

# CEN429 GÃ¼venli Programlama Hafta-10

## Beyaz Kutu Kriptografisi

Yazar: Dr. A. Y. A. Coeyesi U. Y. Coruh

## İçindekiler

<b>1 CEN429 GÃ¼venli Programlama</b>	<b>1</b>
1.1 Hafta-10	1
1.1.1 Outline	1
1.1.2 Hafta-10: Beyaz Kutu Kriptografisi	1
1.1.3 SonuÅŸ	4

## Åekil Listesi

## Tablo Listesi

## 1 CEN429 GÃ¼venli Programlama

### 1.1 Hafta-10

#### 1.1.0.1 Beyaz Kutu Kriptografisi Åndir

- PDF<sup>1</sup>
- DOC<sup>2</sup>
- SLIDE<sup>3</sup>
- PPTX<sup>4</sup>

#### 1.1.1 Outline

- Beyaz Kutu Kriptografisi Nedir?
- Beyaz Kutu Åzifreleme YÅntemleri
- Uygulama AlanlarÅ± ve Tehditler

#### 1.1.2 Hafta-10: Beyaz Kutu Kriptografisi

Bu hafta, Åzifreleme iÅylemlerinin aÅŸÅk sistemlerde gÃ¼venli bir Åyekilde nasÅ±l uygulandÅ±Å±nÅ± inceleyen Beyaz Kutu Kriptografisi'ni ele alacaÅ±z. Beyaz kutu kriptografisi, Åzelleme dijital hak yÅnetimi (DRM) ve mobil uygulamalarda veri gÃ¼venliÅ±ini saÅ±lamak iÅŸin Ånemli bir tekniktir.

**1.1.2.1 1. Beyaz Kutu Kriptografisinin Temelleri Teorik AÅŸÅklama:** Beyaz kutu kriptografisi, Åzelleme saldÅrganÅ±n sistemin tÅ¼m kaynaklarÅ±na eriÅ±imi olduÅ±u durumlarda gÃ¼venliÅ±i saÅ±lamak amacÅ±yla geliÅtirilmiÅtir. Buradaki temel amaÅŸ, Åzifreleme anahtarlarÅ±nÅ± ve iÅylemlerini dÅ±ÅrÅ±dan gelebilecek saldÅrÅ±lara karÅ± gizli tutmaktÅ±r.

<sup>1</sup>pandoc\_cen429-week-10.pdf

<sup>2</sup>pandoc\_cen429-week-10.docx

<sup>3</sup>cen429-week-10.pdf

<sup>4</sup>cen429-week-10.pptx

Saldırrgan, sistem üzerinde kodu analiz edebilir, belleği okuyabilir ve şifreleme işlemlerini takip edebilir. Beyaz kutu kriptografi, bu durumlarda bile güvenli saılayacak teknikler sunar.

- **Kara Kutu Modeli (Blackbox):** Anahtar ve veri, şifreleme işlemi sırasında sistemde gizli kalır. Saldırrganın şifreleme algoritmasına erişimi yoktur.
- **Beyaz Kutu Modeli (Whitebox):** Saldırrgan sistemde tam erişime sahiptir. Şifreleme algoritması ve anahtarlar saldırrgan tarafından güvenli olarak elde edilir.

#### Uygulama Örnekleri:

1. Beyaz kutu ortamında bir şifreleme algoritmasının nasıl gizlenebileceğini analiz etmek.
2. Kara kutu ve beyaz kutu modelleri arasındaki farkları karşılaştırarak açıklamak.

**1.1.2.2 2. Beyaz Kutu Şifreleme Yöntemleri Teorik Açıklama:** Beyaz kutu şifreleme, özellikle simetrik şifreleme algoritmaları için kullanılır. Beyaz kutu ortamında şifreleme yapılırken, şifreleme anahtarının bellekten çıkarılması veya tahmin edilmesi zorlaştırılır.

- **Whitebox AES:** AES şifreleme algoritmasının, beyaz kutu ortamlarında güvenli bir şekilde uygulanması saılar.
- **Whitebox DES:** DES algoritmasının benzer şekilde beyaz kutu güvenli işi saılanması hali.

#### Uygulama Örnekleri:

1. **Whitebox AES** ile bir metni şifreleme ve işleme işlemi.
2. **Whitebox DES** kullanarak verilerin şifrelenmesi ve şifre çözülmesi.

**1.1.2.3 3. Whitebox AES ve DES Teorik Açıklama:** AES ve DES, simetrik şifreleme algoritmalarıdır. Beyaz kutu uygulamalarında, bu algoritmaların iş yapışları gizlemek için çeşitli teknikler kullanılır.

- **Whitebox AES:** Normalde güvenli bir ortamda çalıştırılan AES algoritması, saldırrganın belleğe ve koda erişebileceği durumlarda dahi anahtarları gizli tutacak şekilde değiştirilerek çalıştırılır. Bu, değiştirilmiş tablosu kullanılarak yapılır.
- **Whitebox DES:** DES algoritmasında da benzer bir yaklaşım izlenir, ancak AES'e göre daha düşük güvenlik seviyelerine sahiptir.

#### Uygulama Örnekleri:

1. Whitebox AES algoritmasının nasıl çalıştırılarak analiz edilip analiz edilmediği analiz etmek.
2. Whitebox DES'in yarıklarını ve güvenlik açıklarını tartışma.

**1.1.2.4 4. Beyaz Kutu Kriptografisinde Kullanılan Teknikler Teorik Açıklama:** Beyaz kutu kriptografisi, saldırrganın anahtarları elde etmesini zorlaştıran çeşitli teknikler kullanılır.

- **Tablo Dönüşümü (Table Lookups):** Anahtar işlemleri, tabloya dayalı dönüşümlerle gerçekleştirilir ve böylece anahtarlar kod içinde saklanmaz.
- **Obfuscation:** Kodun karmaşıklığı artırılarak, şifreleme işlemlerinin izlenmesini zorlaştırılır.
- **Çoklu Maskeler (Multiple Masking):** Anahtarlar, birden fazla maskeleyme katmanıyla korunur, böylece saldırrganın tek bir anahtar ele geçmesi yeterli olmaz.

#### Uygulama Örnekleri:

1. **Tablo Dönüşümü** yöntemi ile şifreleme işlemi beyaz kutuda nasıl güvenli hale getirebiliriz?
2. **Obfuscation** teknikleri kullanarak şifreleme algoritmasını karmaşıklığı artırma.

**1.1.2.5 5. Beyaz Kutu Kriptografisinde G $\frac{1}{4}$ venlik Tehditleri Teorik A $\frac{1}{2}$ klama:** Beyaz kutu kriptografisi, tam g $\frac{1}{4}$ venlik sunamayabilir ve  $\frac{1}{2}$ itli sald $\pm$ r $\pm$  t $\frac{1}{4}$ rlerine kar $\frac{1}{2}$  savunmas $\pm$  kalabilir.

- **Yan Kanal Sald $\pm$ r $\pm$ lar $\pm$  (Side-Channel Attacks):** Sald $\pm$ rgan,  $\frac{1}{2}$ ifreleme i $\frac{1}{2}$ lemi s $\pm$ ras $\pm$ nda enerji t $\frac{1}{4}$ ketimi, elektromanyetik yay $\pm$ l $\pm$ m veya zamanlama bilgilerini analiz ederek  $\frac{1}{2}$ ifreleme anahtarlar $\pm$ n $\pm$  elde etmeye  $\frac{1}{2}$ al $\pm$ abilir.
- **Kapsaml $\pm$  Sald $\pm$ r $\pm$ lar (Brute Force):** T $\frac{1}{4}$ m olas $\pm$  anahtar kombinasyonlar $\pm$ n $\pm$  deneyerek do $\frac{1}{2}$ ru anahtar $\pm$  bulmaya  $\frac{1}{2}$ al $\pm$ Yan sald $\pm$ r $\pm$ lard $\pm$ .
- **Differential Fault Analysis (DFA):** Sald $\pm$ rgan,  $\frac{1}{2}$ ifreleme i $\frac{1}{2}$ lemi s $\pm$ ras $\pm$ nda bellek veya i $\frac{1}{2}$ lemcide k $\frac{1}{4}$  $\frac{1}{2}$  hatalar olu $\frac{1}{2}$ turarak,  $\frac{1}{2}$ ifre  $\frac{1}{2}$ zme s $\frac{1}{4}$ recini manip $\frac{1}{4}$ le eder ve anahtar bilgilerini elde edebilir.

**Uygulama  $\frac{1}{2}$ rneklere:**

1. Yan kanal sald $\pm$ r $\pm$ lar $\pm$ na kar $\frac{1}{2}$  beyaz kutu ortam $\pm$ nda nas $\pm$ l koruma sa $\frac{1}{2}$ lanabilir?
2. Brute force sald $\pm$ r $\pm$ lar $\pm$ n etkilerini ve korunma y $\frac{1}{2}$ ntemlerini analiz etme.

**1.1.2.6 6. G $\frac{1}{4}$ venlik Kapsam $\pm$ nda Beyaz Kutu Kriptografisinin Avantaj ve Dezavantajlar $\pm$  Teorik A $\frac{1}{2}$ klama:** Beyaz kutu kriptografisi, dijital hak y $\frac{1}{2}$ netimi ve mobil uygulamalarda s $\pm$ k $\frac{1}{2}$  kullan $\pm$ lsa da, her durumda m $\frac{1}{4}$ kemmel bir  $\frac{1}{2}$ z $\frac{1}{4}$ m sunmaz. Avantajlar ve dezavantajlar  $\frac{1}{2}$ unlard $\pm$ :

- **Avantajlar:**
  - Sald $\pm$ rgan $\pm$ n t $\frac{1}{4}$ m sisteme eri $\frac{1}{2}$ imi oldu $\frac{1}{2}$ u durumlarda dahi g $\frac{1}{4}$ venlik sa $\frac{1}{2}$ lar.
  - Dijital hak y $\frac{1}{2}$ netimi (DRM) gibi uygulamalarda yayg $\pm$ n olarak kullan $\pm$ l $\pm$ .
- **Dezavantajlar:**
  - Yan kanal sald $\pm$ r $\pm$ lar $\pm$  gibi  $\frac{1}{2}$ itli sald $\pm$ r $\pm$  t $\frac{1}{4}$ rlerine kar $\frac{1}{2}$  hala savunmas $\pm$ z olabilir.
  - Performans a $\frac{1}{2}$ s $\pm$ ndan maliyetli olabilir,  $\frac{1}{2}$ nk $\frac{1}{4}$  ek maskeler ve d $\frac{1}{2}$ n $\frac{1}{4}$  $\frac{1}{2}$ mlerle i $\frac{1}{2}$ lem yap $\pm$ l $\pm$ .

**Uygulama  $\frac{1}{2}$ rneklere:**

1. Beyaz kutu kriptografisinin avantajlar $\pm$ n $\pm$  ve dezavantajlar $\pm$ n $\pm$  tart $\pm$ l $\pm$ .
2. Beyaz kutu ve kara kutu g $\frac{1}{4}$ venlik modellerinin kar $\frac{1}{2}$ la $\frac{1}{2}$ t $\pm$ lmas $\pm$ .

**1.1.2.7 7. Beyaz Kutu Kriptografisinin Uygulama Alanlar $\pm$  Teorik A $\frac{1}{2}$ klama:** Beyaz kutu kriptografisi,  $\frac{1}{2}$ itli uygulama alanlar $\pm$ nda kullan $\pm$ l $\pm$ :

- **Dijital Hak Y $\frac{1}{2}$ netimi (DRM):** M $\frac{1}{4}$ zik, film ve yaz $\pm$ l $\pm$ m gibi dijital i $\frac{1}{2}$ eriklerin korsan kullan $\pm$ m $\pm$ n $\pm$   $\frac{1}{2}$ nlemek i $\frac{1}{2}$ in kullan $\pm$ l $\pm$ .
- **Mobil Uygulama G $\frac{1}{4}$ venli $\frac{1}{2}$ :** Mobil cihazlarda  $\frac{1}{2}$ al $\pm$ Yan uygulamalarda,  $\frac{1}{2}$ zellikle finansal uygulamalarda hassas bilgilerin korunmas $\pm$ n $\pm$  sa $\frac{1}{2}$ lar.
- **IoT G $\frac{1}{4}$ venli $\frac{1}{2}$ :** Nesnelerin interneti (IoT) cihazlar $\pm$ nda veri g $\frac{1}{4}$ venli $\frac{1}{2}$ ini sa $\frac{1}{2}$ lamak i $\frac{1}{2}$ in kullan $\pm$ l $\pm$ .

**Uygulama  $\frac{1}{2}$ rneklere:**

1. DRM sistemlerinde beyaz kutu kriptografinin nas $\pm$ l kullan $\pm$ ld $\pm$  $\frac{1}{2}$ n $\pm$  inceleme.
2. Mobil uygulamalarda beyaz kutu kriptografinin uygulanmas $\pm$  ve test edilmesi.

**1.1.2.8 8. Beyaz Kutu Kriptografi Ara $\frac{1}{2}$ lar $\pm$  Teorik A $\frac{1}{2}$ klama:** Beyaz kutu kriptografisini uygulamak i $\frac{1}{2}$ in  $\frac{1}{2}$ itli ara $\frac{1}{2}$ lar ve k $\frac{1}{4}$ t $\frac{1}{4}$ phaneler kullan $\pm$ labilir. Bu ara $\frac{1}{2}$ lar,  $\frac{1}{2}$ ifreleme i $\frac{1}{2}$ lemlerini karma $\frac{1}{2}$ kl $\frac{1}{2}$ t $\pm$ rarak g $\frac{1}{4}$ venli $\frac{1}{2}$  art $\pm$ r $\pm$ .

- **Tigress:** C/C++ programlar $\pm$  i $\frac{1}{2}$ in obfuscation (kod karma $\frac{1}{2}$ kl $\frac{1}{2}$ t $\pm$ rma) ve beyaz kutu kriptografi teknikleri sa $\frac{1}{2}$ layan bir ara $\frac{1}{2}$ .
- **Whitebox Toolkits:** Beyaz kutu AES ve di $\frac{1}{2}$ er  $\frac{1}{2}$ ifreleme algoritmalar $\pm$ n $\pm$  uygulayan  $\frac{1}{2}$ itli a $\frac{1}{2}$ k kaynak ve ticari k $\frac{1}{4}$ t $\frac{1}{4}$ phaneler.

**Uygulama  $\frac{1}{2}$ rneklere:**

1. **Tigress** kullanarak bir Åifreleme algoritmasÄ±nÄ± karmaÅŸlaÅŸtÄ±rma.
2. Beyaz kutu kriptografi araÅŸlarÄ±yla basit bir uygulama geliÅŸtirme.

**1.1.2.9 9. Beyaz Kutu Kriptografisinde Gelecek YÄ¶nelimleri Teorik AÄŸÄ±klama:** Beyaz kutu kriptografisi, dijital hak yÄ¶netimi ve gÄ¼venli mobil uygulamalar iÅŸin kritik bir rol oynamaya devam ediyor. Gelecekte, beyaz kutu gÄ¼venlik tekniklerinin daha da geliÅŸtirilmesi ve yeni saldÄ±rÄ± tehditlerine karÅŸÄ± daha direnÅŸli hale getirilmesi bekleniyor.

- **Post-Kuantum Kriptografi:** Kuantum bilgisayarlarÄ±n ortaya ÅŸÄ±kmasÄ±yla birlikte, mevcut Åifreleme algoritmalarÄ±nÄ±n gÄ¼venliÄŸi sorgulanmaktadÄ±r. Beyaz kutu kriptografisi, bu yeni tehditlere karÅŸÄ± daha gÄ¼venli hale getirilmeye ÅŸalÄ±ÅŸlanÄ±yor.

#### **Uygulama Ä±rnekleri:**

1. Beyaz kutu kriptografisinin gelecekteki gÄ¼venlik tehditlerine karÅŸÄ± nasÄ±l geliÅŸtirilebileceÄŸini analiz etme.

#### **1.1.3 SonuÅŸ**

Bu hafta, beyaz kutu kriptografisinin temellerini, uygulama alanlarÄ±nÄ± ve gÄ¼venlik tehditlerine karÅŸÄ± nasÄ±l koruma saÄŸlandÄ±ÄŸÄ±nÄ± Ä¶ÄŸendik. Beyaz kutu kriptografisi, dijital iÅŸeriklerin ve hassas bilgilerin gÄ¼venliÄŸini saÄŸlamak iÅŸin Ä¶nemli bir araÅŸtÄ±r.