

CEN429 G venli Programlama Hafta-9

Sertifikalar ve  zifreleme Y ntemleri

Yazar: Dr.    r.   eyesi U  ur CORUH

  indekiler

1 CEN429 G�venli Programlama	1
1.1 Hafta-9	1
1.1.1 Outline	1
1.1.2 Hafta-9: Sertifikalar ve �zifreleme Y�ntemleri	1

 ekil Listesi

Tablo Listesi

1 CEN429 G venli Programlama

1.1 Hafta-9

1.1.0.1 Sertifikalar ve  zifreleme Y ntemleri  ndir

- PDF¹
- DOC²
- SLIDE³
- PPTX⁴

1.1.1 Outline

- Sertifikalar ve  zifreleme Y ntemleri
- Simetrik ve Asimetrik  zifreleme
- Dijital  mzalar ve Sertifika Y ntemi

1.1.2 Hafta-9: Sertifikalar ve  zifreleme Y ntemleri

Bu hafta, yaz l m g venli yi ve ileti iminde kullan lan  zifreleme y ntemleri ile sertifikalar n temel ilkelerini inceleyece iz. Hem asimetrik hem de simetrik  zifreleme algoritmalar n , dijital sertifikalar n nas l  sal  t    n  ve uygulama g venli ine nas l katkı sa lad klar n  ke fedece iz.

1.1.2.1 1.  zifreleme Y ntemlerinin Temelleri Teorik A   klama:  zifreleme, verilerin gizlili ini korumak ve yetkisiz eri imlere kar   koruma sa lamak amac yla kullan lan bir tekniktir.  zifreleme y ntemleri iki ana kategoriye ayr l r: simetrik ve asimetrik.

- **Simetrik  zifreleme:** Ayn  anahtar hem  zifreleme hem de  yfre    zme i lemlerinde kullan l r.  rne  algoritmalar: AES, DES.

¹[pandoc_cen429-week-9.tr_doc.pdf](#)

²[pandoc_cen429-week-9.tr_word.docx](#)

³[cen429-week-9.tr_slide.pdf](#)

⁴[cen429-week-9.tr_slide.pptx](#)

- **Asimetrik Ğifreleme:** Ğki farklı anahtar kullanılır. Bir anahtar Ğifreleme için, diğeri ise Ğifre Ğzme için kullanılır. Ğrnekteki algoritmalar: RSA, ECC.

1.1.2.2 2. Simetrik Ğifreleme Yöntemleri Teorik Açıklama: Simetrik Ğifreleme, hız ve verimlilik açısından asimetrik Ğifrelemeye göre avantajlıdır, ancak anahtar paylaşımı sorunu vardır.

- **AES (Advanced Encryption Standard):** Yaygın kullanılan ve oldukça güvenli bir blok Ğifreleme algoritmasıdır. 128, 192 veya 256 bit anahtar uzunluklarıyla çalışır.
- **DES (Data Encryption Standard):** Daha eski bir algoritma olup, günümüzde güvenli değil kabul edilir.
- **Blok Ğifreleme ve Modlar:** Blok Ğifreleme, veriyi sabit uzunluklardaki bloklar halinde Ğifreler. Ğrneğin, ECB (Electronic Codebook), CBC (Cipher Block Chaining) gibi Ğifreleme modları vardır.

Uygulama Örnekleri:

1. AES kullanarak bir metni Ğifreleyip Ğzme işlemi.
2. CBC modunu kullanarak bir dosyanın Ğifrenmesi ve Ğifre Ğzme işlemi.

1.1.2.3 3. Asimetrik Ğifreleme Yöntemleri Teorik Açıklama: Asimetrik Ğifrelemede iki anahtar bulunur: bir kamuya açık anahtar (public key) ve bir özel anahtar (private key). Veri, kamuya açık anahtar ile Ğifrenilir ve sadece özel anahtar ile Ğzilebilir.

- **RSA (Rivest-Shamir-Adleman):** Yaygın kullanılan asimetrik Ğifreleme algoritmasıdır. Büyük asal sayılara dayalıdır ve hem Ğifreleme hem de dijital imza işlemlerinde kullanılır.
- **ECC (Elliptic Curve Cryptography):** Daha küçük anahtar boyutlarıyla RSA'ya kıyasla daha güvenli sayılan asimetrik bir Ğifreleme algoritmasıdır.

Uygulama Örnekleri:

1. RSA kullanarak bir metni Ğifreleme ve Ğzme işlemi.
2. ECC kullanarak dijital imza oluşturma ve doğrulama.

1.1.2.4 4. Hibrit Ğifreleme Teorik Açıklama: Hibrit Ğifreleme, hem simetrik hem de asimetrik Ğifrelemeyi bir arada kullanır. Simetrik anahtarlar, asimetrik Ğifreleme ile güvenli bir şekilde paylaşılır, ardından veriler simetrik anahtarla Ğifrenilir.

- **Uygulama:** E-posta ve HTTPS gibi birçok güvenli iletişim protokolünde kullanılır.

Uygulama Örnekleri:

1. Simetrik anahtarın asimetrik olarak Ğifrenmesi ve ardından verilerin simetrik Ğifre ile korunması.
2. Hibrit Ğifreleme kullanarak iki cihaz arasında güvenli veri alışverişi.

1.1.2.5 5. Dijital Sertifikalar ve Sertifika Yetkilileri (CAs) Teorik Açıklama: Dijital sertifikalar, bir kişinin veya kuruluşun kimliğini doğrulayan elektronik belgeler olarak tanımlanabilir. Bu sertifikalar genellikle bir sertifika yetkilisi (Certificate Authority - CA) tarafından imzalanır ve kullanıcılarına güvenli bir şekilde iletilir.

- **X.509 Sertifikası:** En yaygın kullanılan sertifika türüdür.
- **Sertifika Yetkilisi (CA):** Sertifikaları dijital olarak imzalayan güvenilir otoriteler.
- **Sertifika Zinciri:** Sertifikaların doğrulanabilir bir hiyerarşi ile bağlandırılması yapar. Her sertifika, bir üst otorite tarafından imzalanır.

Uygulama Örnekleri:

1. Bir web sunucusu için SSL/TLS sertifikası oluşturma ve yükleme.
2. X.509 sertifikalarının doğrulanması ve güvenli zincirinin incelenmesi.

1.1.2.6 6. Dijital Ėmzalar Teorik AĖĖklama: Dijital imzalar, verilerin kimliĖini doĖrulamak ve deĖiĖikliĖe uĖrayıp uĖramadıĖı kontrol etmek iĖin kullanılır. Ėmza, bir mesajın karması (hash) hesaplayarak ve bu karmayla Ėzel bir anahtarla Ėifreleyerek oluĖturulur.

- **Ėmzanın DoĖrulanması:** Ėmza, kamuya aĖk anahtar kullanılarak doĖrulanabilir.
- **Uygulama Alanları:** E-posta, yazılım dağıtım, dijital sözleşmeler.

Uygulama Ėrnekleri:

1. Bir dosya iĖin **dijital imza** oluĖturma ve doĖrulama.
2. **PGP/GPG** kullanarak bir mesajın imzalanması ve doĖrulanması.

1.1.2.7 7. Sertifika Tabanlı Kimlik DoĖrulama Teorik AĖĖklama: Sertifikalar, Ėzellikle sunucular arasında güvenli iletiĖimde kimlik doĖrulama iĖin kullanılır. Ėstemci ve sunucu birbirlerinin sertifikalarını doĖrularak güvenli bir iletiĖim kanalı oluĖturur.

- **SSL/TLS:** Web tarayıcılar ve sunucular arasındaki güvenli iletiĖimde kullanılan bir protokoldür.
- **Mutual Authentication:** Hem sunucu hem de istemci birbirlerini sertifikalar aracılığıyla doĖrular.

Uygulama Ėrnekleri:

1. **SSL/TLS** kullanarak güvenli bir bağlantı kurulması.
2. Sertifika tabanlı Ėift taraflı kimlik doĖrulama senaryosu uygulama.

1.1.2.8 8. PKI (Public Key Infrastructure - AĖk Anahtar Altyapısı) Teorik AĖĖklama: PKI, dijital sertifikaların oluĖturulması, dağıtılması, yĖnetilmesi ve doĖrulanması süreçlerini iĖeren bir yapıdır. PKI, güvenli iletiĖim sağlamak iĖin gerekli anahtar Ėiftlerinin ve sertifikaların yĖnetimini sağlar.

- **BileĖenler:** CA (Certificate Authority), RA (Registration Authority), CRL (Certificate Revocation List), OCSP (Online Certificate Status Protocol).
- **Uygulama Alanları:** SSL/TLS, VPN, e-posta güvenliği, kod imzalama.

Uygulama Ėrnekleri:

1. **PKI** kullanarak bir sertifika yĖnetim altyapısı kurma.
2. **OCSP** ve **CRL** ile sertifika iptallerinin kontrol edilmesi.

1.1.2.9 9. Beyaz Kutu Kriptografisi (Whitebox Cryptography) Teorik AĖĖklama: Beyaz kutu kriptografisi, Ėzellikle Ėifreleme algoritmalarının açık bir sistemde güvenli bir Ėekilde uygulanmasını sağlar. Bu teknikle, Ėifreleme iĖlemleri sırasında anahtarlar ve diĖer hassas bilgiler koruma altında tutulur.

- **Whitebox AES/DES:** AES ve DES gibi simetrik Ėifreleme algoritmalarının beyaz kutu ortamlarında uygulanması.
- **Uygulama Alanları:** Dijital hak yĖnetimi (DRM), mobil uygulama güvenliği.

Uygulama Ėrnekleri:

1. **Whitebox AES** kullanarak bir dosya Ėifreleme iĖlemi gerĖekleĖtirmek.
2. Whitebox kriptografi ile hassas verileri koruma altına almak.

1.1.2.10 10. Sertifika ve Anahtar YĖnetimi Teorik AĖĖklama: Sertifikaların ve kriptografik anahtarların etkin bir Ėekilde yĖnetilmesi, güvenli sistemlerin temel yapı taşlarıdır. Sertifikaların zamanında yenilenmesi, iptal edilmesi ve saklanması, güvenli bir iletiĖim ortamını iĖin kritik Ėneme sahiptir.

Uygulama Ėrnekleri:

1. Sertifikaların otomatik olarak yenilenmesi ve eski sertifikaların iptal edilmesi (CRL veya OCSP kullanımı).
2. **Anahtar Yönetim sistemleri** (Key Management Systems) ile anahtarların güvenli bir şekilde yönetilmesi.

9.Hafta – Sonu