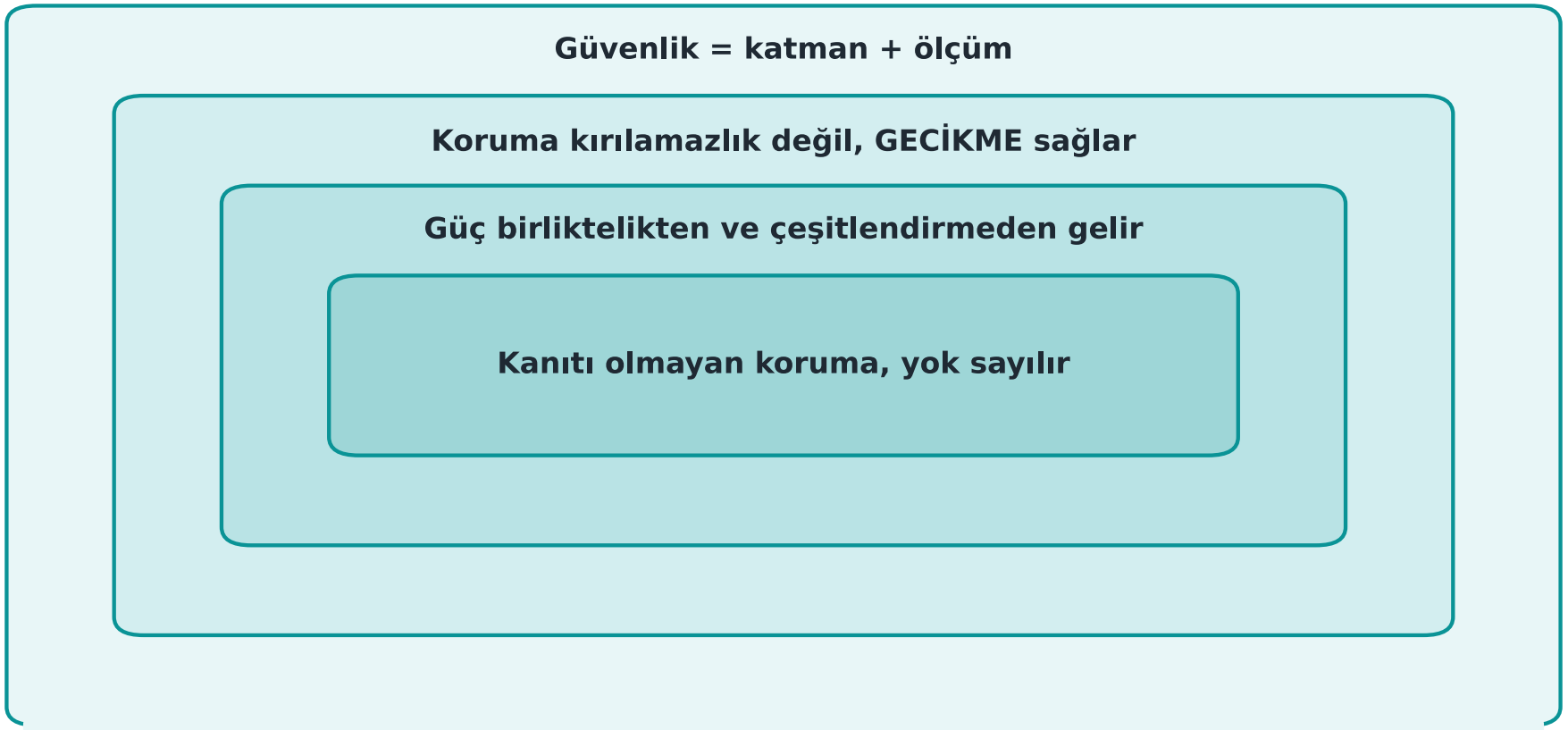
Good Luck

- Answers on the Week 16 page
- Your guide is a **portfolio** item (make sure it contains no confidential information)

The Term in One Sentence — Diagram

Dönemin tek cümlesi

16 haftanın özeti



Bu dört cümle, her hafta farklı bir teknikle tekrar edildi.

Appendix · Week-by-Week Topic Map (9–14)

Week 9 · Key Points

- Obfuscation: not unbreakability, but **cost**.
- Techniques: opaque predicates, control-flow flattening, bogus/dead code, data encoding.
- Measurement: potency, resilience, stealth, cost.
- Diversification.

Week 10 · Key Points

- Security level; weakest link.
- Modes and padding; padding oracle → AEAD.
- HMAC, encrypt-then-MAC, replay.
- OAEP/PSS, Ed25519/X25519; PKI, X.509, CRL/OCSP.

Week 11 · Key Points

- Black/gray/white box.
- Table-based WBC; internal/external encoding.
- "All broken" → WBC is one layer.
- Key renewal + device binding + server.

Week 12 · Key Points

- 13-step assessment.
- Attack potential + CVSS.
- Penetration test plan; test card.
- Impact analysis vs. delta.

Week 13 · Key Points

- Good requirement; traceability.
- Compliance matrix; deferred requirements.
- CC (TOE/ST/PP/SFR/SAR/EAL); FIPS 140-3.
- ETSI/EMVCo/PCI/MASVS.

Week 14 · Key Points

- Source-to-source (Tigress).
- Transformation pipeline; seed-based diversification.
- Cost + resilience measurement.
- Build pipeline (S15).

Frequently Confused

A	B	Difference
CBC	GCM	Padding / AEAD
OAEP	PSS	Encryption / signature
Ed25519	X25519	Signature / key
EAL	Attack potential	Depth / attacker resources
Met	Deferred	Product / another party
Impact analysis	Delta	Documents / re-assesses only what changed

Appendix · Solved Practice (9, 11, 14)

Question · Week 9

Difference between bogus code and dead code?

Answer: Bogus code executes but doesn't change the result; dead code with an opaque predicate never executes. Both hide the real logic.

Question · Week 9

The four dimensions that measure obfuscation? Which ones trade off?

Answer: Potency, resilience, stealth, cost. As potency/resilience increase, cost increases and stealth decreases.

Question · Week 11

How does "all published pure-software WBCs have been broken" affect your decision?

Answer: WBC alone cannot count as key assurance; combine with renewal + device binding + server checks + obfuscation; move to hardware where possible.

Question · Week 11

Which hardware attack does DCA resemble?

Answer: DPA (power analysis); it applies statistics to software traces and often defeats internal encoding.

Question · Week 14

Two things that must always be done after a transformation pipeline?

Answer: Unit tests (is behaviour preserved?) and size/speed measurement (cost).

Question · Week 14

What does the seed (`--Seed`) provide?

Answer: Diversification; the same transformations produce a different binary with a different seed, so an attack written against one copy won't work on another.

Question · Week 10

The four questions of chain validation?

Answer: Is the signature valid, does it reach a trusted root, has it not expired, does the name (SAN) match.

Question · Weeks 12–13

Is "EAL4+ is always more secure" true?

Answer: No; EAL is depth, security depends on the threats and objectives in the ST.

Example · Multiple Choice

What is the limit of external encoding (F,G) in white-box cryptography?

A) Too slow B) **Not standard AES** ✓ C) Table too small D) Key exposed

Study Plan

- Do the solved practice items on the Week 9, 11, and 14 pages.
- Review the Week 10 OpenSSL steps.
- Fill in the Week 13 compliance matrix activity yourself.

Final Word (Quiz-2 Prep)

> Protection = **delay**; strength comes from layering and **measurement**. Reasoning is measured, not memorized.

Good luck.