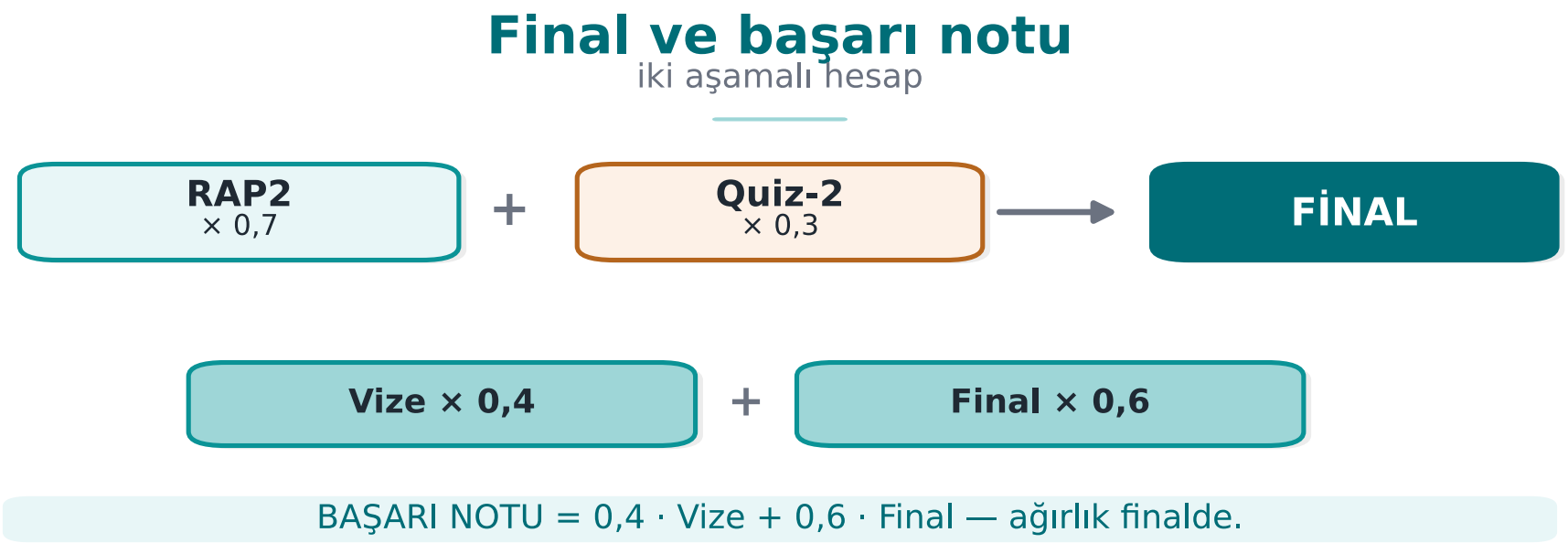
Final Dönemi: Quiz-2

CEN429 Güvenli Programlama — Hafta 16

Dr. Öğr. Üyesi Uğur CORUH · 04–17.01.2027

Final ve başarı notu — şema



Quiz-2: ne, ne zaman?

- Kapsam: **9–14. haftalar** · finalin **%30**'u
- Tarih, saat, yer, süre, biçim: **ders sınıfında**
- En iyi hazırlık: Kendini sınama soruları · 10. hafta OpenSSL adımları · 13. hafta uyum matrisi

Konu haritası

Hafta	Odak
9	Gizlemenin amacı, maliyeti, ölçülmesi (güç, dayanıklılık, maliyet)
10	Güvenlik düzeyi · kip ve dolgu · HMAC, EtM, yeniden oynatma · OAEP/PSS, Ed25519/X25519 · imza · DH · PKI, X.509 · CRL/OCSP · PKCS#11
11	Beyaz/kara kutu modelleri · whitebox'ın katmanlı savunmadaki yeri ve sınırları
12	13 adım · gereksinim şablonu · bulgu–aksiyon · etki analizi · delta değerlendirme
13	İyi gereksinim · uyum matrisi · devredilenler · CC, EAL · FIPS 140-3 · ETSI, EMVCo, PCI, MASVS
14	Çeşitlendirmenin amacı · maliyet ve etkinlik ölçümü

Quiz-2 kapsamı — şema

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.

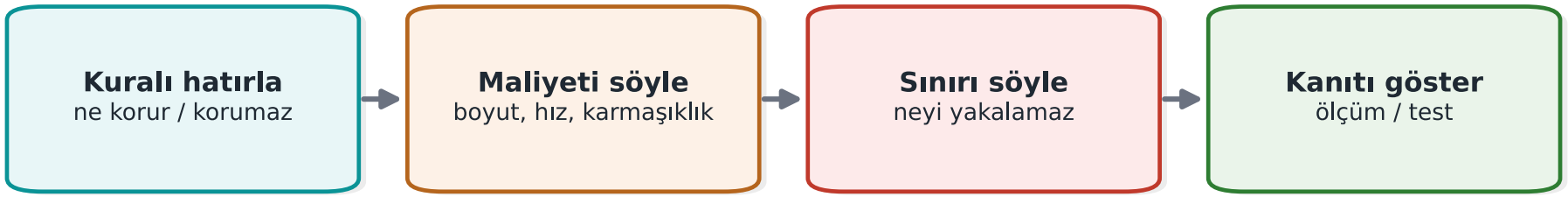
Sık karıştırılanlar

A	B	Fark
CBC	GCM	Gizlilik + dolgu · AEAD, dolgu yok
OAEP	PSS	Şifreleme · imza
Ed25519	X25519	İmza · anahtar anlaşması
CN	SAN	Ad denetimi SAN'a
CRL	OCSP	Liste · anlık sorgu
ST	PP	Ürün hedefi · ürün sınıfı seti
EAL	Saldırı potansiyeli	Derinlik · saldırganın kaynağı
Karşılandı	Devredildi	Ürün karşılar · başka taraf (kime, neden, nasıl)
Etki analizi	Delta değerlendirme	Belgeler · yalnız değişeni değerlendirir

Cevap kalıbı — şema

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.

Örnek sorular (10. hafta)

1. RSA-2048 + AES-256: güvenlik düzeyi?
2. "Dolgu geçersiz" ile "MAC geçersiz" ayrı iletiler: risk?
3. `if (EVP_DigestVerify(...))` neden hatalı?
4. `verify` ara sertifika olmadan neden başarısız?
5. OCSP'ye ulaşamayınca kabul: hangi örüntü?
6. Kimliksiz DH'ye karşı ne yapılır?

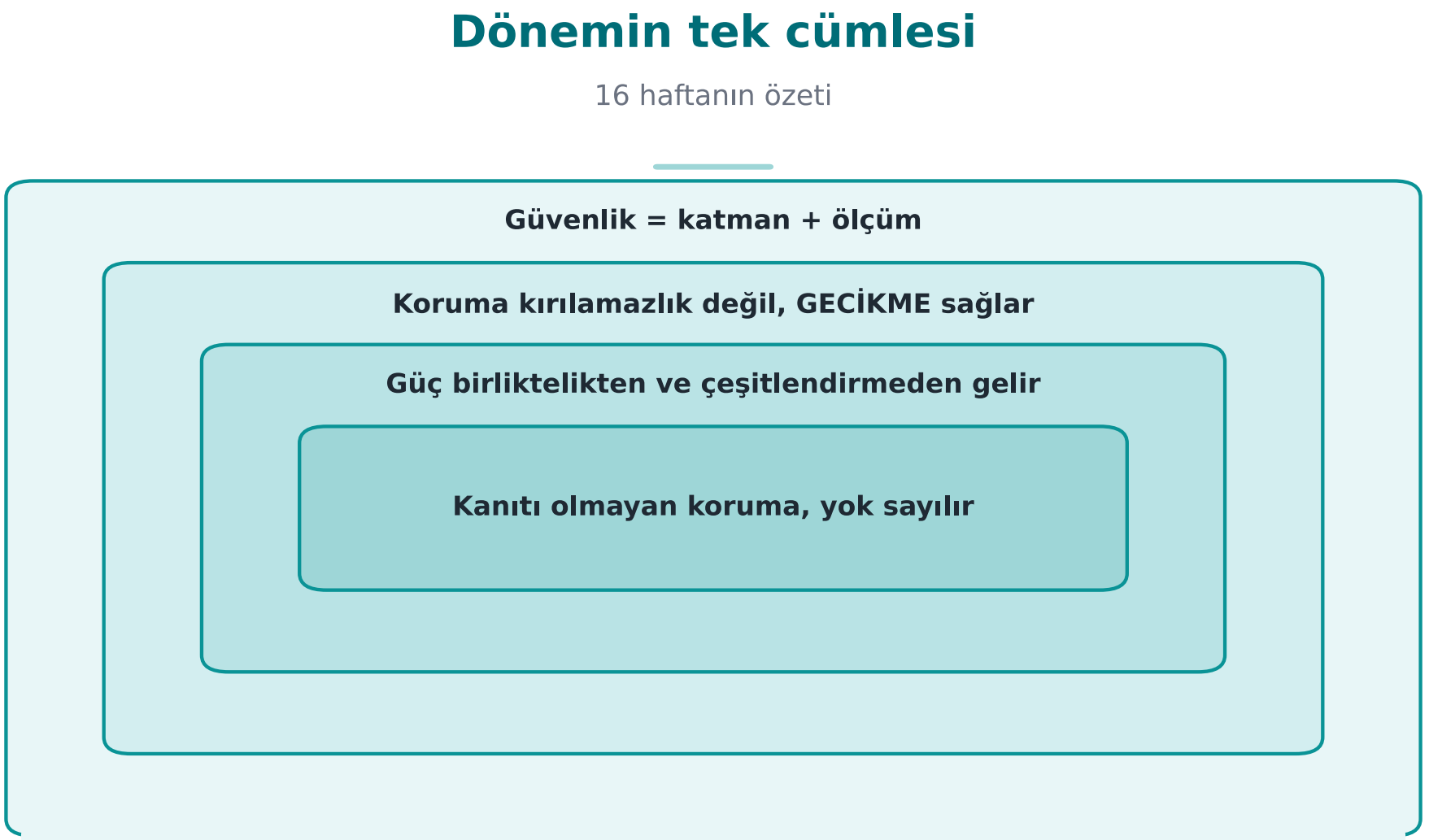
Örnek sorular (12–13. haftalar)

7. TOE neden benzersiz tanımlanır?
8. Etki analizi ile delta değerlendirme ilişkisi?
9. "Uygulama güvenli olmalıdır" nasıl düzeltilir?
10. Kanıtsız "karşılandı" ne anlama gelir?
11. Kütüphane güvenli güncellemeyi karşılayamıyorsa?
12. EAL4+ her zaman EAL2'den güvenli mi?
13. FIPS doğrulanmış kütüphane = uygulama FIPS uyumlu mu?

İyi şanslar

- Cevapları 16. hafta sayfasında
- Kılavuzunuz bir **portfolyo** öğesidir (gizli bilgi içermediğinden emin olun)

Dönemin tek cümlesi — şema



Ek · Hafta hafta konu haritası (9–14)

9. hafta · anahtar noktalar

- Gizleme: kırılamazlık değil **maliyet**.
- Kurallar: opak yüklem, düzleştirme, sahte/ölü, veri kodlama.
- Ölçme: güç, dayanıklılık, gizlilik, maliyet.
- Çeşitlendirme.

10. hafta · anahtar noktalar

- Güvenlik düzeyi; en zayıf halka.
- Kip ve dolgu; dolgu kâhini → AEAD.
- HMAC, encrypt-then-MAC, replay.
- OAEP/PSS, Ed25519/X25519; PKI, X.509, CRL/OCSP.

11. hafta · anahtar noktalar

- Kara/gri/beyaz kutu.
- Tablo tabanlı WBC; iç/dış kodlama.
- "Hepsi kırıldı" → WBC bir katman.
- Anahtar yenileme + cihaz bağlama + sunucu.

12. hafta · anahtar noktalar

- 13 adım değerlendirme.
- Saldırı potansiyeli + CVSS.
- Sızma testi planı; test kartı.
- Etki analizi vs delta.

13. hafta · anahtar noktalar

- İyi gereksinim; izlenebilirlik.
- Uyum matrisi; devredilenler.
- CC (TOE/ST/PP/SFR/SAR/EAL); FIPS 140-3.
- ETSI/EMVCo/PCI/MASVS.

14. hafta · anahtar noktalar

- Kaynaktan kaynağa (Tigress).
- Dönüşüm hattı; tohumla çeşitlendirme.
- Maliyet + dayanıklılık ölçümü.
- Derleme hattı (S15).

Sık karıştırılanlar

A	B	Fark
CBC	GCM	Dolgu / AEAD
OAEP	PSS	Şifre / imza
Ed25519	X25519	İmza / anahtar
EAL	Saldırı potansiyeli	Derinlik / saldırgan kaynağı
Karşılandı	Devredildi	Ürün / başka taraf
Etki analizi	Delta	Belgeler / yalnız değişeni değerlendirir

Ek · Çözümlü pratik (9, 11, 14)

Soru · 9. hafta

Sahte işlem ile ölü dal farkı?

Cevap: Sahte işlem çalışır ama sonucu değiştirmez; ölü dal opak yüklemle hiç çalışmaz. İkisi de gerçek mantığı gizler.

Soru · 9. hafta

Gizlemeyi ölçen dört boyut? Hangileri ödünleşir?

Cevap: Güç, dayanıklılık, gizlilik, maliyet. Güç/dayanıklılık artarken maliyet artar, gizlilik azalır.

Soru · 11. hafta

"Yayımlanmış saf-yazılım WBC'lerin hepsi kırıldı" kararınızı nasıl etkiler?

Cevap: WBC tek başına anahtar güvencesi sayılamaz; yenileme + cihaz bağlama + sunucu denetimi + gizleme ile; mümkünse donanıma taşı.

Soru · 11. hafta

DCA hangi donanım saldırısına benzer?

Cevap: DPA'ya (güç analizi); yazılım izlerine istatistik uygular, iç kodlamayı çoğu zaman aşar.

Soru · 14. hafta

Bir dönüşüm hattından sonra mutlaka yapılacak iki şey?

Cevap: Birim testleri (davranış korunmuş mu?) ve boyut/hız ölçümü (maliyet).

Soru · 14. hafta

Tohum (`--Seed`) ne sağlar?

Cevap: Çeşitlendirme; aynı dönüşümler farklı tohumla farklı ikili üretir, bir kopyaya yazılan saldırı diğerinde çalışmaz.

Soru · 10. hafta

Zincir doğrulamanın dört sorusu?

Cevap: İmza geçerli mi, güvenilir köke ulaşıyor mu, süre dolmamış mı, ad (SAN) eşleşiyor mu.

Soru · 12–13. hafta

"EAL4+ her zaman daha güvenli" doğru mu?

Cevap: Hayır; EAL derinliktir, güvenlik ST'deki tehdit ve amaçlara bağlı.

Örnek · çoktan seçmeli

Whitebox kriptografide dış kodlamanın (F,G) sınırı nedir?

A) Çok yavaş B) **Standart AES değil** ✓ C) Tablo küçük D) Anahtar açık

Çalışma planı

- 9, 11, 14. hafta sayfalarındaki çözümlü sınamaları yap.
- x. haftanın OpenSSL adımlarını tekrar et.
- xiii. haftanın uyum matrisi etkinliğini kendin doldur.

Son söz (Quiz-2 hazırlık)

> Koruma = **gecikme**; güç katmandan ve **ölçümden**. Ezber değil, gerekçe ölçülür.

İyi şanslar.