**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTRİK-ELEKTRONİK FAKÜLTESİ**

**BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics*

*Department of Computer Engineering*

**STAJ DEFTERİ**

*(Internship Report)*

**STAJ TÜRÜ: GENEL STAJ**

*Type of Internship: …………..……………………………………………*

|  |
| --- |
| **ÖĞRENCİNİN *(****Student’s)*  **ADI – SOYADI** *(Name Surname)* **: Basel KELZİYE**  **SINIFI** *(Grade)*  **: 4**  **OKUL NO** *(Student ID Number)* **: 20011906** |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics Department of Computer Engineering*

**HAFTALIK STAJ ÇALIŞMA ÇİZELGESİ**

*Weekly Internship Work Schedule*

|  |  |  |
| --- | --- | --- |
| **STAJIN KONUSU** *(Internship topic):* **Kriptografi ve uygulamaları** | | |
| **21.08.2023 TARİHİNDEN 25.08.2023 TARİHİNE KADAR**  *from (21.08.2023) to (25.08.2023)* | | |
|  | **YAPILAN İŞLER**  *(Performed tasks)* | **ÇALIŞMA GÜNÜ**  *(working days)* |
| **PAZARTESİ**  *(Monday)* | Oryantasyon ve tanıtım gerçekleşti | 1 |
| **SALI**  *(Tuesday)* | TÜBİTAK yerleşkesi ve yapılan projeler  anlatıldı | 2 |
| **ÇARŞAMBA**  *(Wednesday)* | Stajyerlere bilgisayarlar teslim edildi ve  kurulum yapıldı | 3 |
| **PERŞEMBE**  *(Thursday)* | AES şifreleme metodu ve blok modları konuları araştırıldı. | 4 |
| **CUMA**  *(Friday)* | AES şifreleme algoritmasının C de  implementasyonu | 5 |
| **CUMARTESİ**  *(Saturday)* |  |  |
| **PAZAR**  *(Sunday)* |  |  |

|  |  |  |
| --- | --- | --- |
| **STAJIN KONUSU** *(Internship topic):* **Kriptografi ve uygulamaları** | | |
| **28.08.2023 TARİHİNDEN 01.09.2023 TARİHİNE KADAR**  *from (28.08.2023) to (01.09.2023)* | | |
|  | **YAPILAN İŞLER**  *(Performed tasks)* | **ÇALIŞMA GÜNÜ**  *(working days)* |
| **PAZARTESİ**  *(Monday)* | AES şifreleme algoritmasının C de  implementasyonun devamı | 6 |
| **SALI**  *(Tuesday)* | AES CBC blok modu araştırıldı | 7 |
| **ÇARŞAMBA**  *(Wednesday)* | 30 AĞUSTOS RESMİ TATİL | - |
| **PERŞEMBE**  *(Thursday)* | AES GCM blok modu araştırıldı ve  CBC blok modundan farkları öğrenildi. | 8 |
| **CUMA**  *(Friday)* | Hash fonksiyonları ve sahip olması gereken  özellikler araştırıldı. | 9 |
| **CUMARTESİ**  *(Saturday)* |  |  |
| **PAZAR**  *(Sunday)* |  |  |

|  |
| --- |
| **STAJI DENETLEYEN YETKİLİNİN**  **İMZA VE KAŞESİ**  *(Signature and Stamp of Internship Coordinator)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics Department of Computer Engineering*

**HAFTALIK STAJ ÇALIŞMA ÇİZELGESİ**

*Weekly Internship Work Schedule*

|  |  |  |
| --- | --- | --- |
| **STAJIN KONUSU** *(Internship topic):* **Kriptografi ve uygulamaları** | | |
| **04.09.2023 TARİHİNDEN 08.09.2023 TARİHİNE KADAR**  *from (04.09.2023) to (08.09.2023)* | | |
|  | **YAPILAN İŞLER**  *(Performed tasks)* | **ÇALIŞMA GÜNÜ**  *(working days)* |
| **PAZARTESİ**  *(Monday)* | SHA256’nin kullanım alanları ve önemi araştırıldı | 10 |
| **SALI**  *(Tuesday)* | Anahtar üretme fonksiyonları (KDF) ve  pbkdf2 algoritması öğrenildi | 11 |
| **ÇARŞAMBA**  *(Wednesday)* | JAVA da kullanıcının belirlediği şifreye göre anahtar  Üretip anahtarla şifreleyen basit bir program yazıldı. | 12 |
| **PERŞEMBE**  *(Thursday)* | WEB CRYPTO API kullanarak tarayıcıda pbkdf2  AES ve RSA İşlemini gerçekleştiren uygulama yazıldı | 13 |
| **CUMA**  *(Friday)* | Tarayıcı da gizli anahtar nasıl tutulur ve hangi riskleri  içerdiği konuları araştırıldı. | 14 |
| **CUMARTESİ**  *(Saturday)* |  |  |
| **PAZAR**  *(Sunday)* |  |  |

|  |  |  |
| --- | --- | --- |
| **STAJIN KONUSU** *(Internship topic):* **Kriptografi ve uygulamaları** | | |
| **11.09.2023 TARİHİNDEN 15.09.2023 TARİHİNE KADAR**  *from (11.09.2023) to (15.09.2023)* | | |
|  | **YAPILAN İŞLER**  *(Performed tasks)* | **ÇALIŞMA GÜNÜ**  *(working days)* |
| **PAZARTESİ**  *(Monday)* | WEB CRYPTO API kullanarak tarayıcı da gizli anahtarları tutan uygulama yazıldı. | 15 |
| **SALI**  *(Tuesday)* | Bellekte anahtarın tutulması ve yan kanal saldırıları hakkında araştırma yapıldı | 16 |
| **ÇARŞAMBA**  *(Wednesday)* | Hardware Secure Model (HSM) ve yan kanal saldırılarına nasıl bir çözüm getirdiği incelendi. | 17 |
| **PERŞEMBE**  *(Thursday)* | Trusted Platform Module (TPM) nedir ve yan  kanal saldırılarını nasıl önler konuları araştırıldı. | 18 |
| **CUMA**  *(Friday)* | TPM’neler yapabilir ve TPM’nin mimarisi  incelendi. | 19 |
| **CUMARTESİ**  *(Saturday)* |  |  |
| **PAZAR**  *(Sunday)* |  |  |

|  |
| --- |
| **STAJI DENETLEYEN YETKİLİNİN**  **İMZA VE KAŞESİ**  *(Signature and Stamp of Internship Coordinator)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics Department of Computer Engineering*

**HAFTALIK STAJ ÇALIŞMA ÇİZELGESİ**

*Weekly Internship Work Schedule*

|  |  |  |
| --- | --- | --- |
| **STAJIN KONUSU** *(Internship topic):* **Kriptografi ve uygulamaları** | | |
| **18.09.2023 TARİHİNDEN 22.09.2023 TARİHİNE KADAR**  *from (18..09.2023) to (22.09.2023)* | | |
|  | **YAPILAN İŞLER**  *(Performed tasks)* | **ÇALIŞMA GÜNÜ**  *(working days)* |
| **PAZARTESİ**  *(Monday)* | TSS.JAVA kütüphanesi kullanarak TPM ile temel şifreleme işlemlerini yapan kaynak kod yazıldı. | 20 |
| **SALI**  *(Tuesday)* | Beyaz kutu kriptografi nedir hangi alanlarda  Kullanılır Konuları araştırıldı. | 21 |
| **ÇARŞAMBA**  *(Wednesday)* | Beyaz kutu kriptografi kod güvenliğinden  farkları Nelerdir ve beyaz kutu kriptografisinin  Olabilirliği araştırıldı | 22 |
| **PERŞEMBE**  *(Thursday)* | Beyaz kutu kriptografinin AES algoritmasına  Uygulama Alanları araştırıldı. | 23 |
| **CUMA**  *(Friday)* | Java da beyaz kutu AES algoritmasının  implementasyonu | 24 |
| **CUMARTESİ**  *(Saturday)* |  |  |
| **PAZAR**  *(Sunday)* |  |  |

|  |  |  |
| --- | --- | --- |
| **STAJIN KONUSU** *(Internship topic):* **Kriptografi ve uygulamaları** | | |
| **25.09.2023 TARİHİNDEN 29.09.2023 TARİHİNE KADAR**  *from (25.09.2023) to (29.09.2023)* | | |
|  | **YAPILAN İŞLER**  *(Performed tasks)* | **ÇALIŞMA GÜNÜ**  *(working days)* |
| **PAZARTESİ**  *(Monday)* | Java da beyaz kutu AES algoritmasının  Gerçekleştirilmesinin devamı | 25 |
| **SALI**  *(Tuesday)* | Şifre yöneticisi nedir ve yapılırken nelere dikkat  Edilir konuları öğrenildi | 26 |
| **ÇARŞAMBA**  *(Wednesday)* | Şifre yöneticisinde anahtar yönetimi nasıl yapılmalı  Konuları araştırıldı. | 27 |
| **PERŞEMBE**  *(Thursday)* | Java da bir şifre yöneticisi uygulaması  Gerçekleştirilmesi | 28 |
| **CUMA**  *(Friday)* | Java da bir şifre yöneticisinin uygulaması  Gerçekleşmesinin devamı | 29 |
| **CUMARTESİ**  *(Saturday)* |  |  |
| **PAZAR**  *(Sunday)* |  |  |

|  |
| --- |
| **STAJI DENETLEYEN YETKİLİNİN**  **İMZA VE KAŞESİ**  *(Signature and Stamp of Internship Coordinator)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics Department of Computer Engineering*

**HAFTALIK STAJ ÇALIŞMA ÇİZELGESİ**

*Weekly Internship Work Schedule*

|  |  |  |
| --- | --- | --- |
| **STAJIN KONUSU** *(Internship topic):* **Kriptografi ve uygulamaları** | | |
| **02.10.2023 TARİHİNDEN 02.10.2023 TARİHİNE KADAR**  *from (02.10.2023) to (02.10.2023)* | | |
|  | **YAPILAN İŞLER**  *(Performed tasks)* | **ÇALIŞMA GÜNÜ**  *(working days)* |
| **PAZARTESİ**  *(Monday)* | Çıkış işlemleri ve bilgisayarın teslimi. | 30 |
| **SALI**  *(Tuesday)* |  |  |
| **ÇARŞAMBA**  *(Wednesday)* |  |  |
| **PERŞEMBE**  *(Thursday)* |  |  |
| **CUMA**  *(Friday)* |  |  |
| **CUMARTESİ**  *(Saturday)* |  |  |
| **PAZAR**  *(Sunday)* |  |  |

|  |  |  |
| --- | --- | --- |
| **STAJIN KONUSU** *(Internship topic):* **Kriptografi ve uygulamaları** | | |
| **.………………………………TARİHİNDEN………………………………..TARİHİNE KADAR**  *from (……) to (…..)* | | |
|  | **YAPILAN İŞLER**  *(Performed tasks)* | **ÇALIŞMA GÜNÜ**  *(working days)* |
| **PAZARTESİ**  *(Monday)* |  |  |
| **SALI**  *(Tuesday)* |  |  |
| **ÇARŞAMBA**  *(Wednesday)* |  |  |
| **PERŞEMBE**  *(Thursday)* |  |  |
| **CUMA**  *(Friday)* |  |  |
| **CUMARTESİ**  *(Saturday)* |  |  |
| **PAZAR**  *(Sunday)* |  |  |

|  |
| --- |
| **STAJI DENETLEYEN YETKİLİNİN**  **İMZA VE KAŞESİ**  *(Signature and Stamp of Internship Coordinator)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **:21.08.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:** |
| **YAPILAN İŞ** *(performed task)* **: Kurum Tanıtımı** | |

|  |
| --- |
| TÜBİTAK Hakkında Genel Bilgiler:  TÜBİTAK, Türkiye'de bilimsel ve teknolojik araştırmaları desteklemek ve teşvik etmek amacıyla kurulan önemli bir kamu kurumudur. Kuruluşu 1963 yılına dayanmaktadır ve Türkiye'nin bilim ve teknoloji alanındaki ilerlemesine önemli katkılarda bulunmaktadır.  TÜBİTAK'ın Temel Çalışma Sahası:  TÜBİTAK, çeşitli bilimsel ve teknolojik alanlarda araştırma projelerini finanse etmektedir. Temel çalışma sahaları arasında bilim, teknoloji, mühendislik, sağlık bilimleri, enerji, çevre bilimleri ve daha birçok alan bulunmaktadır. TÜBİTAK, bu alanlarda projeleri destekleyerek Türkiye'nin rekabetçiliğini artırmayı hedeflemektedir.  TÜBİTAK'ın Organizasyon Yapısı:  TÜBİTAK, merkezi yönetim ve bir dizi enstitü, araştırma merkezi ve birimden oluşur. Merkezi yönetim, kurumun genel politikalarını ve yönergelerini belirlerken, enstitüler ve araştırma merkezleri özgün alanlarda çalışmalar yapmaktadır. Bu organizasyon yapısı, çeşitli disiplinlerdeki bilim insanlarının işbirliği yapmasını sağlar.  TÜBİTAK'ın Üretimi ve Ürünleri:  TÜBİTAK, çeşitli araştırma projeleri sonucunda ürünler ve çözümler geliştirmektedir. Bu ürünler arasında özgün yazılımlar, cihazlar, yöntemler ve patentler bulunmaktadır. TÜBİTAK'ın ürünleri genellikle bilim ve teknoloji alanındaki gelişmeleri desteklemekte ve Türkiye'nin endüstriyel kapasitesini artırmaktadır.  Bilgisayarın Kurumdaki Yeri ve Kullanım Alanları:  TÜBİTAK, bilgisayarları araştırma projelerinin önemli bir parçası olarak kullanmaktadır. Bilgisayarlar, veri analizi, modelleme, simülasyonlar ve bilimsel hesaplamalar gibi birçok farklı alanda kullanılmaktadır. Bu teknolojiler, bilim insanlarına verileri işleme, sonuçları analiz etme ve yeni bulgular elde etme konularında büyük kolaylıklar sağlamaktadır. Ayrıca, bilgisayarlar TÜBİTAK'ın bilimsel araştırma ve geliştirme faaliyetlerinin vazgeçilmez bir parçasıdır. |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı:Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **:21.08.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:** |
| **YAPILAN İŞ** *(performed task)* **: Birim Tanıtımı** | |

|  |
| --- |
| BTE Hakkında Genel Bilgiler:  TÜBİTAK'ın bir parçası olan Bilgi Teknolojileri Enstitüsü (BTE), 1972 yılında kurulan bir kurumdur. Temel amacı, bilgi ve iletişim teknolojilerini kullanarak toplumsal refahı artırmak ve yaşam kalitesini yükseltmek olan BTE, bilgi ve teknolojinin gücünü toplumun her kesimine ulaştırmayı hedeflemektedir.  BTE'nin Görevleri:  BTE, vatandaşların, özel sektörün ve toplumun tüm katmanlarının ekonomik ve sosyal koşullarını iyileştirmek için bilgi ve iletişim teknolojilerinin potansiyelini en etkin şekilde kullanmayı amaçlamaktadır. Bu doğrultuda, millî ve özgün projeleri gerçekleştirerek kritik teknolojilerde bağımsızlığı artırmayı ve ülkenin güvenliğini güçlendirmeyi ön planda tutmaktadır.  BTE'nin Vizyonu:  BTE, bilgi sektörünün ve bilgi sermayesinin önemini kavramış ve eğitimin sürekliliğine vurgu yapmış bir enstitüdür. Ayrıca iletişim teknolojileri, bilgi otoyolları, elektronik ticaret gibi yeni gelişmelerle toplumu ekonomik, sosyal, kültürel ve siyasal açıdan ileriye taşıma hedefini benimsemektedir.  BTE'nin Misyonu:  TÜBİTAK BİLGEM BTE, "Bilgiye Değer Katar" ilkesi doğrultusunda, diğer enstitüler, üniversiteler ve sanayi kuruluşları ile iş birliği yaparak yüksek teknoloji ürünlerinin geliştirilmesine öncülük etmektedir. Bilgeliğe ve yeni projelere odaklanarak, Türkiye'nin bilim ve teknoloji alanında ilerlemesine katkı sağlamayı amaçlamaktadır. |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı:Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **:21.08.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:** |
| **YAPILAN İŞ** *(performed task)* **: Birim Tanıtımı** | |

|  |
| --- |
| BTE Hakkında Genel Bilgiler:  TÜBİTAK'ın bir parçası olan Bilgi Teknolojileri Enstitüsü (BTE), 1972 yılında kurulan bir kurumdur. Temel amacı, bilgi ve iletişim teknolojilerini kullanarak toplumsal refahı artırmak ve yaşam kalitesini yükseltmek olan BTE, bilgi ve teknolojinin gücünü toplumun her kesimine ulaştırmayı hedeflemektedir.  BTE'nin Görevleri:  BTE, vatandaşların, özel sektörün ve toplumun tüm katmanlarının ekonomik ve sosyal koşullarını iyileştirmek için bilgi ve iletişim teknolojilerinin potansiyelini en etkin şekilde kullanmayı amaçlamaktadır. Bu doğrultuda, millî ve özgün projeleri gerçekleştirerek kritik teknolojilerde bağımsızlığı artırmayı ve ülkenin güvenliğini güçlendirmeyi ön planda tutmaktadır.  BTE'nin Vizyonu:  BTE, bilgi sektörünün ve bilgi sermayesinin önemini kavramış ve eğitimin sürekliliğine vurgu yapmış bir enstitüdür. Ayrıca iletişim teknolojileri, bilgi otoyolları, elektronik ticaret gibi yeni gelişmelerle toplumu ekonomik, sosyal, kültürel ve siyasal açıdan ileriye taşıma hedefini benimsemektedir.  BTE'nin Misyonu:  TÜBİTAK BİLGEM BTE, "Bilgiye Değer Katar" ilkesi doğrultusunda, diğer enstitüler, üniversiteler ve sanayi kuruluşları ile iş birliği yaparak yüksek teknoloji ürünlerinin geliştirilmesine öncülük etmektedir. Bilgeliğe ve yeni projelere odaklanarak, Türkiye'nin bilim ve teknoloji alanında ilerlemesine katkı sağlamayı amaçlamaktadır. |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı:Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **:21.08.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:** |
| **YAPILAN İŞ** *(performed task)* **: Giriş** | |

|  |
| --- |
| Bulunduğum proje veri depo hizmeti sağlama projesi olduğundan verileri saklamak için nasıl ve hangi tür algoritmaların kullanıldığı öğrenildi. Java kullanarak şifreleme işlemleri ve kriptografik protokoller gerçekleştirildi.  Raporun 2. Bölümünde yapılan projeler ve çalışmalar her hafta için gösterilmiştir. Raporun 3. Bölümünde stajı yapılan kurum hakkında bilgi verilmiştir. Raporun 4. Bölümünde ise stajı yapılan birim hakkında bilgi verilmiştir. 5. Bölümde staj raporunun giriş kısmı verilmiştir. 6. Bölümde staj süresince yapılan projeler hakkında bilgiler verilmiştir. 7. Bölümde her gün yapılan işler hakkında bilgi verilmiş olup 8. Bölümde ise staj sırasında kazanılan deneyimler ve bilgiler sonuç olarak yazılmıştır |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı:Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **:21.08.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:** |
| **YAPILAN İŞ** *(performed task)* **: Proje Özeti** | |

|  |
| --- |
| Çalışmış olduğum proje “Safir Depo” [1] adlı güvenli dosya depolama, paylaşma ve işbirliği sağlayan milli bir bulut hizmetidir. Safir Depo doküman, resim, ses, görüntü gibi her tür dosyayı saklayabilecek ve verilerin güvenliğini garantileyebilecek bir alt yapıya sahiptir. Kişisel ve kurumsal hesap seçeneklerine sahip Safir Depo, kullanıcılarına her nerede olursa olsunlar hesaplarına akıllı telefon, tablet ve bilgisayarlarından ulaşabilmelerini sağlayacaktır.  Proje de aldığım rol ise kullanıcıların veri güvenliği için şifreleme algoritmaları öğrenildi. Anahtar güvenliği için geliştirilen anahtar yönetimi ve değişimi protokoller araştırıldı. Ve bunların hepsini yazılımsal olarak geliştirebilmek için JAVA dilinde hazır kriptografi kütüphanelerine çalışılmıştır. Versiyon kontrolü sağlayabilmek için git üzerinden pratikler yaptım. |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı:Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **:21.08.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **: 1** |
| **YAPILAN İŞ** *(performed task)* **: Oryantasyon ve Tanıtım** | |

|  |
| --- |
| Öncelikle şirket hakkında genel bilgiler ve şirketin tarihçesi hakkında kısaca bahsedildi. Daha sonra TÜBİTAK BİLGEM yerleşkesi ve birimleri hakkında bilgi verildi. Her birim hangi tür projeleri yürüttüğünü anlatıldı. Yeni başlayanlar için afet ve acil durum eğitimi verildi. Yeni çalışanlar için iş sağlığı ve güvenliği iş hayatımızdakinin önemini anlatılıp iş sağlığı ve eğitimi verildi. |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı:Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 22.08.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **: 2** |
| **YAPILAN İŞ** *(performed task)* **: TÜBİTAK Yerleşkesi ve Yapılan Projeler Tanıtımı** | |

|  |
| --- |
| Oryantasyon işlerine devam edildi. Stajyerlerin birimleri açıklanıp birimlere gidildi. Birim tanıtıldı ekipteki kişiler ve görevleri hakkında bilgilendirme yapıldı daha sonra ekibim projeleri projelerde kullanılan teknolojiler ve bu teknolojilerin kullanılma sebepleri konuşuldu. |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı:…………………………………………………………**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 23.08.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **: 3** |
| **YAPILAN İŞ** *(performed task)* **: Bilgisayar Kurulumu** | |

|  |
| --- |
| Stajyerlere bilgisayarlar teslim edildi, Java dilinin çalışabilmesi için JDK (Java Development Kit) kuruldu ve geliştirme ortamı olarak intellij tercih edilip indirildi. Birim içerisinde kontrol versiyonu için git kullanıldığı için git kuruldu takımın haberleşmek için kullandığı uygulama mattermost indirilip üzerinden takım ile iletişim kuruldu. Birim ve dahil olunacağı proje belirlendi. Proje için araştırılması gereken teknolojiler verildi. |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 24.08.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:4** |
| **YAPILAN İŞ** *(performed task)* **: AES Şifreleme Algoritması ve Blok Modların Araştırılması** | |

|  |
| --- |
| AES şifreleme metodu, AES’in blok modları (EBC,CBC,CTR,GCM) modları araştırıldı. Blok modların birbirine göre avantaj ve dezavantajları. Proje de hangi mod ve neden kullanılması gerektiğini, AES’in anahtar uzunluğunu neyi değiştirdiğini, Hangi durumda hangi anahtar uzunluğunu kullanılması gerektiğini detaylı bir şekilde araştırıldı.  EBC: Girişe bağlı çıktı verdiği için tercih edilmeyen bir mod. **Şekil 1** gösterilmiştir.  CBC: blok modları birbirine beklemek zorunda olduğundan paralel olarak işlenmeyip yavaş olduğu için tercih edilmeyen blok modu. CTR: EBC ve CBC modların problemlerini çözdüğü için tercih edilen bir metoddur. GCM: CTR özelliklerien sahip ancak verinin bütünlüğünü de kontrol edebildiğimiz için bazı durumlarda kullanılabilir.  A screenshot of a computer generated image  Description automatically generated  **Şekil 1.** ECB Şifreleme örneği |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 25.08.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:5** |
| **YAPILAN İŞ** *(performed task)* **: AES Şifreleme Algoritmasının C de Gerçekleştirilmesi** | |

|  |
| --- |
| Şifreleme algoritmaları, zaman ve yer karmaşıklığı açısından verimli olmaları gerektiği için, onları alt seviyeli bir dil olan C gibi bir dilde geliştirmek son derece kritik bir öneme sahiptir. Bu, şifreleme algoritmasının matematiksel doğruluğunun yanı sıra, gerçek dünyada hatasız bir şekilde uygulanmasının ne kadar önemli olduğunu vurgular.  Özellikle AES algoritması gibi güçlü şifreleme algoritmaları, farklı anahtar boyutlarını desteklese de, projenizin gereksinimlerine uygun bir yaklaşım benimsemek önemlidir. Ben, tasarımı basit ve etkili tutmak amacıyla 128 bit anahtar uzunluğunu tercih ettim, çünkü projem için bu boyut yeterliydi. Ancak, güvenlik gereksinimlerine göre daha uzun anahtarlar da gerekebilir. Bu nedenle, şifreleme algoritmalarının tasarımında, hem güvenlik hem de performans dengesini sağlama amacıyla dikkatli bir yaklaşım benimsemek önemlidir. |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 28.08.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:6** |
| **YAPILAN İŞ** *(performed task)* **: AES Şifreleme Algoritmasının C de Gerçekleştirilmesi** | |

|  |
| --- |
| AES şifreleme algoritmasının C İmplementasyonun devamını getirmeye çalıştım. Bu aşamada key üretme aşaması (Key expansion) aşaması bitmiş olup SubByte,ShiftRow, MatrixMultiplication aşamaları kalmıştır. Burda uygulamayı tasarlarken bellek alanından biraz vazgeçip hıza odaklandığım için AES için gereken bazı tabloları çalıştırırken hesaplamak adına önceden hesaplanıp programın içine gömülmüştür.  Galios sonlu alanında 2 ile çarpma işleminin tüm durumlar önceden hesaplanıp tutulmuştur:  static uint8\_t mul2[256] = {  0x00,0x02,0x04,0x06,0x08,0x0a,0x0c,0x0e,0x10,0x12,0x14,0x16,0x18,0x1a,0x1c,0x1e,  0x20,0x22,0x24,0x26,0x28,0x2a,0x2c,0x2e,0x30,0x32,0x34,0x36,0x38,0x3a,0x3c,0x3e,  0x40,0x42,0x44,0x46,0x48,0x4a,0x4c,0x4e,0x50,0x52,0x54,0x56,0x58,0x5a,0x5c,0x5e,  0x60,0x62,0x64,0x66,0x68,0x6a,0x6c,0x6e,0x70,0x72,0x74,0x76,0x78,0x7a,0x7c,0x7e,  0x80,0x82,0x84,0x86,0x88,0x8a,0x8c,0x8e,0x90,0x92,0x94,0x96,0x98,0x9a,0x9c,0x9e,  0xa0,0xa2,0xa4,0xa6,0xa8,0xaa,0xac,0xae,0xb0,0xb2,0xb4,0xb6,0xb8,0xba,0xbc,0xbe,  0xc0,0xc2,0xc4,0xc6,0xc8,0xca,0xcc,0xce,0xd0,0xd2,0xd4,0xd6,0xd8,0xda,0xdc,0xde,  0xe0,0xe2,0xe4,0xe6,0xe8,0xea,0xec,0xee,0xf0,0xf2,0xf4,0xf6,0xf8,0xfa,0xfc,0xfe,  0x1b,0x19,0x1f,0x1d,0x13,0x11,0x17,0x15,0x0b,0x09,0x0f,0x0d,0x03,0x01,0x07,0x05,  0x3b,0x39,0x3f,0x3d,0x33,0x31,0x37,0x35,0x2b,0x29,0x2f,0x2d,0x23,0x21,0x27,0x25,  0x5b,0x59,0x5f,0x5d,0x53,0x51,0x57,0x55,0x4b,0x49,0x4f,0x4d,0x43,0x41,0x47,0x45,  0x7b,0x79,0x7f,0x7d,0x73,0x71,0x77,0x75,0x6b,0x69,0x6f,0x6d,0x63,0x61,0x67,0x65,  0x9b,0x99,0x9f,0x9d,0x93,0x91,0x97,0x95,0x8b,0x89,0x8f,0x8d,0x83,0x81,0x87,0x85,  0xbb,0xb9,0xbf,0xbd,0xb3,0xb1,0xb7,0xb5,0xab,0xa9,0xaf,0xad,0xa3,0xa1,0xa7,0xa5,  0xdb,0xd9,0xdf,0xdd,0xd3,0xd1,0xd7,0xd5,0xcb,0xc9,0xcf,0xcd,0xc3,0xc1,0xc7,0xc5,  0xfb,0xf9,0xff,0xfd,0xf3,0xf1,0xf7,0xf5,0xeb,0xe9,0xef,0xed,0xe3,0xe1,0xe7,0xe5  }; |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 29.08.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:7** |
| **YAPILAN İŞ** *(performed task)* **: AES CBC Block Modu** | |

|  |
| --- |
| AES CBC ve GCM blok modları hakkında araştırma yapıldı.  Block cipher CBC modu.  CBC modunda her bloka normal şifreleme uygulandıktan sonra, bir önceki şifrelenmiş blok ile ‘’XOR’’ işlemine sokulur. Bunu EBC modundaki aynı giriş için aynı çıkışı üretme problemini ortadan kaldırmak için yapılır. İlk bloktan önce, blok bulunmadığı için önceden hazırlanmış bir ‘’Initialization Vector’’ ile XOR işlemine sokulur. IV gizli olmasına gerek yok çünkü IV sadece ilk durumu karıştırmak için kullanılır. Örneğin: IV olmasaydı ve bütün blokları aynı olsaydı biz yine tıpkı EBC modundaki çıktı alacağız.  Algoritmanın İskeleti **Şekil 2** gösterilmiştir.  Avantajlar: Aynı mesaj ve anahtar için farklı çıktı üretir bu yüzden daha güvenli olduğu söyleyebiliriz. Dezavantaj: Yeni bloğun şifrelenmesi için bir önceki blok şifrelenmiş olması gerekir, bu durum bizi Parallel hesaplama yapmamıza engel olur.  A black background with a black square  Description automatically generated with medium confidence  **Şekil 2.** CBC Blok Modu Gösterimi |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 31.08.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:8** |
| **YAPILAN İŞ** *(performed task)* **: AES GCM Blok Modu** | |

|  |
| --- |
| GCM modu, CTR modun gelişmiş versiyonu olduğunu düşünebiliriz. İlk önce ‘’Nonce’’ (sadece bir kere kullanılacak sayı) alınır bir yanına bir Sayaç (Counter) değeri eklenir. Genelde bu değer 0 dan başlar ve birer birer artar. Örneğin Nonce 10000 olsun ve Counter değerimiz 1111 olsun. Bizim giriş değerimiz Nonce || Counter -> 100001111 olur. Biz şifreleme algoritmamıza bu değeri giriş olarak veririz, ve çıkan şifreli bloğu asıl şifrelemek istediğimiz mesaj ile XOR işlemi uygularız. GCM modu aynı anda bize verinin bütünlüğünü (İntegrity) i kontrol etmemize de izin verir. Bu özelliğe AEAD (Authenticate encrypt with associated data) denir. Biz verinin Mesaj Kodunu (MAC) hesaplarız ve şifreli metinle birleştirip gönderilir. Biz AES-GCM i sadece verilerin bütünlüğünü sağlamak için de kullanabiliriz[2].  Avantajları: -Paralel hesaplamaya izin verir çünkü bloklar birbirine bağlı değil, hatta mesajı almadan bile şifreleme işlemine başlayabiliriz çünkü biz mesaja sadece XOR işlemini uygularız, AES e beslediğimiz değerleri önceden belirleyebiliriz. -Veri bütünlüğünü sağlar, Biz hem verileri şifreleme hem de bütünlüğünü sağlamayı bir seferde sağladık, verileri ayrı Mesaj kodun  Dezavantajlar:  -Dikkatli kullanılması gerekir, “Aynı Nonce” ı iki defa kullanmak bir tehlike oluşturabiliyor. |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 01.09.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:9** |
| **YAPILAN İŞ** *(performed task)* **: Hash Fonksiyonların araştırılması** | |

|  |
| --- |
| Hash fonksiyonları ne olduğu araştırıldı, Hash fonksiyonu herhangi bir girişi alır şifreleme yapar ve onu belirli bir boyuta sıkıştırıp (sha 256 da bu boyut 256 bit) bir sonuç üretir.  Hash fonksiyonları bu 3 özelliği barındırmalıdır:  **1)Verilen bir çıkıştan giriş bilgisini elde edememek**  Hash fonksiyonları Encrypt yöntemlerinden ayıran kısım budur. Eğer elinizde bir Encrypt edilmiş bir sonuç varsa ve siz uygun decrypt anahtarı kullanırsanız asıl girişi bulursunuz fakat hash fonksiyonları için böyle bir durum söz konusu değildir.  Eğer bir Hash sonucundan verilen girişi bulabiliyorsanız kullandığınız hash fonksiyonu güvenli değil demektir.  **2) X ≠ Y iken H(X) = H(Y) olmaması**  X ve Y birbirinden farklı 2 giriş olarak düşünelim. Bu girişlerin ayrı ayrı Hashleri alındığında ve ikisinin Hash sonuçların eşit olması durumuna Hash Collision(Hash çakışması) denir, **Sekil 3** de gösterilmiştir.  **3)Şifreleme işlemini uygun bir zamanda yapması**  Şifreleme işlemi ne kadar karışık olsa da Hash fonksiyonunun gereken bütün işlemleri hızlı bir şekilde bitirmesi gerekiyor çünkü Hash fonksiyonları sürekli kullanılıyor ve hızlı bir şekilde üretmesi gerekmektedir.  A diagram of a graph  Description automatically generated with medium confidence  **Şekil 3.** Hash Çakışma Örneği |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 04.09.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:10** |
| **YAPILAN İŞ** *(performed task)* **: SHA256 Kullanım Alanları ve Özellikleri** | |

|  |
| --- |
| Hash fonksiyonların kullanım alanları araştırıldı. **1) Bitcoin madenciliği** Bitcoin transferlerinin şifrelenmesi ve valid bloğun bulunması için SHA256 kullanılır.  **2)İnternette parola saklama**  İnternette herhangi bir siteye parolanız doğrudan saklanmaz. Çünkü herhangi bir siber saldırı olması durumunda parolanız direkt açığa çıkar. Onun yerine parolanız bir Hash fonksiyonundan geçirilir ve o şekilde saklanır. Giriş yapmaya çalıştığınızda parolanızın Hashleri karşılaştırılır daha sonra girişe izin verilir.  3) Büyük dosyaların karşılaştırılması  Elinizde iki büyük dosya olduğunu varsayın ve onların birebir aynı olup olmadığına bakmak istediğinizi farz edin. İki dosyanın Hashleri hesaplanır ve sonuçları aynı çıkar ise iki dosyanın eşit olduğunu söyleyebiliriz.Özetleyecek olursak Hash fonksiyonları herhangi bir boyutta giriş alır daha sonra o girişi şifreleyerek ona özel bir kimlik oluşturur. |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 05.09.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:11** |
| **YAPILAN İŞ** *(performed task)* **: Anahtar Türetme Algoritmaların incelenmesi** | |

|  |
| --- |
| Key derivation algoritmaları nedir? Neden ihtiyaç duyurulur? Pbkdf2 i araştırıldı.  Anahtar türetme algoritmaları, kullanıcının girdiği bir şifreyi (parolayı) kriptografik bir anahtara çevirme işlemidir. Kullanıcının girdiği şifreler bazen kolay ve kriptografik olarak güçlü değiller diğer yandan bir kullanıcının kriptografik güçlü bir anahtarı şifre olarak belirleyip ezbere bilmesi mümkün değildir. O yüzden normal ezbere bilinen bir şifreyi kriptografik güçlü anahtar üretilmesine ihtiyaç duyurulur. pbkdf2 de anahtar üretme algoritmaların en popülerinden birtanesi, kısaca şifrenin özetini (hash) alır, yanına bir salt (random sayı) ekle ve bunları birbirlerine karıştırıp anahtar üretir[3].  **Şekil 4** te PBKDF2 algoritmasının giriş ve çıkışları gösterildi.  A diagram of a salt and no iterations  Description automatically generated  **Şekil 4.** PBKDF2 Girdi-Çıktı ilişkisi |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 06.09.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:12** |
| **YAPILAN İŞ** *(performed task)* **: Java da Basit Bir Şifreleme Programı Yazmak** | |

|  |
| --- |
| Java da hazır kütüphaneler kullanarak kullanıcıdan şifre isteyen sonra o şifreden pbkdf2 algoritmasıyla anahtar üreten. Ve 256bitlik AES, 4096 bitlik RSA anahtarları üreten, pbkdf2 ile üretilen anahtarla AES256 bitlik anahtarı şifreleyen ve RSA çift anahtarıyla basit şifreleme/çözme işlemleri test eden kod parçası yazıldı. |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 07.09.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:13** |
| **YAPILAN İŞ** *(performed task)* **: WEB CRYPTO API Kullanarak Şifrelemek** | |

|  |  |
| --- | --- |
| Web crypto api nedir? Web Crypto API, web tarayıcılarında kullanılabilen bir JavaScript API'dır ve tarayıcılar aracılığıyla güvenli şifreleme ve şifre çözme işlemleri gerçekleştirmek için tasarlanmıştır. Bu API, web uygulamalarının tarayıcı içinde güçlü şifreleme işlemleri yapabilmesini sağlar ve özellikle web tabanlı uygulamaların güvenliğini artırmak için kullanılır.  Web Crypto API kullanılarak typescript dilinde AES anahtarını kullanıcının girdiği boyuta bağlı bir AES anahtarını üreten. Ve yine de kullanıcının belirlediği boyuta bağlı RSA anahtar çiftini üreten Metodlar yazıldı. Üretilmiş AES anahtarını RSA açık anahtarıyla şifreleyip daha sonra bu şifreyi çözen metod geliştirildi. PBKDF2 ile anahtar üreten ve AES anahtarını Wrap/Unwrapp (Şifreleme/Şifre çözme) işini yapan program geliştirildi.   |  | | --- | | **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* | |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 08.09.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:14** |
| **YAPILAN İŞ** *(performed task)* **: Tarayıcı da Nasıl Anahtar Tutulur Konusu Araştırıldı** | |

|  |
| --- |
| Tarayıcı gizli anahtarlar nasıl tutulur? Tarayıcı gizli anahtar tutmak ne kadar güvenli konuları araştırıldı. Webde anahtar tutmak biraz tehlike arz edebilir, çünkü bir eğer iyi saklanmazsa bir XSS saldırısı ile anahtarlar doğrudan çalınabilir. Genelde anahtarlar localstorage, cookies ve indexedDB de tutulur, bunların localstorage ve indexedDB güvenlik açısından birbirleriyle aynı ama cookies daha çok riskli olduğunu söyleyebiliriz çünkü cookies her https isteğiyle gönderilir. Biri internet üzerinden giden paketinizi ele geçirirse anahtarlar açığa çıkar. Sonuç: gizli anahtarı webde tutmak her zaman risk içerir, ve XSS ataklar yukarıda anlatıldığı gibi anahtarı ele geçirebilir. Tersine mühendislikte anahtarı açığa çıkarabilir. |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 11.09.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:15** |
| **YAPILAN İŞ** *(performed task)* **: Tarayıcı da Anahtar Tutma İşlemi** | |

|  |
| --- |
| IndexedDB nedir?  IndexedDB (Indexed Database) web tarayıcılarında kullanılabilen bir veritabanı depolama teknolojisidir. Web geliştiricilerinin tarayıcı içinde yapılandırılabilir ve performanslı bir şekilde büyük miktarlarda veri saklamalarına ve sorgulamalarına olanak tanır. IndexedDB, özellikle çevrimdışı uygulamalar ve büyük ölçekli veri yönetimi gereksinimlerini karşılamak için kullanışlıdır.  IndexedDB ve Web Api crypto kullanarak tarayıcı da tehlikeleri göz önünde bulundurarak efektif ve güvenilir bir şekilde gizli anahtarı tutan programı typescriptte yazıldı. |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 12.09.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:16** |
| **YAPILAN İŞ** *(performed task)* **:Yan Kanal Saldırıları ve Anahtar Arama Saldırıları** | |

|  |
| --- |
| Bilgisayarda anahtarı tutmak neden tehlike arz eder? Hangi saldırılar gerçekleşebilir? Bu saldırlardan nasıl korunuz? Konuları araştırıldı  Bir program çalıştırırken hafıza da (RAM) de tutulduğunu hepimiz biliyoruz, bizim program bir gizli anahtarla işlem yapacağını düşünelim. Anahtarı Kullanabilmek için onu da hafızaya almak durumundayız. Gizli anahtar Hafıza da dururken saldırgan kişi bu anahtarı hafızadan okuyabilir (bufferoverflow, hafızaya erişimi varsa “Key findings attacks” vb.) saldırıları gerçekleşebilir.  Bu yüzden genelde anahtar kısa süreliğine olsa da hafıza da tutulması tehlike arz eder. Bunu çözmek için donanımsal olarak güvenli ve dışardan erişilmediği bir birime sahip olmamız lazım. |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 13.09.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:17** |
| **YAPILAN İŞ** *(performed task)* **: HSM ve Kullanım Alanları Araştırıldı** | |

|  |
| --- |
| HSM nedir? Nerelerde kullanılır? Gizli Anahtarı nasıl korur? Hardware Secure Model anahtar üretme, anahtar saklama, anahtar doğrulama gibi kriptografik işlemleri gerçekleştirmek için tasarlanan bir donanım. Bu donanım sunucu gibi düşünülebilir, Bilgisayarımızın içerisinde bulunmamaktadır. Tam tersi uzaktan erişmemiz gerekmektedir[5].  HSM bütün anahtar yönetimini halledebilir(anahtar üretme, değiştirme,yok etme). HSM Aynı anda Rastgele sayı üretme modülü de bulunduruyor. Rastgele sayıları anahtarlar için oldukça kritiktir. Kriptografik özellikleri sağlayarak tasarlandığı için şifreleme/şifre çözme işlemleri için de kullanılabilir. |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 14.09.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:18** |
| **YAPILAN İŞ** *(performed task)* **: TPM ve Kullanım Alanlar Araştırıldı** | |

|  |
| --- |
| TPM nedir? TPM 1.2 ve 2.0 farkları nedir? TPM HSM den farkı nedir? Trusted Platform Module yine gizli bilgileri ve işlemleri korumak için geliştirilen donanımsal bir çözümdür. TPM genelde anakartın içine gömülü bir şekilde gelir, sonradan eklenebilir bir aygıt değil yani (bazı versiyonları öyle olabiliyor)[6]. Görüldüğü gibi HSM den temel farkı budur.TPM anahtar yönetimi için kullanılır, Oturum (Session) oluşturma imkanı verir. TPM bilgisayarın Boot sırasında ortamın bilgilerini hesaplar ve ilerde bu bilgilerini Bilgisayarın durumunu karşılaştırmak için kullanabilir. TPM in temel amacı anahtar yönetimi ve onlarla ilgili işlemlere Yüksek güvenli bir alan oluşturmak. |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 15.09.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:19** |
| **YAPILAN İŞ** *(performed task)* **: TPM’nin Kapasitesi ve Mimarisi** | |

|  |
| --- |
| TPM sadece bir kere üretilen "Onay Anahtar" (Endorsement Key) bulundurmaktadır, bu asimetrik anahtarı üreten firma oluşturur ve TPM nin içine gömer. Bu anahtarlar ile Anahtar tasdiki ‘’Key Attestation’’ dediğimiz olayı gerçekleştirebiliriz. Kısaca Bir sertifika doğrulama mekanizması bu her taraf kendisine verilmek EKpub (Endorsement Key public) i diğer tarafalara verir ve bu doğrulama mekanizması yazılımsal (login bilgiler, ip vb) doğrulamalardan daha güvenli çünkü fiziksel donanımsal yapılar ile sağlanıyor.  A screenshot of a computer  Description automatically generated |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 18.09.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:20** |
| **YAPILAN İŞ** *(performed task)* **: TSS.JAVA ile TPM’e Erişmek** | |

|  |
| --- |
| TPM in hazır kütüphaneleri araştır, TPM in hazır kütüphanesi kullanılarak TPM’e bazı kriptografik işlemler yaptıran Java kod yazılmaya çalışıldı. Öncelikle Java dili ile yazılması gerektiği için java kütüphaneleri araştırıldı, Karşımıza jTSS ve tpmj kütüphaneleri karşımıza çıktı. Anca bu kütüphaneler TPM1.2 i destekledikleri için ve güncel cihazların hepsi TPM2.0 barındırdığı için kullanılamaz halde geldiler. Microsoftun geliştirdiği TSS.Java kütüphanesi ile yapıldı. Not: Kütüphane halen geliştirilmekte olduğu için tam çalışmayıp bazı istenen sonuçlar elde edilememiştir. |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 19.09.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:21** |
| **YAPILAN İŞ** *(performed task)* **: Beyaz Kutu Kriptografisi Araştırıldı** | |

|  |
| --- |
| Whitebox crypto nedir? Hangi alanlarda kullanılır?  Whitebox cryptografi algoritmalarda kullanılan gizli anahatarları bellekte açık bir şekilde tutmadan şifreleme işlemini hedefler. Saldırganın beyaz kutu(whitebox) modelinde düşünür, yani saldırgan hem giriş,hem çıkış hem de çalıştırma ortamı bulunmaktadır.Peki bu neden kullanılır? Örneğin siz bir oyun aldınız ve oyunun bir kısmı paralı, oyun sizin bilgisayarda çalıştığı için çalıştırma ortamına 100% yetkilisiniz. Siz bazı şartları sağlamadan(özel kısımları satın almak vs.) o anahtarı bulamamanız lazım, beyaz kutu kriptografi bunun için kullanılır. Yani haberleşme güvenliğinden çok dijital telif hakkı gibi durumlarda kullanılır[4]. |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 20.09.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:22** |
| **YAPILAN İŞ** *(performed task)* **: Beyaz Kutu Kriptografisi ve Kod Güvenliği farklılıkları** | |

|  |
| --- |
| Beyaz kutu kriptografi kod güvenliği (code obfuscation)dan farkı nedir? Beyaz kutu kriptografi mümkün mü?  Kod güvenliğini bir algoritmayı tersine mühendisliğinden korumayı çabalarken, Whitebox crypto anahtarı gizlemeyi çalışır. Teorik olarak 100% dayanıklı beyaz kutu kriptografisi tasarlamak mümkün değil, ancak anahtarı parçalayıp ve bir kısmını beyaz kutu ile korumak faydalı olabilir. Şekil 5 de beyaz kutu kriptografisinin işleyişi gösterildi.  A diagram of a random data configuration  Description automatically generated  **Şekil 5.** Beyaz Kutu Kriptografi İçeriği |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 21.09.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:23** |
| **YAPILAN İŞ** *(performed task)* **: Beyaz Kutu AES Algoritması** | |

|  |
| --- |
| AES beyaz kutu algoritması araştırılması, ve JAVA da implementasyon incelenmesi. AES beyaz kutu algoritması AES in “Shift Row” ,“Sub Byte” ve “Add round key” adımlarını birleştirerek bir Tbox tablo oluşturmaya hedefler, bu tabloya sonlu alan çarpma işlemleriyle anahtar gizlenir, şifreleme yapılacağı zaman anahtara gerek kalmaz. Bu tabloları kullanarak şifreleme ve deşifreleme kullanılır. Aşağıda **Şekil 6** da AES ile Beyaz Kutu AES karşılaştırılması gösterilmiştir.  A diagram of a computer program  Description automatically generated  **Şekil 6.** AES ile Beyaz Kutu AES karşılaştırılması |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 22.09.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:24** |
| **YAPILAN İŞ** *(performed task)* **: Java da Beyaz Kutu AES İmplementasyon** | |

|  |
| --- |
| AES beyaz kutunun önemini öğrendikten sonra, Anahtarı parçalayıp saklamak için kullanılabildiğini gördüm. Bu yüzden bu AES beyaz kutu algoritmasını JAVA da gerçekleştirmeye çalıştım.  **Şekil 7.** De Algoritmanın genel yapısı ve Tboxlar gösterilmiştir.  A computer screen with text on it  Description automatically generated    **Şekil 7.** Beyaz Kutu AES Java implementasyonu |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 25.09.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:25** |
| **YAPILAN İŞ** *(performed task)* **: Java da Beyaz Kutu AES İmplementasyon** | |

|  |
| --- |
| Java da implementasyonun devamı gerçekleşti ve test durumları yazıldı. Test durumları yazarken İmplementasyon için gereken tboxlar oluşturulup uygun olup olmadığı test edildi. Daha sonra normal AES’te kullandığımız shiftRow, subByte gibi metodların testleri yazıldı. Ve algoritmanın en zor kısmı olan matrislerin çarpımı “Mixing Bijection” kısmı test edildi. En son hazırlamış olduğumuz metodları kullanarak beyaz kutu AES in şifreleme ve şifre çözme durumlar test edildi. Şifreleme testi Şekil 8. De gösterilmiştir.  A screen shot of a computer code  Description automatically generated  **Şekil 8.** Şifreleme İşlemin Testi |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 26.09.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:26** |
| **YAPILAN İŞ** *(performed task)* **: Şifre Yöneticisi Nedir ve Nasıl Çalışır Araştırıldı** | |

|  |
| --- |
| Şifre Yöneticisi nedir? Anahtarı nasıl korumaya alırız? Konuları araştırıldı 1/2.  Şifre Yöneticisi genelde bizim şifreleri korumak için kullandığımız bir hizmet, şifre yöneticisi güvenli olması oldukça önemlidir. Genelde bizim bir “Master Key” dediğimiz anahtar bulunmaktadır ve biz bu anahtarı kullanarak diğer şifreleme anahtarlarını şifreleriz.    Daha sonra bu anahtarların şifrelenmiş halini verilerin yanında tutabiliriz. |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 27.09.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:27** |
| **YAPILAN İŞ** *(performed task)* **:Şifre Yöneticisinde Anahtar Yönetimi** | |

|  |
| --- |
| Master key nasıl üretilmeli? Nasıl korunmalı? Nerde saklanmalı? Şifremizi unutursak ne yapılır?  Kullanıcı bir hatırlayabileceği bir şifre seçer ve bu şifreden bir kriptografik anahtar üretilir (KDF) kullanarak. Bu anahtar genelde giriş yapılırken üretilir (aynı şifreyi girdiği takdirde aynı anahtarı elde ederiz). Sonra bu anahtarı korumak için donanım seviyesi koruma yöntemine ihtiyaç duyulur (TPM vs. gibi). Şifremizi unutursak bu anahtarı elde edemeyiz ve bu sefer sakladığımız bütün verileri kaybetmiş oluruz. O yüzden biz kullanıcıya soru/cevap tarzı bir kaç bilgi alıp, o bilgilerle yine anahtar üretip ve o anahtarla bütün verileri şifreleyip depolarız. Bellek alanı açısından maliyetli olduğunu söyleyebiliriz. |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 28.09.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:28** |
| **YAPILAN İŞ** *(performed task)* **: Java da Şifre Yöneticisi Uygulaması Gerçekleştirilmesi** | |

|  |
| --- |
| Şifre yöneticisi araştırıldıktan sonra benden JAVA da şifre yöneticisi program yazılması istedi, yukarıdaki kurallara dikkat ederek tasarlanması istendi. İlk önce kullanıcıdan bir şifre istendi O şifreye pbkdf2 algoritması uygulayarak bir master key oluşturuldu.  PBKDF2 parametreleri olarak rastgele oluşturulmuş (Ama ileri için sakladığımız) bir salt değeri, Adım olarak 10000 adım ve uzunluk olarak 256 bit uzunluğunda bir anahtar üretilecek. Şekil 9 da pbkdf2 ile Anahtar üreten kod gösterilmiştir.  A screen shot of a computer code  Description automatically generated  **Şekil 9.** Pbkdf2 ile anahtar üretme |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 29.09.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:29** |
| **YAPILAN İŞ** *(performed task)* **: Java da Şifre Yöneticisi Uygulaması Gerçekleştirilmesi** | |

|  |
| --- |
| Şifre yöneticisinin devamı olarak önceden araştırılan yöntem izlendi, Yani oluşturmuş olduğum master key ile her şifre için özel oluşturduğum anahtarı şifreleyip veri tabananında şifrelenmiş anahtarı ve şifrelenmiş şifreyi tuttum. Kullanıcı giriş yaptığında uygulama bir şifre ister ve bu şifreyi kullanarak master key oluşturulur yani biz master key i sadece program çalışırken bellekte tutarız diğer durumlarda bellekten silinir. Şifreleri şifreleyen anahtarlar ise oluşturulur oluşturulmaz şifreleme işlemleri yapıp yok edilir ki belleğe saldırı durumunda elde edilmesin. Şekil 10 da şifre yöneticisine yeni şifre ekleme işlemi gösterilmiştir.  A computer screen shot of text  Description automatically generated  **Şekil 10.** Yeni Şifre Ekleme |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 02.10.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:30** |
| **YAPILAN İŞ** *(performed task)* **: Çıkış İşlemleri** | |

|  |
| --- |
| Stajın son günü bana verilmiş olan bilgisayar temizleyerek teslim edildi, proje arkadaşlarıyla staj değerlendirilmesi yapıp projenin geleceği hakkında konuşuldu. Son olarak TÜBİTAK BİLGEM den çıkış işlemleri yaparak staj süreci resmi bi şekilde bitmiş oldu. |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 02.10.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:** |
| **YAPILAN İŞ** *(performed task)* **: Sonuç** | |

|  |
| --- |
| Bu staj deneyimi, kriptografi, AES ve blok modları, anahtar yönetimi, donanımsal güvenlik (TPM ve HSM) gibi önemli konuları kapsayan zengin bir bilgi ve deneyim kazandırdı. Staj süresince katıldığım projeler ve yaptığım araştırmalar, beni bilgisayar güvenliği ve kriptografinin önemini daha iyi anlamaya yönlendirdi.  Stajım boyunca, AES ve blok modlarına dair detaylı bilgi edindim ve bu alandaki şifreleme yöntemlerinin gücünü ve zayıflıklarını inceledim. Anahtar yönetimi konusu, güvenli veri iletimi ve depolaması için kritik bir öneme sahiptir ve bu alanda çalışma fırsatı bulmak, benim için büyük bir öğrenme deneyimi oldu.  Donanımsal güvenlik konusunda, TPM ve HSM gibi güvenilir platformlar hakkında bilgi edinmek, bilgisayar sistemlerinin güvenliği ve veri bütünlüğü açısından ne kadar önemli olduklarını anlamama yardımcı oldu. Bu donanımsal güvenlik cihazlarının uygulama alanları ve nasıl kullanıldıkları hakkında bilgi sahibi oldum.  Ayrıca, şifre yöneticisi gibi güvenlikle ilgili pratik uygulamaları inceleyerek, günlük hayatta sıkça karşılaşılan güvenlik sorunlarına daha duyarlı hale geldim. Kullanıcıların şifrelerini güvenli bir şekilde yönetmelerinin neden önemli olduğunu ve bu tür uygulamaların nasıl geliştirilebileceğini daha iyi anladım.  Stajımın sonucunda, bilgisayar güvenliği ve kriptografi alanlarına olan ilgim daha da arttı. Bu alandaki bilgi ve deneyimlerim, gelecekteki kariyerimde güvenlik odaklı projelere ve çözümlere katkı sağlama konusundaki motivasyonumu artırdı. Stajımın bana kazandırdığı bu bilgi ve deneyimleri, gelecekteki profesyonel yaşantımda daha da geliştirmek ve bu alandaki katkılarımı sürdürmek istiyorum. |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**ELEKTİRİK-ELEKTRONİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

*Yildiz Technical University | Faculty of Electrical and Electronics | Department of Computer Engineering*

**STAJ GÜNLÜĞÜ***(Internship diary)*

|  |  |
| --- | --- |
| **TARİH** *(Date)* **: 02.10.2023** | **ÇALIŞMA GÜNÜ** *(Day)* **:** |
| **YAPILAN İŞ** *(performed task)* **: Referans** | |

|  |
| --- |
| [1] Safir Depo Proje Detayları: <https://safirdepo.b3lab.org/about>  [2] AES-GCM Blok Modu: <https://csrc.nist.rip/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-spec.pdf>  [3] PBKDF2 Algoritmasının Detayları: <https://en.wikipedia.org/wiki/PBKDF2#:~:text=PBKDF2%20applies%20a%20pseudorandom%20function,cryptographic%20key%20in%20subsequent%20operations.>  [4] WhiteBox Cryptography: <https://www.whiteboxcrypto.com/index.php>  [5] HSM ve uygulamaları: <https://www.techtarget.com/searchsecurity/definition/hardware-security-module-HSM>  [6] TPM nedir: <https://www.intel.com/content/www/us/en/business/enterprise-computers/resources/trusted-platform-module.html#:~:text=A%20TPM%2C%20or%20a%20trusted,motherboard%20or%20in%20its%20processor.> |

|  |
| --- |
| **Stajı Denetleyen Yetkilinin Adı-Soyadı-Unvanı: Uzman Araştırmacı Ayşe İnanç**  *(Name-Surname -Title of Internship Coordinator)*  **İmza ve Kaşe :…………………………………………………………**  *(Signature and Stamp)* |