**T.C.**

**TRAKYA ÜNİVERSİTESİ**

**FEN BİLİMLERİ ENSTİTÜSÜ**

# GÜVENLİ ELEKTRONİK SEÇİM İÇİN SIR PAYLAŞIM ŞEMALARININ UYGULANMASI

**SELİN DEMİRBİLEK AYYILDIZ**

**YÜKSEK LİSANS TEZİ**

**BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI**

**Tez Danışmanı: Dr. Öğr. Üyesi DERYA ARDA**

**EDİRNE-2021**

**Selin DEMİRBİLEK AYYILDIZ**'ın hazırladığı **"GÜVENLİ ELEKTRONİK SEÇİM İÇİN SIR PAYLAŞIM ŞEMALARININ UYGULANMASI"** başlıklı bu tez, tarafımızca okunmuş, kapsam ve niteliği açısından Bilgisayar Mühendisliği Anabilim Dalında bir **Yüksek lisans tezi** olarak kabul edilmiştir.

Jüri Üyeleri İmza

Dr. Öğr. Üyesi Derya ARDA

Dr. Öğr. Üyesi Tarık YERLİKAYA

Dr. Öğr. Üyesi Halil Nusret BULUŞ

Tez Savunma Tarihi: 19/02/2021

Bu tezin Yüksek lisans tezi olarak gerekli şartları sağladığını onaylarım.

İmza

Dr.Öğr.Üyesi Derya ARDA
Tez Danışmanı

Trakya Üniversitesi Fen Bilimleri Enstitüsü Onayı
Prof. Dr. Hüseyin Rıza Ferhat KARABULUT
Fen Bilimleri Enstitüsü Müdürü

**T.Ü. FEN BİLİMLERİ ENSTİTÜSÜ**

**BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI YÜKSEK LİSANS PROGRAMI**

**DOĞRULUK BEYANI**

Trakya Üniversitesi Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında, tüm verilerin bilimsel ve akademik kurallar çerçevesinde elde edildiğini, kullanılan verilerde tahrifat yapılmadığını, tezin akademik ve etik kurallara uygun olarak yazıldığını, kullanılan tüm literatür bilgilerinin bilimsel normlara uygun bir şekilde kaynak gösterilerek ilgili tezde yer aldığını ve bu tezin tamamı ya da herhangi bir bölümünün daha önceden Trakya Üniversitesi ya da farklı bir üniversitede tez çalışması olarak sunulmadığını beyan ederim.

*19/02/2021*

*Selin DEMİRBİLEK AYYILDIZ*

Yüksek Lisans Tezi
Güvenli Elektronik Seçim İçin Sır Paylaşım Şemalarının Uygulanması
T.Ü. Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

# ÖZET

Seçimler demokrasinin vazgeçilmez en temel öğesidir. Bu nedenle seçimlerin güvenilir, hızlı, doğru ve herhangi bir şüpheye yer verilmeyecek şekilde yapılması önemlidir. Geleneksel olarak kâğıt üzerinde oy kullanma yöntemiyle gerçekleştirilen seçimlerde oy pusulalarının basılması ve dağıtımı, salonda ve sandık başında görevli olan sorumluların görevlendirilmesi ve seçim sonucunda oyların sayılması ülkeler için büyük bir maliyete neden olmaktadır. Geçersiz oy kaybını engellemek, oy sayımındaki hız ve sistemin güvenilirliği gibi konuları amaç edinerek geliştirilen elektronik oylama sistemlerinin önemli getirilere sahip olacağı düşüncesi ile çalışmalar devam etmektedir. Bu nedenle teknolojinin gelişmesi ve bilgisayar kullanımının artması ile çeşitli ülkelerde elektronik seçimlerin bir bilgisayardan ya da tasarlanan elektronik cihazdan daha hızlı, daha güvenilir ve daha az maliyetle yapılması fikri kabul görmektedir. Ancak her teknolojik gelişme ile gelen birçok soru işareti ve olumsuzluk bu sistemler için de geçerli olup, tartışmalar ve çalışmalar özellikle sistemin güvenilirliğini arttırmak üzerine yoğunlaşmaktadır. İçinde yaşadığımız mevcut pandemi koşulları da göz önünde bulundurulduğunda ve bilgisayar okuryazarlığının artmakta olduğu dijitalleşen dünyada e-seçim sisteminin de güvenilirliğini kanıtlanmış elektronik sistemler ile yapılması araştırılmaya değer bir problem olarak karşımıza çıkmaktadır.

E-seçim sisteminin en önemli ve hassas noktası güvenlik ihtiyacıdır. Bu güvenlik ihtiyaçları içerisinde seçmenin gizliliği, kanunlara göre oyunu kullanabilmesi, sistemin güvenilirliği, oyların değiştirilememesi, oyların kime kullanıldığının anlaşılamaması gerekliliği, oyların doğru sayılması ve sistemin saldırılara karşı dayanıklı olması gibi konular sayılabilir.

Bu tezde e-seçim uygulaması için internet bağlantısı olmayan bir bilgisayar veya elektronik cihaz üzerinde farklı kriptografik yapılar kullanılarak oylama yapılmasına imkan veren bir yazılım geliştirildi. Bu yazılım sayesinde yapılacak bir e-seçim dışardan gelecek herhangi bir siber saldırıya karşı korunmaktadır. Oy sayma işlemi kullanılan cihazın ya da bilgisayarın kendi içerisinde gerçekleşmektedir. Böylece oy kullanma işlemi bittikten sonra yetkili kişiler o cihazdaki oyların sonucunu öğrenmek için kendilerine verilen şifreleri girerek kısmi oy sonuçlarını alabilmektedir. Daha sonra eşik değerdeki yetkili kişilerin elde ettiği oy sonuçları ile diğer eşik değerdeki yetkililerin elde ettiği oy sonuçları aynı ise toplam oyların doğruluğu onaylanmış olur. Sürecin devamında ise yine görevliler kendilerine ait şifreleri kullanarak toplam oy sonuçlarını AES şifreleme algoritmasıyla şifreleyerek seçim sisteminin kullandığı güvenilir internet hattı üzerinden merkeze iletebilmektedir.

Bu tezde özellikle oylama ve sonuçların doğruluğu için kullanılan kriptografik yapıların e-seçim sisteminde güvenliğe etkisi üzerine odaklanılmıştır. İlk olarak seçmenin sisteme giriş yapabilmesine imkan veren kimlik doğrulama için mesaj özeti fonksiyonu olarak SHA256 kullanılmıştır. Oy kullanma esnasında Shamir'in polinom tabanlı sır paylaşım şeması kullanılarak oylama sonucunun doğruluğu sağlanmıştır. Sonuç olarak geliştirilen bu yazılım ile oy kaybının ve kullanılan oyların değiştirilmesinin önüne geçildiğini söyleyebiliriz. Böylece güvenli bir e-seçim sistemi için geliştirilmiş yazılım içerisinde Sır Paylaşım Şemaları'nın kullanılması hem seçmenin mahremiyetini korumakta hem de oylama sonucunun tek bir kişi veya kurumun tekelinde olmasını engellemektedir.

Yıl : 2021

Sayfa Sayısı : 65

Anahtar Kelimeler : Elektronik Seçim, Elektronik Oylama, Sır Paylaşım Şemaları, Güvenlik

Master's Thesis
Application of Secret Sharing Schemes for Secure Electronic Election System
Trakya University Institute of Natural Sciences
Computer Engineering Department

# ABSTRACT

Elections are indispensable elements of democracy. For this reason, it is important that the choices are made reliably, quickly, accurately and without any doubt. The printing and distribution of ballot papers in elections traditionally held by the method of voting on paper, the assignment of those responsible in the hall and the ballot box, and the counting of the votes as a result of the elections cause a great cost for the countries. Electronic voting systems, which are developed with the aim of preventing the loss of invalid votes, speed in the counting of votes and reliability of the system, continue with the idea that they will have significant returns. Therefore, with the development of technology and the increase in the use of computers, the idea of making electronic selections faster, more reliable and less costly than a computer or designed electronic device is accepted in various countries. However, many questions and negativities that come with every technological development are also valid for these systems, and discussions and studies focus especially on increasing the reliability of the system. Considering the current pandemic conditions we live in, and in the digitalizing world where computer literacy is on the rise, making the e-selection system with proven electronic systems is a problem worth investigating.

The most important and sensitive point of the e-election system is the security need. Among these security needs, issues such as the privacy of the voters, the ability to vote according to the laws, the reliability of the system, the inability to change the votes, the need to not understand who the votes were cast, the correct counting of the votes and the resistance of the system to attacks can be counted.

In this thesis, a software that allows voting by using different cryptographic structures on a computer or electronic device without an internet connection was developed for e-election application. Thanks to this software, an e-election to be made is

protected against any cyber-attack from outside. The counting of votes takes place within the device or computer used. Thus, after the voting process is completed, authorized persons can get partial voting results by entering the passwords given to them to learn the results of the votes on that device. Then, if the results of the votes obtained by the officials with the threshold value are the same, the accuracy of the total votes is confirmed. In the continuation of the process, the officials can transmit the total vote results with the AES encryption algorithm in an encrypted form to the headquarters via the reliable internet line used by the election system, again using their own passwords.

This thesis focuses on the effect of cryptographic structures used for voting and the accuracy of the results on the security of the e-election system. First of all, SHA256 is used as the message digest function for authentication, which allows the voter to log into the system. During voting, the accuracy of the voting result was ensured by using Shamir's polynomial-based secret sharing scheme. As a result, we can say that with this software developed, loss of votes and changing the votes cast is prevented. Thus, the use of Secret Sharing Schemes in software developed for a secure e-election system protects the privacy of the voter and prevents the voting result from being monopolized by a single person or institution.

Year : 2021

Number of Pages : 65

Keywords : Electronics Election, Electronic Voting, Secret Sharing Schemes, Security

# TEŞEKKÜR

Lisans eğitimimden yüksek lisans eğitimimin sonuna kadar her konuda desteğini, bilgisini ve tavsiyelerini benden esirgemeyen, istisnasız her durumda beni anlayışla karşılayan ve bana çözüm sunan, tez danışmanlığımı üstlenen çok sevdiğim değerli hocam Dr.Öğr.Üyesi Derya ARDA'ya teşekkürlerimi sunarım.

Beni bu günlere getiren, her zaman yanımda olan ve her koşulda destekleyen AİLEME emekleri ve fedakârlıkları için teşekkür ederim.

Eğitim hayatım boyunca beni daima dinleyen ve elinden gelen yardımı benden esirgemeyen Okcan AYYILDIZ'a teşekkür ederim.

# İÇİNDEKİLER

**ÖZET** ..... iv
**ABSTRACT** ..... vi
**TEŞEKKÜR** ..... viii
**İÇİNDEKİLER** ..... ix
**KISALTMALAR DİZİNİ** ..... xi
**ŞEKİLLER DİZİNİ** ..... xii
**ÇİZELGELER DİZİNİ** ..... xiv
**BÖLÜM 1** ..... 1
**GİRİŞ** ..... 1
**BÖLÜM 2** ..... 4
2.1. Elektronik Seçim (E – Seçim) ..... 4
2.2. E-Seçim Tarihçesi ..... 4
2.3. E-Seçim'in Faydaları ..... 5
2.4. E-Seçimlerde Yaşanan Sorunlar ..... 6
2.5. Elektronik Oy Verme Sistemlerinde Güvenlik ..... 6
2.6. Seçmenin Güvenini Arttırmak İçin Neler Yapılmalıdır? ..... 7
2.7. E-Seçimin Temel Gereksinimleri ..... 7
**BÖLÜM 3** ..... 10
**KRİPTOLOJİ** ..... 10
3.1. Kriptoloji Nedir? ..... 10
3.2. Asimetrik Şifreleme Algoritması ..... 11
3.3. Simetrik Şifreleme Algoritmaları ..... 11
3.4. AES Algoritması ..... 12
3.5. Kriptografik Mesaj Özeti Fonksiyonları ..... 13
3.6. SHA-256 Özet Algoritması ..... 14
**BÖLÜM 4** ..... 16
**SIR PAYLAŞIM ŞEMALARI** ..... 16
4.1. Sır Paylaşım Şemaları ..... 16
4.2. Shamir'in Lagrange İnterpolasyon Polinom Tabanlı Sır Paylaşım Şeması ..... 17

4.3. Shamir'in Polinomsal Sır Paylaşım Şeması Tabanlı E-Oylama Uygulaması...19
**BÖLÜM 5**...24
**GÜVENLİ E-SEÇİM SİSTEMİ UYGULAMASI**...24
5.1. Güvenli E-Oylama için Genel Tasarım Kısmı...24
5.1.1 E-Seçim Sistemine Giriş...24
5.1.2. E-Seçim Oy Kullanma Ekranı...27
5.1.3. E-Seçim Sistemi Yöneticisi...29
5.2. Sır Paylaşım Şeması Tabanlı Homomorfik E-Oylama Uygulaması...33
**BÖLÜM 6**...39
**SONUÇLAR VE TARTIŞMA**...39
**KAYNAKLAR**...41
**EKLER**...44
**EK A. Kullanılan Teknolojiler**...44
**EK B. Tez İçin Geliştirilen Uygulamanın Kodlarının Açıklanması**...44
**EK C. Tez İçin Geliştirilen Uygulamanın Algoritmaları**...48
**TEZ ÖĞRENCİSİNE AİT TEZ İLE İLGİLİ BİLİMSEL FAALİYETLER**...51

# KISALTMALAR DİZİNİ

| | |
|---|---|
| AES | Advanced Encryption Standart (Gelişmiş Kodlama Standardı) |
| DRE | Direct Recording Elektronic Voting Systems (Doğrudan Kayıtlı Elektronik Oylama Sistemleri) |
| ECC | Elliptic Curve Cryptography |
| MS SQL Server | Microsoft SQL(Structure Query Language) (Yapılandırılmış Sorgu Dili) |
| RSA | Rivest-Shamir-Adleman |
| SEÇSİS | Seçim Bilişim Sistemi |
| SHA | Secure Hashing Algorithm (Güvenli Hashing Algoritması) |
| SMS | Short Message Service (Kısa Mesaj Hizmeti) |
| YSK | Yüksek Seçim Kurulu |

# ŞEKİLLER DİZİNİ

Şekil 3.1.Asimetrik şifreleme algoritması şeması. 11
Şekil 3.2.Simetrik şifreleme algoritması şeması. 11
Şekil 3.3.Toplam oyların AES-256 algoritmasıyla şifrelenerek oy toplama merkezine gönderilmesi. 13
Şekil 3.4.Verinin SHA-256 algoritması ve base-64 sonucu. 13
Şekil 3.5.SHA256 özet fonksiyonun genel yapısı. 15
Şekil 5.1.E-seçim sistemi login ekranı. 25
Şekil 5.2.Veri tabanında TC kimlik ve password'un SHA256 ile mesaj özeti. 25
Şekil 5.3.Hatalı TC kimlik ve parola girildiğinde çıkan uyarı mesajı. 26
Şekil 5.4.SMS giriş ekranı. 26
Şekil 5.5.Oy kullanma ekranı. 27
Şekil 5.6.Oy onaylama ekranı. 28
Şekil 5.7.Sistem yönetici ekranı. 29
Şekil 5.8.Yeni aday ekleme ekranı. 30
Şekil 5.9.Aday listeleme ekranı. 30
Şekil 5.10.Aday silme ekranı. 31
Şekil 5.11.Yeni seçmen ekleme ekranı. 31
Şekil 5.12.Seçmen listeleme ekranı. 32
Şekil 5.13.Seçmen silme ekranı. 32
Şekil 5.14. 1. ve 2. Yetkili kişilerle elde edilen oylama sonucu ekranı. 33
Şekil 5.15. 2. ve 3. Yetkililer ile toplam oy sonucuna ulaşma. 34
Şekil 5.16. 7 Seçmen ve 4 parti ile oylama kısmı. 34
Şekil 5.17.Partilerin aldıkları oy sayısı. 35
Şekil 5.18.Oylama sonuçlarının yetkililer tarafından doğrulanması. 36
Şekil 5.19.Oylama sonuçlarının şifrelenmesi için yetkililer tarafından anahtar değerlerinin girilmesi. 36

Şekil 5.20.Her bir N oylama cihazındaki toplam oy sonucunun AES ile şifrelenerek merkeze gönderilmesi ve toplam oyun hesaplanması süreci. ..... 37
Şekil 5.21.Merkezdeki yetkililerin gizli anahtarlarını birleştirerek şifreli toplam oyu AES ile çözerek sonucu görüntülemesi..... 37
Şekil 5.22.Önerilen e-seçim siteminin akış şeması. ..... 38

# ÇİZELGELER DİZİNİ

Çizelge 4.1. Shamir’in polinom tabanlı e-oylama örneği. ..... 20
Çizelge 4.2. Lagrange interpolasyon ile elde edilen toplam e-oy sonucu..... 23

# BÖLÜM 1

# GİRİŞ

Günümüzde insanların büyük bir kısmı demokratik sistemlerle yönetilmektedir. E-devletin bu yönetim biçimini mümkün olduğunca etkileşimli ve katılımlı olmasını sağlamak için teknolojinin kullanılmasıyla e-demokrasi kavramı ortaya çıkmıştır.

E-seçim ise e-demokrasinin en önemli noktalarından biridir. E-seçim tüm seçim sürecindeki aşamaları kapsamakla birlikte, e-oylama bu süreçte teknolojinin getirilerinden en çok faydalanılacak önemli bir aktivitedir. E-oylamanın getirileri olarak oy sayımının hızlı olması, hiçbir oy kaybının olmadığının, fazladan oy eklenmediğinin kanıtı, oy sahtekarlığının önüne geçilmesi ve ayrıca özel ihtiyaçları olan vatandaşların da sistemi kullanabilecekleri şekilde tasarlanmasıyla katılımın artmasını sağlamak şeklinde sayılabilir.

Teknoloji çağına girilmesi ile birlikte internet üzerinde bilgi akışı artmaya başlamış ve günlük hayatta yaptığımız birçok işlem sağladığı kolaylıklar nedeniyle bilgisayar ortamına ya da akıllı cihazlara taşınmıştır. Geleneksel yapılan seçimlerde oy pusulalarının, sandıkların kullanılması, seçimde salon ve bina sorumlularının görevlendirilmesi büyük bir maliyet oluşturmaktadır. Seçim öncesi hazırlıkların yapılması, seçmen listelerinin hazırlanması uzun bir hazırlık sürecine ihtiyaç duyulmasına neden olmaktadır. Ülke ekonomisini etkileyen yüksek maliyetli bu geleneksel sistemden vazgeçerek elektronik ortamda güvenilirliği kanıtlanmış seçim sistemi kullanmak teknolojinin gelişmesi, zamanın insanlar için öneminin artması sonucu bir ihtiyaç haline gelmiştir. Ancak elektronik ortamda verilerin güvenilirliği ve gizliliği sorunu karşımıza çıkmaktadır.

Literatürde e-seçimde güvenlik konularında pek çok çalışmalar yapılmaktadır. Salman (2016)'nın "Elektronik Seçim Sistemlerinde Güvenlik Amaçlı Algoritma Önerisi" adlı Yüksek Lisans Tezinde genel olarak e-seçimde kullanılan kriptografik protokollerden, dünyada kullanılan e-seçim mimarilerini inceleyerek yeni bir güvenli e-seçim algoritması önerisinde bulunmuştur. Alemdaroğlu, (2014) de "Mercuri Modeline Dayalı Örnek Elektronik Seçim Uygulaması*"* adlı tezinde Mercuri modeli üzerinden bir e-seçim uygulaması yapmıştır. Çinpolat (2005)'ın "Türkiye'deki Genel Seçimler İçin Bir Elektronik Seçim Modeli Uygulaması " adlı Yüksek Lisans Tezinde Türkiye'deki seçim sistemini incelemiş ve zaman, maliyet ve güvenilirlik konusunda iyi olduğunu savunduğu bir elektronik sandık tasarlamışlardır. Şahin , (2005)'nin "Elektronik Seçim Modellerinin Analizi ve Bir Model Önerisi" adlı Yüksek Lisans Tezinde e-seçim sistemlerini inceleyerek, küçük ölçekli seçimler için bir model önermiştir. Yuan, Li, Guo, Hu ve Wang (2017) makalelerinde seçmenler ve sayım merkezi arasındaki güven problemini ortadan kaldırmak için Mignotte (1983)'nin eşik sır paylaşım şemasını kullanmışlardır. Iftene (2007)'de e-oylama uygulamasında Çin kalan teoremi kullanarak genel sır paylaşım şemasını önermiştir. Schoenmakers (1999)'da kamuya açık olarak doğrulanabilir sır paylaşım şeması ve bunun e-oylama uygulamasını önermiştir. Nair vd , (2014) makalelerinde Shamir (1979)'in sır paylaşımını kullanarak e-seçim sonuçlarının güvenli olarak hesaplandığını ortaya koymuşlardır.

Yapılan çalışmalardan esinlenerek güvenli bir e-seçim için kriptografik protokolleri de kullanarak oylama sonuçlarının güvenli bir şekilde hesaplanmasında Shamir'in polinomsal sır paylaşım şemasından faydalanılarak bir e-seçim özellikle e-oylama yazılımı geliştirilmiştir.

Bu tezde e-seçim uygulaması internet bağlantısı olmayan bir bilgisayar veya elektronik cihaz üzerinde oylama yapılması şeklinde geliştirilmiştir. Bu sayede herhangi bir siber saldırıya karşı korunmuş olur. İlk olarak seçmen oy kullanılacak sisteme girişte kimlik doğrulama için SHA256 mesaj özeti algoritması kullanılmıştır. Oylama esnasında her seçmenin oyu bir fonksiyona sokularak oy kodlanmıştır. Oy sayma işlemi kullanılan cihazın ya da bilgisayarın kendi içinde yapılmıştır. Oy kullanma işlemi bittikten sonra yetkili kişiler kendilerine verilen kısmi gizli anahtarlarını birleştirerek oy sonuçlarını AES şifreleme algoritmasıyla şifreleyerek seçim sisteminin kullanacağı güvenilir internet hattından merkeze gönderecektir. Bu tezde özellikle yapılan oylama sonucunun doğruluğu

için Shamir'in polinom tabanlı şemasından faydalanılmıştır. Böylece herhangi bir oy kaybı ya da herhangi bir oy değiştirilmesinin önüne geçildiği söylenebilir.

İçinde yaşadığımız mevcut pandemi koşulları da göz önünde bulundurulduğunda ve bilgisayar okur yazarlığının artmakta olduğu dijitalleşen dünyada e-seçim sisteminin de güvenilirliğini kanıtlanmış elektronik sistemler ile yapılması araştırılmaya ve geliştirilmeye değer bir problem olarak karşımıza çıkmaktadır. Yakın bir gelecekte de ülkemizde milli yazılımlarla birlikte güvenli, şeffaf, herkesin güvenini kazanmış bir e-seçim sistemine adım atılacağı düşünülmektedir.

# BÖLÜM 2

# ELEKTRONİK SEÇİM

## 2.1. Elektronik Seçim (E – Seçim)

Gelişmiş ülkeler genellikle demokrasi ile yönetilmektedir. Demokrasi de temelde halkın oy kullanarak kendisini yönetecek olan kişi veya kişileri seçimle belirlemesine dayanır. Ülkemizde seçimler geleneksel yöntemlerle yapılmaktadır. Oy kullanma ve oy sayma işlemlerinin geleneksel şekilde kağıt üzerinden değil, teknolojiden faydalanılarak elektronik ortamda yapıldığı seçimlere elektronik seçim denir. Elektronik seçim için kısaltma olarak e- öneki kullanılır. Seçim sistemi internet tabanlı ise i- öneki kullanılmaktadır. Elektronik seçim sistemleri bir bilgisayar, mobil cihaz veya özel tasarlanmış cihazlarla genel olarak internet protokolü kullanılarak yapılan oy verme işlemidir (Salman, 2016).

E-seçim sisteminin en önemli noktaları güvenlik ihtiyacıdır. Bu güvenlik ihtiyaçları seçmenin gizliliği, kanunlara göre oyunu kullanabilmesi, sistemin güvenilirliği, oyların değiştirilememesi, oyların doğru sayılması ve sistemin saldırılara karşı dayanıklı olması gibi konular sayılabilir.

## 2.2. E-Seçim Tarihçesi

Elektronik seçim için kullanılan teknolojiler olarak delikli kartlar, optik okuma sistemleri DRE(Direct Recording Elektronic voting systems) adı verilen özel oy kullanma kioksları sayılabilir. Ayrıca internetten, telefon hattından oy kullanma sistemleri de e-seçim için kullanılmaktadır (Telciler, 2017). Yapılan araştırmalar sonucunda farklı ülkelerde gerçekleştirilen e-seçimde genel olarak iki yaklaşımdan söz edilebilir. Birisi

oylamanın belirli oy kullanma merkezlerinde yapıldığı seçimler diğeri internet üzerinden yapılan seçimler şeklindedir (Çetinkaya, 2006).

Elektronik seçim sistemleri 1964 ‘den beri kullanılmaktadır. Aynı yılda ABD’de 7 eyalet delikli kartlar ile e-seçim yapmışlardır (Saltman, 1978). Brezilya ve Hindistan DRE makinelerini kullanarak bir e-seçim yapmışlardır.

Belçika, Hollanda, ABD, Rusya, Brezilya, Hindistan, Azerbaycan ve Paraguay’da belirli oy kullanma merkezlerinde genel e-seçim yapılmıştır. İngiltere, İsviçre, Fransa, İspanya ve Estonya gibi Avrupa ülkeleri internet üzerinden e-seçim gerçekleştirmişlerdir.

Elektronik oy verme aygıtları aracılığı ile oy kullanma işleminin bütün ülkede uygulandığı ilk ülke 1996 seçimleri ile Brezilya olurken, ülke çapında en fazla seçmen ile kullanıldığı ülke 2004 yılındaki seçimlerle Hindistan olmuştur. Seçimlerde teknoloji kullanımı delikli kart ve işaretle-algıla sistemleriyle başlamıştır. Bu sistemleri ilk kullanan ülkelerden ABD’de 2000 yılındaki başkanlık seçimleri bu sistemlerden kaynaklanan usulsüzlükler ve tartışmalı oy sayımları nedeniyle doğrudan kaydeden elektronik (DKE) sisteme yönelmiştir(USEAC, 2005a) ve (USEAC, 2005b). Hollanda’da 2004 yılından beri yerel uygulamalar yapılmış, son olarak 2007 seçimlerinin elektronik yapılması kararı alınmıştır (Pieters, 2006). İnternet üzerinden e-seçimi ülke çapında ilk defa uygulayan ülke Estonya ve ikinci uygulayan ülke Norveç’tir (Kiraz, Birinci & Boyacı, 2012). Türkiye’de, 1986 yılında Hacettepe Üniversitesi’nde ilk e-seçim sistemi çalışmaları YSK’nın 1989 yılında kabul ettiği SEÇSİS Projesi ile başlamıştır.

### 2.3. E-Seçim’in Faydaları

Klasik seçimlerden önce seçimler için ön hazırlık sürecinin olması gerekmektedir. Elektronik seçim ile birlikte bu hazırlık süresi kısalmış olacaktır. Ayrıca seçimlerin internet ortamına taşınması ile geleneksel seçimlerde kullanılan oy pusulalarının basım ve dağıtımı, sandık başında görevli personel giderleri gibi maliyetlerin düşmesi ile ülke ekonomisine de katkıda bulunulacağı düşünülmektedir. Oy kullanırken uzun süre kuyruklarda beklemek seçmenlerin oy kullanmak istememesine neden olan faktörlerden biridir. E-seçim sistemi ile istediğimiz yerden devlet tarafından belirlenen süre içerisinde oyumuzu kullanabiliriz. Geleneksel seçimlerde ulaşım ve bedensel engelleri sebebiyle sandık başına gelme konusunda zorluk çeken seçmenler de kolaylıkla oylarını kullanabilir. Seçmenlerin yaşadığı bu sorunların ortadan kalkmasıyla oy kullanan

vatandaş sayında artış meydana geleceği düşünülmektedir. Oy sayım esnasında yaşanan sorunlardan biri de oy kullanırken basılan mührün kağıda bulaşması sebebiyle oy verilen partinin belirlenememesi ve oyun geçersiz sayılmasıdır. Ayrıca seçim işlemi elektronik ortamda yapıldığında fiziksel bir sayım işlemi yapılmayacağından dolayı seçim sonuçlarının açıklanması da daha hızlı olacaktır.

### 2.4. E-Seçimlerde Yaşanan Sorunlar

Elektronik seçim sistemleri elektronik ortamda ve internet üzerinde gerçekleştirildiklerinden dolayı seçmenin seçimin güvenliği ve güvenilir olup olmadığı ile ilgili soru işaretleri olmuştur. Geliştirmelerle ve yeni yöntemlerin kullanılması ile elektronik seçim sistemleri daha da yaygınlaşsa bile alanda güvenlik ve şüphelerden dolayı yeni düşünce ve fikirlerle yeni yöntem ve teknikler denenmeye devam etmektedir (Salman, 2016). Elektronik ortamda bir kere oy kullanmış olan seçmen birden fazla oy kullanamamalıdır ve hangi seçmenin kime oy verdiği erişilemez olmalıdır. 2010 yılında Michigan Üniversitesi öğrencileri, Colombia eyaletinde yapılan e-seçimi hacklemişler, oyları değiştirmişlerdir (Wheaton, 2015). Seçim sistemi üzerinde oylar doğru bir şekilde kaydedilmeli ve değiştirilmemelidir. İnternet üzerinden oy sonuçlarını etkileyecek herhangi bir müdahale ve saldırı olması engellenmelidir. Başarısız sonuçlanan bir seçim sonucu örneği verecek olursak ABD 2006 genel seçimlerinde, Florida ve Miami'de, Cumhuriyetçi adaya verilen oyların Demokrat adaya kaydedildiği bulundu. Yapılan incelemede sorunun dokunmatik ekrandan kaynaklandığı belirlendi (Telciler, 2017). ABD, Brezilya, Japonya, Güney Kore gibi ülkeler elektronik seçimler yapmışlar, ancak sonuçlar ihtilaflı olmuştur ( Kim & Lee, 2005).

### 2.5. Elektronik Oy Verme Sistemlerinde Güvenlik

Geleneksel olarak yapılan seçimlerde oy pusulasının yerini alması için hızla gelişen teknolojiden faydalanılarak elektronik oylama ve e-seçim sistemleri üzerindeki çalışmalar ve uygulamalar geliştirilmektedir. Geliştirilecek e-seçim sistemlerindeki amaçlar arasında seçim maliyetlerinin azaltılması, seçim sürecinin hızlı ve verimli olması, seçim sonuçlarının doğru ve şaibesiz olarak hızını ve doğruluğunu arttırmak, dolayısıyla seçim süreçlerine olan kamu güvenini ve demokratik katılımı arttırmak da bulunmaktadır.

Elektronik oy verme sistemleri teorik gelişmelerin yanı sıra bazı ülkelerdeki seçimlerde başarı ile kullanılmaya başlanmıştır. Ancak bu sistemlerin de bazı güvenlik sorunları vardır (Akın, 2006).

Elektronik seçim ve e-oylama gibi uygulamalarda amaç, sistemin her aşamasında gizlilik, bütünlük, kimlik denetimi gibi temel kriptografik gereklilikler sağlanabilmelidir. E-seçim sistemi açık yazılım ile geliştirilmeli ve kaynak kod incelemeye açık olmalıdır. Sisteme ve iletişim ağlarına yapılacak olası saldırılara karşı ve kötü niyetli otoritelere karşı önlem alınmalıdır (Çetinkaya, 2006).

## 2.6. Seçmenin Güvenini Arttırmak İçin Neler Yapılmalıdır?

Seçimde 18 yaşını doldurmuş, seçmen kütüğünde kaydı bulunan her ülke vatandaşı halk oylamasında oy kullanabilir. Demokrasinin doğru bir şekilde işlemesi adına yapılan seçimlerde seçmenin kimliği her zaman gizli tutulmalıdır ve seçmenin oy kullanırken hangi kişi veya partiyi seçtiği erişilemez olmalıdır. Oy kullanma hakkına sahip her vatandaş bir kereye mahsus oy kullanabilir. Seçimin güvenilirliğini sağlamak amacıyla bir kere oyunu kullanmış olan kişilerin tekrar oy kullanmasına engel olunmalıdır ve oy kullanma hakkı olmayan kişilerin sisteme giriş yapması engellenmelidir. Farklı kişilerin kimlikleriyle onlar adına oy kullanılmasının önüne geçilmelidir. Seçim sonuçlarını sayım aşamasında ve sonuçların tutanağa geçirilerek kamuoyuna duyurulması aşamalarında kullanılan oyların içeriğinin değiştirilemez olması gerekmektedir. Tüm oylar sayılmalı ve herhangi bir nedenle sayılamayan eksik oy kalmamalıdır.

## 2.7. E-Seçimin Temel Gereksinimleri

Çetinkaya ve Çetinkaya (2006)'ya göre e-seçim temel gereksinimlerini şöyle sıralayabiliriz.

**Seçmenin Gizliliği**: Seçmen ile kullandığı oy arasında bir ilişki kurulamamasıdır.

**Seçme Hakkı**: Sadece seçmen olanların oy kullanabilmesidir.

**Seçimin Dürüstlüğü**: Seçim sonuçlarının seçim bitmeden sayılamamasıdır.

**Tek Oy:** Bir seçmenin sadece bir oyunun sayılmasıdır.

**Sistemin Doğruluğu**: Oyların doğru sayılmasıdır. Seçim sisteminin doğruluğunun sağlanabilmesi için;

- Kullanılan bütün oylar sayılmalıdır,
- Herhangi bir oy değiştirilememeli, silinememeli, kopyalanıp çoğaltılamamalı,
- Bir seçmenin yalnız bir oyu sayılmalıdır.

**Sistemin Sağlamlığı**: Kötü niyetli kişiler ya da kuruluşlar, otoriteler vb sistemi ve seçimi bozamamalıdır. Sisteminin sağlamlığı için aşağıdakiler sağlanmalıdır:

- Sistem dışardan gelecek her türlü saldırılara karşı korunuyor olmalıdır.
- Kriptografik teknikler gelecek için de daha güçlü ve hızlı olmalı. Şifreler kırılamamalıdır.
- Teknik altyapı sağlam olmalıdır. Uygulamaya temel teşkil eden e-seçim protokolünde, kesintisiz hatlar, anonim kanallar vb. kullanıldığı varsayılıyorsa bu teknik altyapı sağlanmalıdır.

**Oy Kullanmama Hakkı**: Seçmenin oy kullanmak istemediği taktirde oy kullanmamasıdır. Bu durumda seçmen yerine bir başkası veya otoriteler oy kullanamamalıdırlar.

**Sonuçların İlan Edilmesi**: Seçim sonuçları ve gerekli bilgiler seçim sonunda basın yayın yoluyla ve internet aracılığıyla ilan edilir.

**Sistemin Geçerlenebilirliği**: Sayım sonucunun doğru olduğunun gösterilebilmesidir.

**Sistemin Doğrulanabilirliği:** Seçimin ve sayımın doğru şekilde yapıldığının gösterilebilmesidir.

**Sistemin Etkinliği:** Kayıt, seçim ve sayım gibi işlemlerin tamamı etkin bir biçimde yapılmalı. Klasik seçimlere göre oylar daha kısa sürede sayılmalıdır.

**Kolay Kullanım:** Seçmenin oyunu kullanabilmesi için kullanıcı ara yüzlerinin ve seçim ortamının ergonomik olması gerekmektedir.

**Açık Yazılım:** Açık yazılım yapılmalı ve kaynak kod incelemeye açık olmalıdır. Sistemin güvenliği kaynak kod gizliliğine bağlanamaz. Sadece şifreler gizli olmalıdır ve iyi saklanmalıdır.

**Yedekleme ve Fiziksel Koruma**: Sistemin herhangi bir teknik arızaya karşı yedekleme ve fiziksel koruma mekanizması olmalıdır. Tek bir elektronik cihaza güvenilmemelidir.

**Seçimin Şeffaflığı:** Oyların ve seçmenlerin gizliliğine zarar vermeden, e-seçim sistemlerinde maksimum şeffaflık hedeflenmelidir.

**Oyların Saklanması:** Oyların ve gerekli seçim bilgilerinin sayım sonrasında, elektronik ve basılı ortamda saklanmasıdır.

**Oyların Tekrar Sayılabilmesi**: Hem elektronik hem basılı ortamda saklanan oyların gerekirse yeniden sayılabilmesidir.

# BÖLÜM 3

# KRİPTOLOJİ

## 3.1. Kriptoloji Nedir?

Kriptoloji, kriptografi ve kriptoanaliz olmak üzere iki alanı içeren şifreleme bilimidir. Mesajın orijinal içeriğini koruyarak, metnin değiştirilmesi tekniğiyle yapılmasını sunan kriptografi, teknolojinin gelişmesiyle birlikte sistemlerin en önemli gereksinimlerinden biri olarak bilgi güvenliği ve gizliliğinin sağlanması için çeşitli yöntemlerle yaygın olarak kullanılmaktadır. Bu yöntemlerde gizlilik, güvenilirlik, veri bütünlüğü, erişilebilirlik, kimlik doğrulama ve reddedilemezlik esasları üzerinde çalışılır. Günümüzde kriptografi matematiksel işlemlerin desteklediği şifreleme, anahtarlama ve çözümleme algoritmaları aracılığıyla gerçekleştirilmektedir.

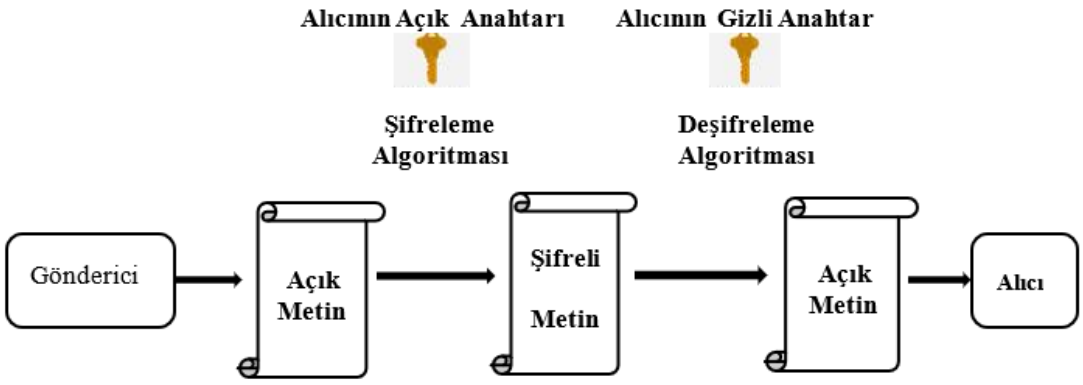
Temel olarak kriptoloji haberleşmede veri güvenliğini sağlayan şifreleme cihazlarını, bu cihazlarda kullanılan algoritmaların tasarımını ve bu algoritmaların güvenilirliğini araştırır.

Kriptanaliz ise şifrelenmiş metinleri çözebilmek için sistemlerin güvenliklerini inceleyen ve zayıf yanlarını bulmaya çalışan daldır. Anahtara sahip olmadan bir gizli metnin açık halini bulma bilimi olarak da nitelendirilebilir (Stinson, 2002).

Şifreleme algoritmaları asimetrik (açık anahtarlı) ve simetrik (gizli anahtarlı) algoritmalar olarak iki kategoride incelenmektedir.

### 3.2. Asimetrik Şifreleme Algoritması

Asimetrik şifreleme algoritmalarında şifrelemede açık bir anahtar kullanılırken şifre çözmede gizli anahtar kullanır. Asimetrik şifreleme algoritmalarından bazıları RSA (Rivest, Shamir & Adleman, 1978), ECC (Koblitz , 1987) ve Elgamal (Elgamal, 1985) dır. Bu algoritmanın çalışma mantığı Şekil 3.1' de verilmiştir.

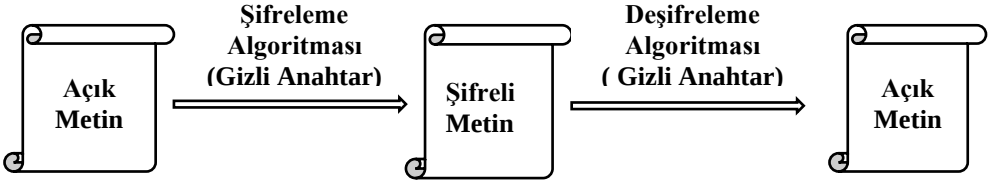



Şekil 3.1. Asimetrik şifreleme algoritması şeması.

Kriptografi sadece veriyi gizlemek, iletmek ve saldırıları engellemek gibi konulara çözüm aramaz. Elektronik imza, elektronik seçim vb. gibi farklı alanlarda da kullanılır. Şifrelemede kullanılan anahtarın korunması için pek çok yöntemler ortaya atılmıştır. Bunlardan birisi de sır paylaşım şemalarıdır.

### 3.3. Simetrik Şifreleme Algoritmaları

Simetrik şifreleme algoritmalarında şifreleme ve şifre çözme işlemlerinde aynı gizli anahtar kullanılır. Şifreleme işleminde açık metin gizli anahtar ile şifrelenirken şifre çözme işleminde de aynı gizli anahtarla şifreli metin çözülür (Stinson, 2002). Simetrik şifreleme algoritmalarının çalışma biçimi Şekil 3.2' de gösterilmiştir. En etkin simetrik algoritmalardan birisi AES şifreleme algoritmasıdır.



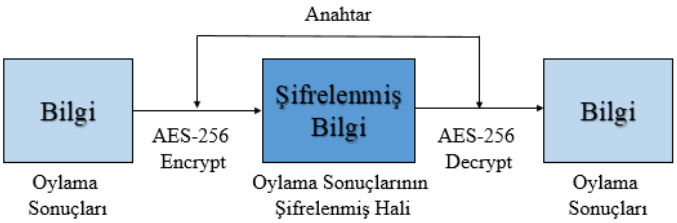

Şekil 3.2. Simetrik şifreleme algoritması şeması.

### 3.4. AES Algoritması

Bilgi paylaşımının artması ile birlikte günümüzde veri gizliliğinin sağlanması konusunu önemli hale getirmiştir. AES Algoritması kriptografide kullanılan en güçlü algoritmalardan biridir. Joan Daemen ve Vincent Rijmen tarafından geliştirilen Rijndael (Daemen & Rijmen,1999) algoritması güvenlik, performans, gerçekleme kolaylığı gibi özellikler dikkate alınarak Amerikan ulusal standartlar ve teknoloji enstitüsü (National Institute of Standards and Technology (NIST)) tarafından gelişmiş kodlama standardı (Advanced Encryption Standard (AES)) olarak seçilmiş ve federal bilgi işleme standardı (Federal Information Processing Standards (FIPS)) olarak yayımlanmıştır (FIPS 197,2001). AES algoritması DES algoritmasına göre daha hızlı ve kırılması daha güç olan bir algoritmadır. Rijndael algoritması Alman bir banka tarafından geliştirildi ve ATM yazılımlarında kullanıldı. Bankacılık sektöründe kullanılmış olması güçlü ve güvenilir bir algoritma olduğunun göstergesidir.

AES simetrik bir şifreleme algoritmasıdır. Simetrik şifrelemede bir anahtar bulunur ve aynı anahtar hem şifreleme işleminde hem de çözme işleminde kullanılır. Dolayısıyla simetrik şifrelemede hem şifreleyende hem de çözücü de aynı anahtar olması gereklidir (Tüfekçi,2018). AES algoritması ile blok şifreleme yapılabilmektedir. Blok şifrelemenin özelliği verilerin bloklar şeklinde alınarak şifreleme/deşifreleme işlemine sokulmasıdır. AES, uzunluğu 128, 192 ve 256 bit olan anahtar kullanabilen ve anahtar ile 128 bitlik veri bloklarını şifreleyebilen simetrik blok şifreleme algoritmasıdır (Daemen&Rijmen,2002). AES şifreleme algoritmasına gelen 128 bitlik blok ilk tur öncesinde 4×4 bayt matrise dönüştürülür ve K0 anahtarı ile xor işlemine tabi tutulur. Her bir turda sırasıyla baytların yer değiştirmesi (Byte Substitution), satırların ötelenmesi (Shift Rows), sütunların karıştırılması (Mix Column) ve tur anahtarı ile xor (Add Round Key) işlemlerine tabi tutulur. Her bir turda bu işlemler tekrarlayarak devam eder. Ancak son turda sütunların karıştırılması yapılmamaktadır (Tüfekçi,2018; Forouzan,2008).

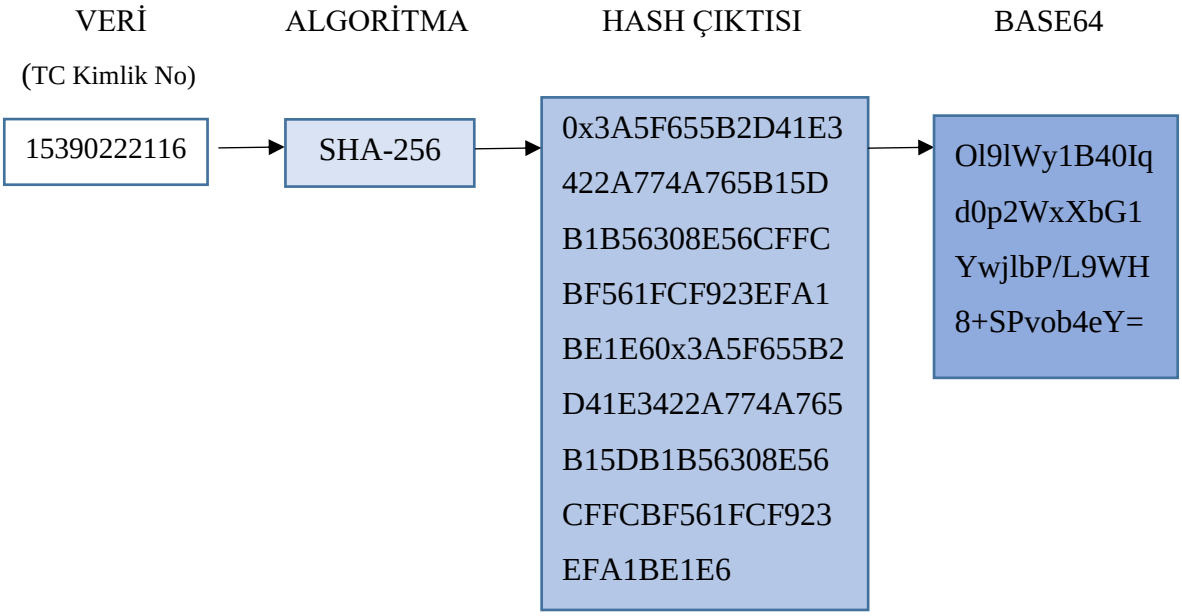
Tezde geliştirmiş olduğumuz uygulamada oy kullanılan elektronik cihazdaki elde edilen toplam oylar yetkili kişilerin kısmi gizli anahtarları ile AES şifreleme algoritmasıyla şifrelenerek Şekil 3.3'de gösterildiği gibi güvenli kanaldan oy toplama merkezine gönderilir.




Şekil 3.3.Toplam oyların AES-256 algoritmasıyla şifrelenerek oy toplama merkezine gönderilmesi.

### 3.5. Kriptografik Mesaj Özeti Fonksiyonları

Mesaj özeti (hash) fonksiyonları istenen verileri belli bir boyuta sığdırmak için kullanılan tek yönlü geri dönüşüm işlemi olmayan matematiksel bir işlemdir. Bir veri mesaj özet algoritmasına sokulduğunda işlem sonucunda elde edilen çıktı ilk veri ile karşılaştırıldığında birbirinden benzersizdir. Örnek verecek olursak TC Kimlik Numarasını SHA-256 mesaj özeti algoritmasına sokalım. Özet sonucu çok uzun bir veri olduğundan veri tabanında az yer tutması amacıyla Base 64'e çevirerek saklanmıştır. Base 64 sonucu olarak Şekil 3.4'deki çıktıyı verecektir. En başta vermiş olduğumuz veri ile mesaj özeti sonucu oluşan çıktı birbirinden benzersiz olmuştur. Tersine çevrilemeyen özet fonksiyonları sayesinde orijinal veri her zaman güvenli ve bilinmez kılınır. İki veri parçasının aynı özeti üretmemesi sebebiyle benzersizdirler.




Şekil 3.4. Verinin SHA-256 algoritması ve base-64 sonucu.

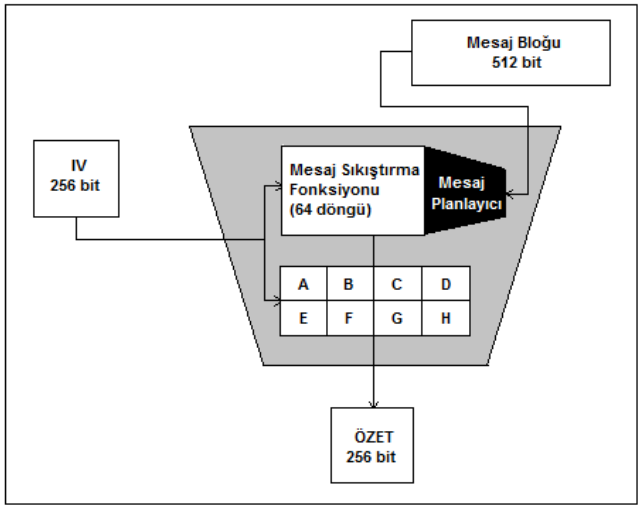
Bazen farklı uzunluktaki metinlerin sabit uzunlukta bir çıktıya çevrilmesinde aynı çıktılar elde edilebilmektedir. Buna çakışma (collision) denilmektedir. Güvenilir ve zor kırılır bir özet için daha uzun karakter kümesi ve daha fazla bit sayısı gerekir. SHA-256 veya SHA-512 mesaj özeti fonksiyonunu örnek olarak verebiliriz (Salman, 2016).

Mesaj özeti fonksiyonları özellikle bilgi güvenliği uygulamalarında kullanılmaktadır. Bunlar arasında sayısal imzalar, mesaj doğrulama kodları(MAC) gibi uygulamalardır. Ayrıca Blockchain uygulamalarında, internet üzerinden yapılan veri alışverişlerinde ve web uygulamalarında kullanıcıların giriş yaptıkları parolaları veri tabanı üzerinde tutulurken özet (Hash) algoritmalarından yararlanılır. Özet algoritmalarının temel özelliği deterministik olmasıdır. Birçok farklı özet fonksiyonları bulunmaktadır. Her özet algoritmasının farklı amaçları vardır. Bazı algoritmalar hız, bazıları güvenlik veya belli veri tiplerini optimize etmek amacıyla kullanılabilir. Bu tezde güvenli e-seçim uygulamasında sisteme girişte kimlik doğrulamak için SHA-256 Hash Algoritması kullanılmıştır.

### 3.6. SHA-256 Özet Algoritması

SHA-256 Özet algoritması Amerika'da kriptoloji konusu üzerinde çalışan Ulusal Güvenlik Ajansı(NSA) tarafından geliştirilmiştir. Bu özet fonksiyonun ayrıntılı açıklaması için (NIST, 2016) standardına bakılabilir. Algoritmaya sokulmak istenen veriler farklı büyüklükte ve yapıda olabilir. SHA-256'nın özelliği verileri aynı yapı ve büyüklüğe çevirmesidir. Özet değerlerinin önceden tahmin edilmesi imkansızdır. Veriler üzerinde yapılan en ufak değişiklikler bile özet değerlerinin tamamen değişmesine neden olabilir. Bu nedenle SHA-256 işlemi deterministik bir işlemdir. Aşağıda Şekil 3.5'de (Erşen, 2017)'den alınmış SHA256 özet fonksiyonun genel yapısı verilmiştir.

Bu tezde güvenli elektronik seçim modelinde kullanıcıların sisteme giriş yapma aşamasında kullanmış oldukları Türkiye Cumhuriyeti Kimlik Numaraları veri tabanında SHA-256 algoritması ile kaydedilmiştir. Bu şekilde kullanıcıların kişisel veri olarak değerlendirdiğimiz TC Kimlik Numarasının herhangi bir kişi veya kişiler tarafından ele geçirilemez olması sağlanır. Aynı zamanda hangi seçmenin hangi adaya oy verdiği bilgisine ulaşılmasının önüne geçilmiş olur.




Şekil 3.5.SHA256 özet fonksiyonun genel yapısı.

# BÖLÜM 4

# SIR PAYLAŞIM ŞEMALARI

## 4.1. Sır Paylaşım Şemaları

Sır paylaşım şemaları birden fazla sayıda kişiler veya kuruluşlar arasında sır bir bilgiyi paylaştırma yoludur. Ancak bu paylaşılan gizli bilgi eşik değerdeki alt kümeler ile yeniden elde edilebilir. Bu alt kümelerin oluşturduğu küme şemanın erişim yapısıdır.

Sır paylaşımı anahtar yönetimi ve anahtar dağıtımı ile ilişkilidir. Bu anahtar dağıtım ve yönetim problemi bütün kriptosistemlerde oldukça sık rastlanan bir problemdir.

Temel olarak $(k, n)$ bir gizlilik paylaşım şemasında $d$ gizliliği $n$ kişi arasında dağıtılır ve herhangi $k$ kişi veya daha fazlası birleşerek gizliliği yeniden elde edebilir. Ancak $k-1$ veya daha az kişi gizliliği elde edemezler (Blakley,1979; Shamir, 1979).

**Tanım:** Bir gizlilik paylaşım şemasında D dağıtıcı ve $P_1,...,P_n$ katılımcılar olmak üzere aşağıdaki protokoller gerçekleştirilir.

- **Dağıtım:** D dağıtıcı S gizliliği $1 \le i \le n$ olmak üzere her $P_i$ katılımcılarına $s_i$ paylaşımlarını dağıtır.
- **Yeniden elde etme:** S gizliliği, $s_i$ paylaşımlarının birleştirilmesi ile yeniden elde edilir. Burada $i \in A$ ve $A \subseteq \{P_1,...,P_n\}$ olmak üzere her yetkilendirilmiş katılımcıların kümesi ile gizlilik elde edilir (Arda ve Buluş 2009; Arda, Buluş, Akgün & Yerlikaya 2008).

Aşağıda gizlilik paylaşım şemasının güvenlik gereksinimleri vurgulanmıştır.

(i) Her yetkilendirilmiş katılımcılar kümesi paylaşımlarını birleştirerek S gizliliğini elde edebilirler.

(ii) Her yetkilendirilmemiş katılımcılar kümesi paylaşımlarını birleştirdiğinde *S* gizliliği hakkında hiçbir bilgiyi elde edemezler.

Bu güvenlik gereksinimlerini doğrulayan Sır Paylaşım Şeması mükemmel olarak adlandırılır.

### 4.2. Shamir'in Lagrange İnterpolasyon Polinom Tabanlı Sır Paylaşım Şeması

Shamir tarafından önerilen sır paylaşımı polinom interpolasyon tabanlıdır. Bir $(k, n)$ sır paylaşımını elde etmek için, $p \rangle n$ büyük bir asal sayı ve $Z_p$ sonlu bir cisim, $k$ eşik değer ve $a_0 \in Z_p$ sır bilgisini göstersin. $a_1, ..., a_{k-1} \in Z_p$ rastgele elemanları seçilip $k-1$dereceli polinomu kurulur (Blakley, 1979).

$$f(x) = (a_{k-1}x^{k-1} + \ldots + a_1 x + a_0) \in Z_p[x] \qquad (4.1)$$

**Paylaşım Kısmı:**

Paylaşımlar aşağıdaki denklem ile elde edilir ve kullanıcılara dağıtılır.

$$h(x) \equiv (a_{k-1}x^{k-1} + \ldots + a_1 x + a_0) \, mod \, p \qquad (4.2)$$

$y_i = h(x_i) \bmod p$ eşitsizliğine göre anahtar parçaları $(x_i, y_i)$ şeklinde kullanıcılara dağıtılır. $k$ noktası $k-1$dereceli polinomu, $h(x)$ ve $a_0$ gizliliğini belirlemek için yeterlidir.

**Gizliliğin Yeniden Elde Edilmesi:**

$h(x)$ lagrange polinomundan yeniden elde edilir. İlk olarak $l_k(x)$ polinomu şu şekilde tanımlanır.

$$l_t(x) = \prod_{\substack{i=1 \\ i \neq t}}^{k} \frac{x - x_i}{x_t - x_i} mod(p) \qquad (4.3)$$

Lagrange interpolasyon polinomu:

$$p(x) = \sum_{t=1}^{k} y_t l_t(x) \qquad (4.4)$$

$h(x)$ polinomunu ve gizli mesajı yeniden elde etmek için $p(x)$ polinomu hesaplanmalıdır.

$$h(x) \equiv \sum_{t=1}^{k} y_t \prod_{\substack{j=1 \\ j \neq t}}^{k} \frac{x - x_j}{x_t - x_j} (mod\ p) \qquad (4.5)$$

**Örnek 4.1**

GF(29) asal cisminde (2,4) eşik sır paylaşım şeması oluşturalım. Eğer s=$a_1$ = 19 gizli değer olmak üzere $a_2$ = 7 olsun. Buna göre aşağıdaki birinci dereceden polinomu tanımlayalım:

f(x) = 19 + 7x

**Paylaşım Kısmı**

Pay değerleri dört katılımcı için

f(1) = 19 + 7.1 = 26 mod 29 = 26

f(2) = 19 + 7.2 = 33 mod 29 = 4

f(3) = 19 + 7.3 = 40 mod 29 = 11

f(4) = 19 + 7.4 = 47 mod 29 = 18

f(1) =$s_1$ = 26 , f(2) = $s_2$ = 4, f(3) = $s_3$ = 11, f(4) = $s_4$ = 18 olarak hesaplanır.

**Yeniden Elde Etme Kısmı**

Sırrı yeniden elde etmek için her bir dört katılımcıdan iki katılımcının bir araya gelmesi gerekir. Örnek olarak, $s_2$, $s_4$ pay değerlerinden, S sırrı aşağıda verilen şekilde elde edilebilir:

($x_1$, $y_1$) =(1,26) ; ($x_2$, $y_2$) =(2,4) ; ($x_3$, $y_3$) =(3,11) ; ($x_4$, $y_4$) =(4,18)

$$S = \left[s_2 \frac{(x - x4)}{(x2 - x4)} + s_4 \frac{(x - x2)}{(x4 - x2)}\right] mod\ 29$$

$$S = \left[4 \frac{(x - 4)}{(2 - 4)} + 18 \frac{(x - 2)}{(4 - 2)}\right] mod\ 29$$

$$S = \left[\frac{4x-16}{-2} + \frac{18x-36}{2}\right] mod\ 29 = \left[\frac{-4x+16+18x-36}{2}\right] mod\ 29$$

$$S = \left[\frac{14x-20}{2}\right] mod\ 29$$

29 =14.2+1

1=29-14.2 =-14+29 =15

$2^{-1}$ mod 29 =15 Paydada bulunan 2'nin mod 29 işlemine göre tersi

$S$=(14x-20).15 $mod\ 29$

$S$=(210x -300) $mod\ 29$

$S$=(7x -10) $mod\ 29$= 7x+19

Bu polinom görüldüğü gibi orijinal S polinomudur. Ayrıca sabit terim olan 19 sır bilgisidir (Arda, Demirbilek & Kavak , 2017).

### 4.3. Shamir'in Polinomsal Sır Paylaşım Şeması Tabanlı E-Oylama Uygulaması

Al-Saidi ve Abdulhadi (2017) makalelerinde sır paylaşım şemasına dayalı yeni bir E-oylama sistemi tasarlamışlardır. Bu makaledeki oylama şeması, her adayın bireysel oylarını hesaplamaya hizmet eden bir yöntemdir. Seçmen sayısı az olduğunda iyi bir güvenlik ve verimlilik sağlayacağını söylemişlerdir. Biz de bu çalışmada oy güvenliğini ve bütünlüğünü korumak için Shamir'in polinom interpolasyon şeması ile bir oylama gerçekleştirdik. Bunun bir örneği aşağıda verilmiştir.

**Örnek 4.2:** Shamir'in (k,n)=(2,3) eşik şemasını kullanarak 4 adayın ve 4 seçmenin olduğu güvenli bir e-seçim için Çizelge 4. 1'de gösterildiği gibi bir e-oylama tasarlayalım. Bu duruma göre her seçmenin oyunun polinomsal olarak şifrelenmesi için

g(x) = (a* x + s) Mod 65537

şeklinde birinci dereceden bir polinom kullanıldı. "s" verilen oyun onluk değeridir.

Çizelge 4.1. Shamir'in polinom tabanlı e-oylama örneği.

| **Adaylar** / **Seçmenler** | A | B | C | D | Oy Değeri | Oyun Onluk Değeri | Oyun Şifrelenmesi İçin Polinom |
|---|---|---|---|---|---|---|---|
| Seçmen 1 | | ✔ | | | 0000/0001/0000/0000 | 256 | 10x+256 |
| Seçmen 2 | ✔ | | | | 0001/0000/0000/0000 | 4096 | 20x+4096 |
| Seçmen 3 | | | ✔ | | 0000/0000/0001/0000 | 16 | 30x+16 |
| Seçmen 4 | | | ✔ | | 0000/0000/0001/0000 | 16 | 40x+16 |

Burada 4 aday ve 4 seçmen için oylamada her bir adayı 4 bitle temsil edip toplam 16 bit kullanılmıştır. Yukarıdaki oylamaya göre Mod alma işlemi için 65537 alınmıştır. Gerekli işlemler aşağıdaki gibi yapılmıştır.

**Oylama Payları Oluşturma Kısmı**

(k,n)=(2,3) şeması için her bir seçmenin oyunun şifrelenmesi ve 3 kısmi oy bilgisi oluşturma için yapılan adımlar şöyledir.

1.Seçmen için oluşturulan rastgele katsayı değeri = 10 olsun;

Pay1=(10*1+256)Mod 65537 = 266

Pay2=(10*2+256)Mod 65537 = 276

Pay3=(10*3+256)Mod 65537 = 286

2. Seçmen için rastgele katsayı değeri = 20 olsun;

Pay1=(20*1+4096)Mod 65537 = 4116

Pay2=(20*2+4096)Mod 65537 = 4136

Pay3=(20*3+4096)Mod 65537 = 4156

3. Seçmen için rastgele katsayı değeri = 30 olsun;

Pay1=(30*1+16)Mod 65537 = 46

Pay2=(30*2+16)Mod 65537 = 76

Pay3=(30*3+16)Mod 65537 = 106

4. Seçmen için rastgele katsayı değeri = 40 olsun;

Pay1=(40*1+16)Mod 65537 = 56

Pay2=(40*2+16)Mod 65537 = 96

Pay3=(40*3+16)Mod 65537 = 136

Her bir Pay1, Pay2, Pay3 kısmi oy toplamları alınır.

1. Yetkili = Tüm seçmenlerin Pay1 değerlerinin toplamını alır.

YPay1= 266+4116+46+56 = 4484

2. Yetkili = Tüm seçmenlerin Pay2 değerlerinin toplamını alır.

YPay2 = 276 + 4136 + 76 + 96 =4584

3. Yetkili = Tüm seçmenlerin Pay3 değerlerinin toplamını alır.

YPay3 = 286 + 4156 + 106 + 136 = 4684

**Toplam oyların yeniden elde edilmesi**

Toplam oy sonucu eşik değerdeki yetkili kişilerin ellerindeki kısmi toplam oyları ile Lagrange interpolasyon metodu kullanılarak hesaplanır. Her bir eşik değerdeki yetkili kişilerin elde ettiği oylama sonucu aynı ise doğrulama yapılıp bu cihazdaki oy sayısının değeri olarak kabul edilir. Aşağıdaki lagrange metodu ile mod 65537' ye göre hesaplanır.

$$Q(x) = \text{YPay1} * \frac{(x - x2)}{(x1 - x2)} + \text{YPay2} * \frac{(X - X1)}{(X2 - X1)}$$

Ypay1: YPay2, YPay1: YPay3 ve YPay2: YPay3 paylarının farklı kombinasyonlarını kullanarak sonuçların hesaplanması aşağıda gösterilmektedir.

YPay1 ve YPay2 için (1.4484) ile (2.4584) için;

$$Q(0) = [4484 * \frac{0-2}{1-2} + 4584 * \frac{0-1}{2-1}] \text{ Mod } 65537$$
$$= 8968 + (-4584)$$
$$= 4384$$

YPay1 ve YPay3 için (1.4484) ile (3.4684) için;

$$Q(0) = [4484 * \frac{0-3}{1-3} + 4684 * \frac{0-1}{3-1}] \text{ Mod } 65537$$
$$= 6726 + (-2342)$$
$$= 4384$$

YPay2 ve YPay3 için (2.4584) ile (3.4684) için;

$$Q(0) = [4584 * \frac{0-3}{2-3} + 4684 * \frac{0-2}{3-2}] \text{ Mod } 65537$$
$$= 13.752 + (-9368)$$
$$= 4384$$

TümYpay1: YPay2, YPay1: YPay3 ve YPay2: YPay3 paylarının sonuçları 4384 olarak aynı olduğu için bir oy kaybı ya da bir şaibe yoktur kararıyla bu oy sonucu doğrulanır. Nihai sonuç, yeniden yapılandırılmış sonucun (4384) ikili olarak kodlanmasıyla elde edilebilir. 4 bitin her aday için temsil edilmesine göre;

4384(Decimal) = 1000100100000 (Binary ama 13 bit)

0001/0001/0010/0000 ( Binary ve 16 bit başına 3 tane 0 koyuldu)

Böylece hangi adayın ne kadar oy aldığı hiçbir kayıp ya da şaibe olmadan Çizelge 4.2'de verildiği gibi hesaplanmıştır. Oyun bütünlüğü, oyu kullananın gizliliği sağlandığı gibi, doğru sonuca ulaşmak için birçok yetkili ile oyların tek elde bulunmasının önüne geçilmiş olur.

Çizelge 4.2. Lagrange interpolasyon ile elde edilen toplam e-oy sonucu.

| **ADAYLAR** | **Toplam Aldıkları oy sayısı** |
|---|---|
| *A* | *1* |
| *B* | *1* |
| *C* | *2* |
| *D* | *0* |

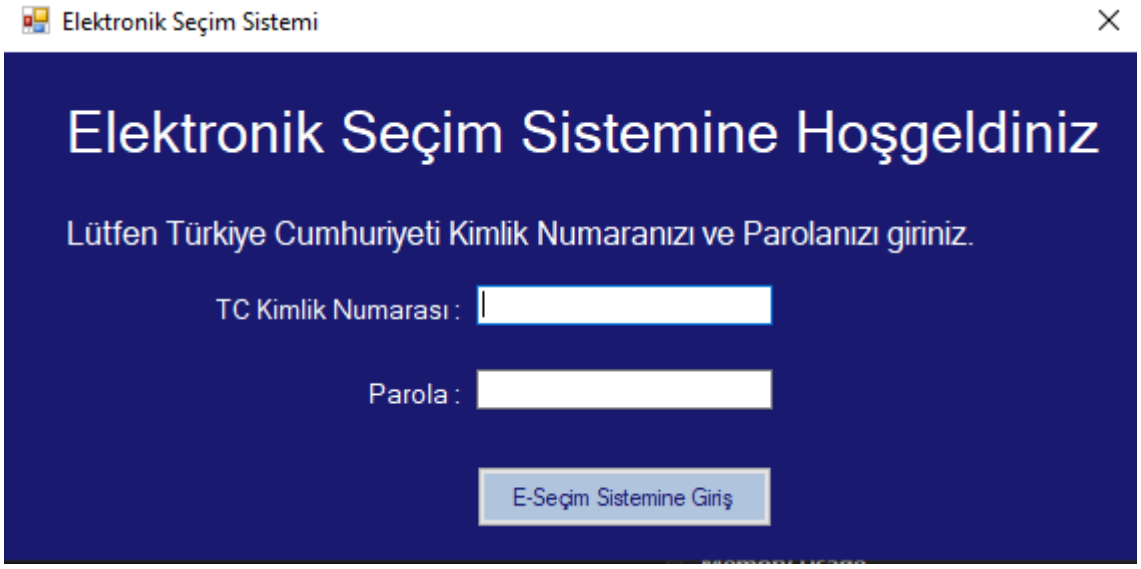
# BÖLÜM 5

# GÜVENLİ E-SEÇİM SİSTEMİ UYGULAMASI

## 5.1. Güvenli E-Oylama için Genel Tasarım Kısmı

### 5.1.1 E-Seçim Sistemine Giriş

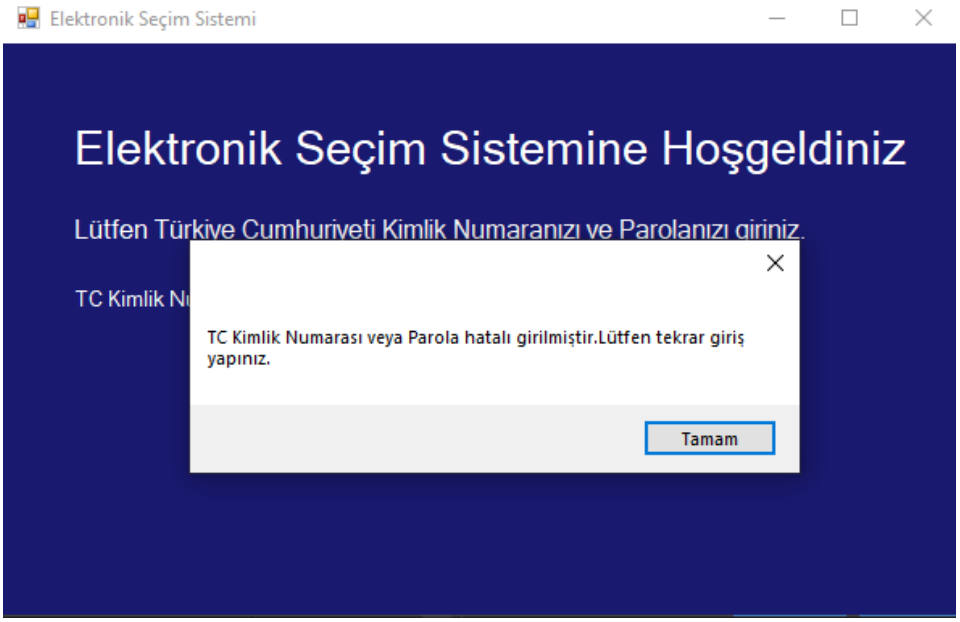
Sır paylaşım şeması tabanlı güvenli e-seçim sistemi uygulaması Visual Studio 2019 üzerinde C# kodu ile geliştirilmiştir. Veri tabanı olarak da MS SQL Server kullanılmıştır. Güvenli e-seçim sistemi uygulamasında Şekil 5.1' de görülmekte olan login ekranından seçmenler TC Kimlik Numarası ve parolalarını girerek giriş butonuna tıkladıklarında sisteme giriş yapabileceklerdir. Kullanıcıların sistem yöneticisi tarafından sisteme kayıtları yapılırken parolaları 8 karakter olarak rastgele atanmaktadır. Bu parola seçim sürecinden önce e-posta veya sms yolu ile seçmene gönderilebilir. Seçmen TC kimlik numarasıyla sisteme giriş yapmak istediğinde ilk olarak girdiği 11 haneli TC kimlik numarası ve parola SHA256 hash fonksiyonuyla mesaj özetine dönüştürülür. Daha sonra dönüştürülmüş mesaj özeti Şekil 5.2'de paylaşıldığı şekilde veri tabanına şifrelenmiş olarak kaydedilir. Seçmen tekrar sisteme giriş yapmak istediğinde girmiş olduğu TC kimlik numarası ve parolasının hash karşılığı veri tabanında bulunuyor mu diye kontrol edilir. Yapılan kimlik doğrulama ile seçmen sisteme giriş yapar. Seçmenin TC Kimlik Numarası ve Parolası veri tabanında bulunmuyor ise Şekil 5.3'te paylaşılan uyarı mesajı gösterilir. Sisteme herhangi bir saldırı durumunda veri tabanında bulunan seçmen bilgileri SHA256 hash fonksiyonu kullanılarak şifrelenip saklandığından dolayı kimliklerine ve oy verilerine erişim engellenmiş olacaktır.




Şekil 5.1. E-seçim sistemi login ekranı.

| | TC | Password |
|---|---|---|
| 1 | U0pKjq/NhlmvMjVtWnol+lxwz+BEhTmnxClkwbiXo1k= | Ho1ZMGxwZr4N4v0Ks5D2F73nURNZxAXa82iGhjLL/KA= |
| 2 | Il9puu+2AobGAmK0Dc9AcXoiJ+712wDJtxfV3iRFNRE= | Z5wcURnjq+NUTrQR0BJA0MQC/4yXkMNJQaRMXHG87s= |
| 3 | qW+wmcn+KyhmxRXOBjU5GGxxA90Uud8akXQaev1/IP0= | AXXL7X0olJSg//rcdYC4xPZUJzmbQjbZBSDIgV+hjg= |
| 4 | ckvcvGLxRNstx/OhExLxS3/4NA7WeRZRmsjVJXvr/ug= | nYucu4Ycp+j30+aY3r/aWP7TDreJ6r9naO/GsrK0A3g= |
| 5 | 3ySDKnP2cbyvjhf8hsKhr500cj0ThavIB3EJESXqD6c= | bYkt/MfcdmQL3G5tDwJbrXMQKFP+WQYXsH6nFlTkAI8= |
| 6 | ckvcvGLxRNstx/OhExLxS3/4NA7WeRZRmsjVJXvr/ug= | 4DJhhAzRtcLscWh2ntUUbhPeYkyM0MA9QRzWVlg7tic= |
| 7 | ckvcvGLxRNstx/OhExLxS3/4NA7WeRZRmsjVJXvr/ug= | LfL+cHEcR1+Ac3DaafaAvBmOV0G3R1aQBeNU/BOELhg= |
| 8 | Ol9lWy1B40lqd0p2WxXbG1YwjlbP/L9WH8+SPvob4eY= | +jkzB7HO55lp73BeEn/RyDy9ak65zUDTD+dUwSHU9SA= |
| 9 | MrcLGdWwOV1D3LTCHPxH1CWrsGQiwy0RwusX42C7uel= | erLXCXMeLQJYcCt9RfMY88qbZdhMA1YrG7yO/xEYGdU= |
| 10 | +E4J24tCpn1MZOkzScp3H8lrTtkHR0rCtzY+ZxRavok= | cmLHLwqbyAdXkSOxh3eUgNEDYRt0aW5Rr2tuMYvTAGI= |
| 11 | Y+h6YLwSNfSUlbAhSvRrOJ+qkJGJCuULUpT2WkaJZ3A= | IBMpapmGl8NuTm+SZO3kGk9QdHNQsiywVfansj4XlyI= |

Şekil 5.2.Veri tabanında TC kimlik ve password'un SHA256 ile mesaj özeti.




Şekil 5.3. Hatalı TC kimlik ve parola girildiğinde çıkan uyarı mesajı.

Şekil 5.4'te paylaşılmış olan ekran görüntüsündeki SMS Gönderme ekranında sistemin güvenilirliğini arttırmak amacıyla sms doğrulama kullanılmıştır. Seçmen cep telefonu numarasını ilgili alana girerek 'telefona sms gönder' butonuna tıklar. Telefonuna gelen sms kodunu ilgili alana girerek giriş yap butonuna tıklar. Gelen sms kodu doğru ise seçmenin oy kullanacağı oy kullanma ekranı açılır. Sms kodu hatalı girildiğinde ise 'SMS kodu hatalı girilmiştir. Lütfen tekrar giriş yapınız.' uyarı mesajı gösterilir.




Şekil 5.4. SMS giriş ekranı.

### 5.1.2. E-Seçim Oy Kullanma Ekranı

Oy kullanma ekranında Şekil 5.5'te görüldüğü gibi seçmen oy vermek istediği partiyi radio buton kullanarak seçer. Daha sonra oy kullan butonu ile seçmiş olduğu adaya oyunu kullanır.




Şekil 5.5. Oy kullanma ekranı.

Seçmen Şekil 5.5'te paylaşılan ekranda oyunu kullandıktan sonra Şekil 5.6'da bulunan oy onaylama ekranında bir önceki ekranda oy kullandığı adayı son kez görür ve oy verme işlemini tamamlamak isteyip istemediği sorulur. Seçmen eğer hayır butonuna tıklar ise oy kullanma ekranına tekrar dönüş yapılır. Evet butonuna tıklar ise seçmenin vermiş olduğu oy veri tabanına kaydedilir ve başarılı bir şekilde oy kullanıldığına dair uyarı mesajı kişiye gösterilir.




Şekil 5.6. Oy onaylama ekranı.

Bu tezde önerilen ve bir yazılımı gerçekleştirilen güvenli e-seçim sistemi uygulamasında e-seçim cihazında 2 tip kullanıcı bulunmaktadır. Bu kullanıcılar ve rollerini açıklamak istersek;

**1) Seçmen:** Kendisine verilen parola ve TC kimlik numarası ile oy verme işlemini yapan kişi.

**2) Yetkili Kişiler:** Oylama yapılan E-seçim cihazından ya da bilgisayardan seçim süresi bittikten sonra kendilerine verilen parola ile seçim sonucunu görüntüleme ekranından kısmı oy sonucunu alan yetkili kişilerdir. Daha sonra "k" eşik değerdeki yetkili kişiler kısmi oy bilgilerini sisteme girerler. Diğer yetkili kişilerce eşik değerde girilen kısmi oy bilgisi ile elde edilen sonuçları karşılaştırırlar. Eğer sonuçlar aynı ise bu cihazdaki oylama sonucu doğrudur sonucuna varılır. Farklı partilere mensup yetkili kişiler böylece hiçbir şaibe olmadığına kanaat getirirler. Daha sonra bu toplam sonucu kendilerine verilen kısmi anahtar paylarını birleştirerek AES şifreleme algoritmasıyla şifreleyip güvenli internet kanalından merkeze iletirler. Merkezdekiler de yine kendilerine ait kısmi anahtar paylarını birleştirerek gelen şifreli oy sonucunu çözerler.

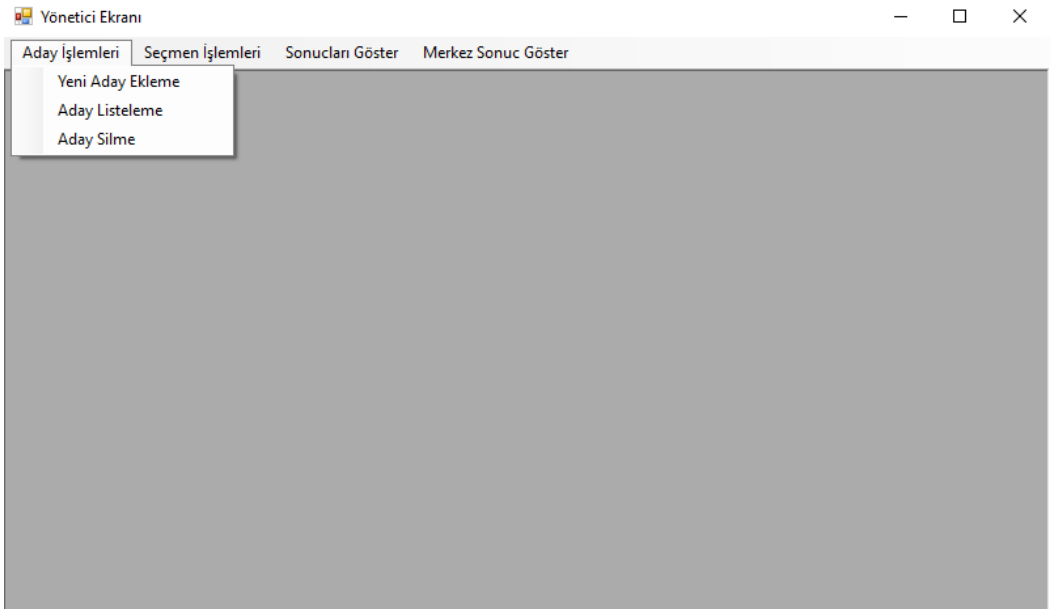
Sonra sistemde genel toplam oy sonucu ikili sisteme dönüştürülerek hangi adayın kaç oy aldığı açıklanır.

### 5.1.3. E-Seçim Sistemi Yöneticisi

Ayrıca yapılan yazılımın sistem yöneticisi kısmını da açıklayalım.

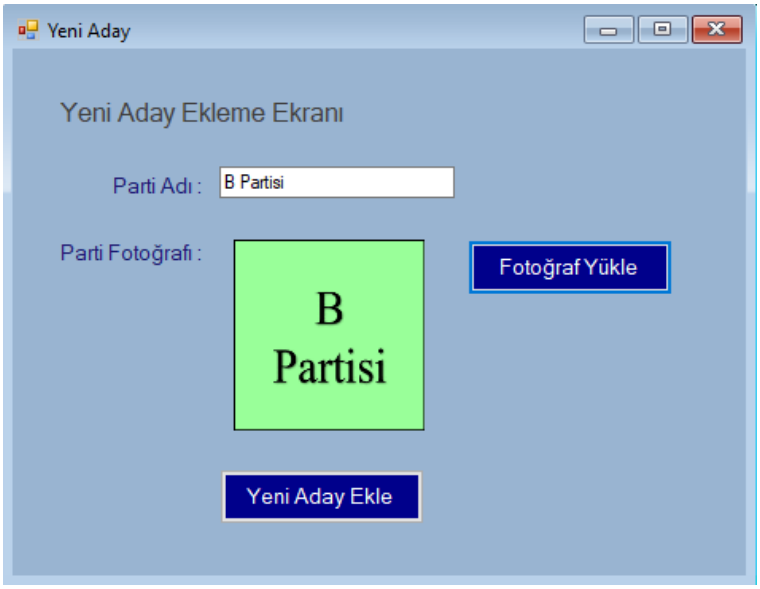
**Sistem Yöneticisi:** Seçimden önce seçmen ve partileri tanımlama, listeleme ve silme işlemlerini yapan güvenilir ve denetlenen kişilerdir.

Adayların ve seçmenlerin bilgilerinin sisteme girilmesi amacıyla bir sistem yönetici ekranı oluşturulmuştur. Şekil 5.1'de paylaşılmış olan login ekranında eğer kullanıcı sisteme sistem yöneticisi olarak tanımlanmış ise TC Kimlik numarası, parola bilgisini girdikten sonra sistem yöneticisi ekranı açılır. Şekil 5.7'de paylaşılmış olan ekranda aday işlemleri, seçmen işlemleri ve oylama sonucu görüntüleme işlemleri bulunmaktadır.



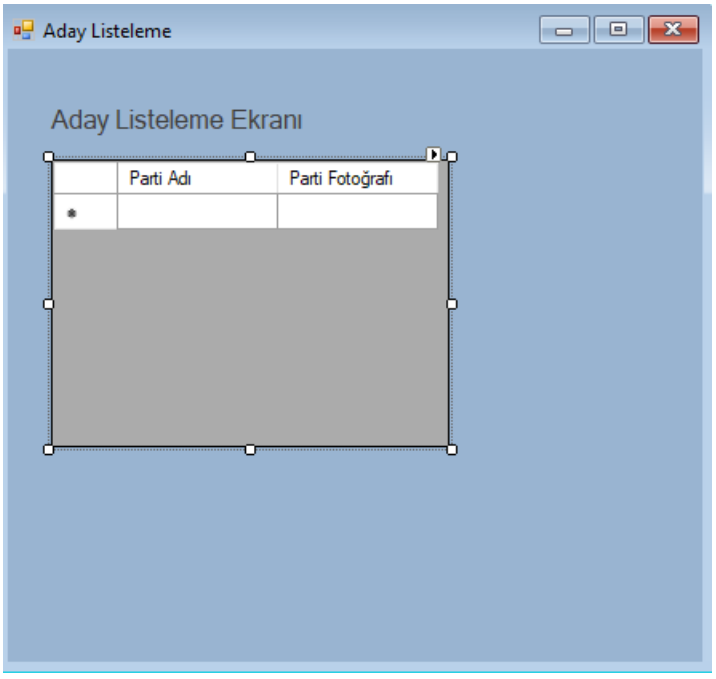

Şekil 5.7.Sistem yönetici ekranı.

Sistem yönetici ekranında bulunan aday işlemleri menüsünden yeni aday ekleme seçilir. Şekil 5.8'de bulunan Yeni aday ekleme ekranında seçimlere katılacak partinin adı ve fotoğrafı girilerek yeni aday ekleme işlemi yapılır.



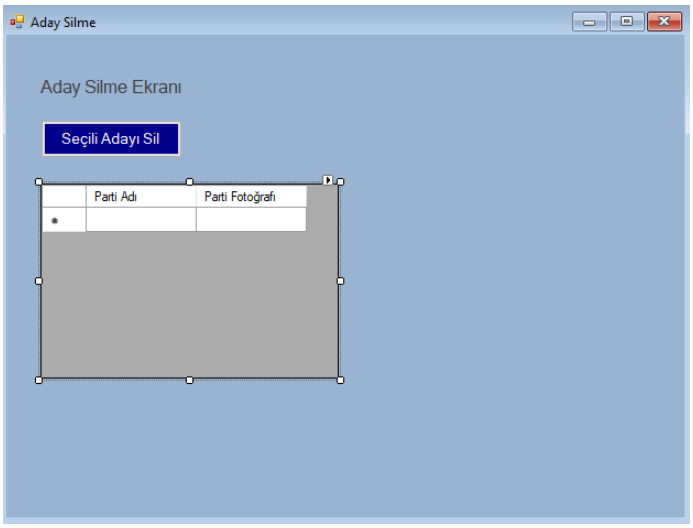

Şekil 5.8.Yeni aday ekleme ekranı.

Sistem yönetici ekranında bulunan aday işlemleri menüsünden aday listeleme seçilir. Şekil 5.9'da görüntülenen aday listeleme ekranında veri tabanına kaydedilmiş olan adaylar listelenir.




Şekil 5.9.Aday listeleme ekranı.

Yönetici ekranında bulunan aday işlemleri menüsünden aday silme seçilir. Şekil 5.10'da gösterilen aday silme ekranında veri tabanına bilgileri yanlış kaydedilmiş veya seçime katılmayacak olan adaylar silinebilir.



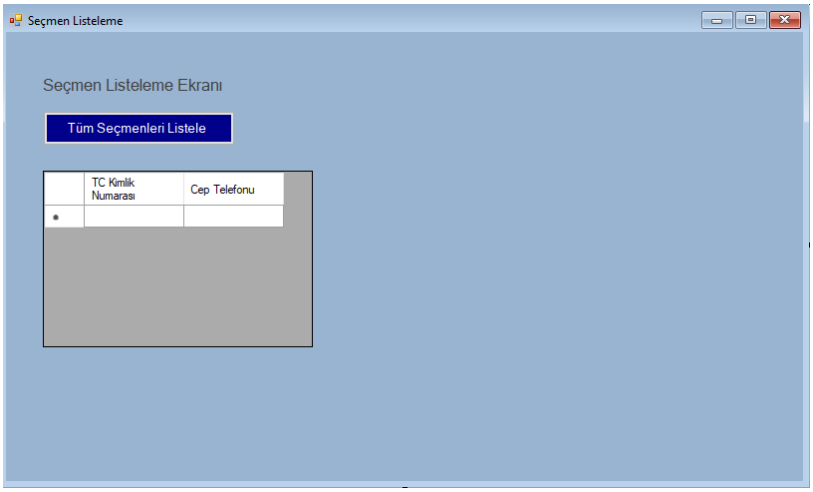

Şekil 5.10. Aday silme ekranı.

Sistem yönetici ekranında bulunan seçmen işlemleri menüsünden yeni seçmen ekleme seçilir. Şekil 5.11'de görülen yeni seçmen ekleme ekranından seçmenlerin tc kimlik numarası, adı, soyadı, cep telefonu, e-mail adresi ve doğum tarihi bilgileri girilerek sisteme kaydedilmesi sağlanır. Bu şekilde seçmen sisteme login olurken veri tabanına kaydedilmiş olan seçmenler oy kullanabilecektir.



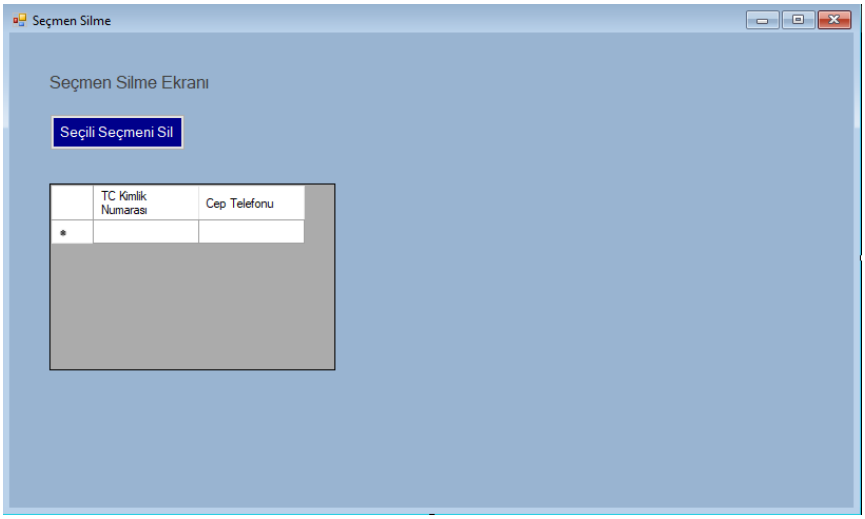

Şekil 5.11.Yeni seçmen ekleme ekranı.

Sistem yönetici ekranında bulunan seçmen işlemleri menüsünden seçmen listeleme seçilir. Şekil 5.11'de görülen yeni seçmen ekleme ekranında kaydedilmiş olan seçmenler seçmen listeleme ekranından Şekil 5. 12'deki gibi listelenir.




Şekil 5.12.Seçmen listeleme ekranı.

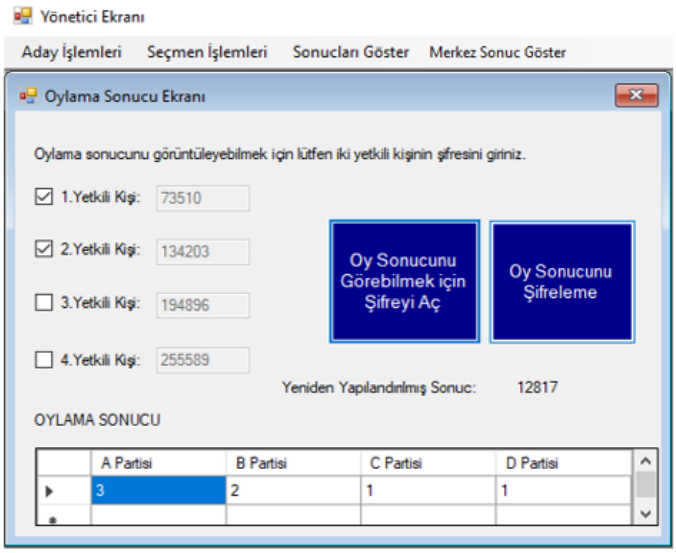
Seçmen ekleme ekranından bilgileri yanlış eklenmiş veya oy kullanamayacak olan kişiler Şekil 5.13'te paylaşılan seçmen silme ekranından silinebilir.




Şekil 5.13.Seçmen silme ekranı.

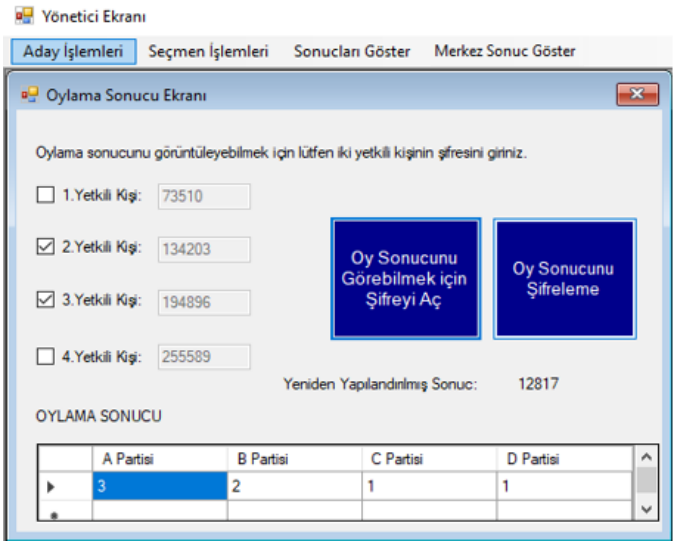
## 5.2. Sır Paylaşım Şeması Tabanlı Homomorfik E-Oylama Uygulaması

Burada (k,n)=(2,4) Shamir'in eşik şemasına göre bir oylama yapılmıştır. Oylama için 1. dereceden polinom ve sabit terim kullanılan oy olmak üzere, 4. Bölüm 4.2 numaralı 8 örnekte detaylı anlatıldığı gibi yapılmıştır. Oylama süreci bittikten sonra sistem yöneticisi ekranında bulunan oylama sonucu işlemleri menüsünden oylama sonucunu görüntüle aktif hale gelir. Şekil 5.14'te paylaşılmış olan ekran görüntüsünde 4 yetkili kişi arasından en az iki yetkili aldığı kısmi oy sonucunu girerek 'oylama sonucunu görebilmek için şifreyi aç' butonuna tıklanır. Burada 1. Yetkili Kişi ve 2. Yetkili Kişi kısmi oy bilgilerini girmektedir. Tüm hesaplamalarda her bir ikili yetkili kişi aynı işlemi yapar ve tüm sonuçlar aynı ise toplam oy elde edilen değerdir şeklinde sonuç alınır. Buradaki hesaplamalarda Lagrange interpolasyon kullanılmış ve o cihazdaki seçim sonuçları oylama sonucu alanında gösterilmiştir.




Şekil 5.14. 1. ve 2. Yetkili kişilerle elde edilen oylama sonucu ekranı.

Aşağıdaki Şekil 5.15'te 2.Yetkili ve 3. Yetkili elindeki kısmi oy bilgisini girerek toplam oy sonucunu elde ederler. Diğer yetkililerde benzer şekilde en az ikisi birleşerek toplam oy sonucuna ulaşırlar.




Şekil 5.15. 2. ve 3. Yetkililer ile toplam oy sonucuna ulaşma.

Aşağıdaki Şekil 5.16'da seçmenlerin farklı adaylar için kullanmış olduğu oyların ikili sistemle ve ondalık olarak değerleri verilmiştir.

| | A Partisi | B Partisi | C Partisi | D Partisi | Oy Kullanma | Decimal Dönüşüm |
|---|---|---|---|---|---|---|
| **Seçmen 1** | EVET | | | | 0001/0000/0000/0000 | 4096 |
| **Seçmen 2** | EVET | | | | 0001/0000/0000/0000 | 4096 |
| **Seçmen 3** | EVET | | | | 0001/0000/0000/0000 | 4096 |
| **Seçmen 4** | | EVET | | | 0000/0001/0000/0000 | 256 |
| **Seçmen 5** | | EVET | | | 0000/0001/0000/0000 | 256 |
| **Seçmen 6** | | | EVET | | 0000/0000/0001/0000 | 16 |
| **Seçmen 7** | | | | EVET | 0000/0000/0000/0001 | 1 |

Şekil 5.16. 7 Seçmen ve 4 parti ile oylama kısmı.

Öncelikle her seçmenin kullanmış olduğu parti bilgisini tutabilmek amacıyla örnekte görüldüğü üzere 4 parti için dörder bitlik toplamda 16 bit bir dizi kullandık. İlk 4 bit A, ikinci 4 bit B, üçüncü 4 bit C ve son 4 bit D partisine verilen oyu temsil etmektedir. 1.adaya oy verilirse oluşturduğumuz bu dizinin 4.elemanı 1 oluyor ve kalanı 0 olarak kalıyor. Böylece seçmenin o adaya oy vermiş olduğunu anlamış oluyoruz. Elde ettiğimiz

ikili ifade olan diziyi formülde kullanabilmek için ondalık dönüşüm uyguluyoruz. Burada mod sayısı, aday sayısı ve seçmen sayısına göre değişmekte olup bunlardan büyük bir asal sayı olarak seçilmiştir. Her seçmen için g(x) = (Random katsayı * x + Decimal) Mod 65537 formülünü uyguluyoruz.

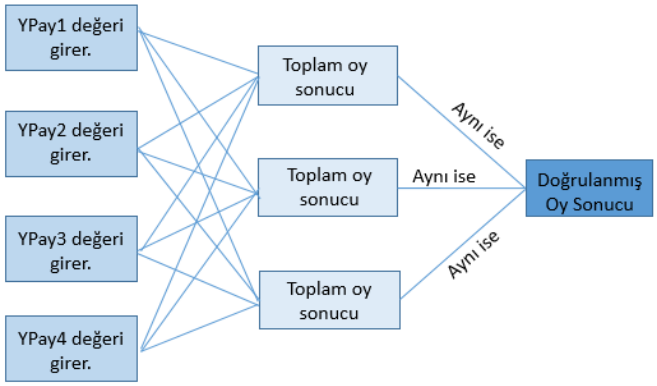
Formülde kullanmış olduğumuz rastgele katsayı random fonksiyonu ile uygulamada üretilmektedir. Ondalık (Decimal) değerler ise her bir seçmen için ayrı olarak oluşturduğumuz ikili ifadenin tablodaki ondalık dönüşümüdür.

Buradaki amacımız Shamir'in gizli paylaşım şemasında olduğu gibi oyu 4 yetkili arasında paylaştırmaktır. Ancak eşik değerdeki yetkili kişiler bir araya gelerek ellerindeki kısmi oylarla toplam oy bilgisine ulaşabilirler. Sonuç olarak elde edilen değerler detaylı olarak Bölüm 4'de Örnek 4.2.'de anlatıldığı gibidir. Toplam oy sonucu aşağıdaki Şekil 5.17'deki gibi elde edilmiştir.

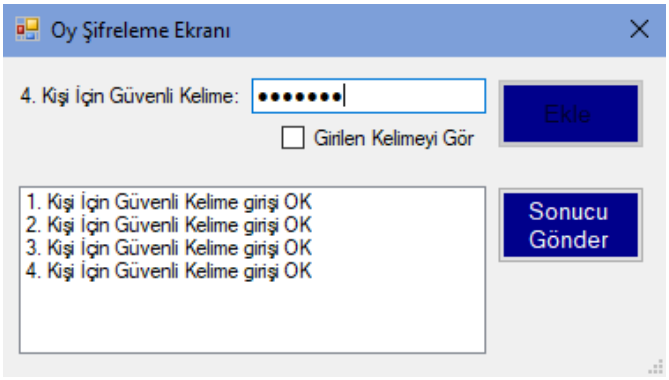
| Partiler | Aldıkları Toplam Oy Sayısı |
|---|---|
| A Partisi | 3 |
| B Partisi | 2 |
| C Partisi | 1 |
| D Partisi | 1 |

Şekil 5.17. Partilerin aldıkları oy sayısı.

Tüm yetkililer denedikten sonra tamamının sonuç ekranı Şekil 5.18'de açıklandığı gibi aynı ise (burada 4 yetkili için görselleştirilmiş) bu toplam oylar Şekil 5.19'da gösterilen oy şifreleme ekranından yetkililerin girmiş oldukları kısmi gizli anahtarlar kullanılarak AES ile şifrelenir ve e-imzalı olarak güvenli internet kanalından seçim merkezine iletilir.

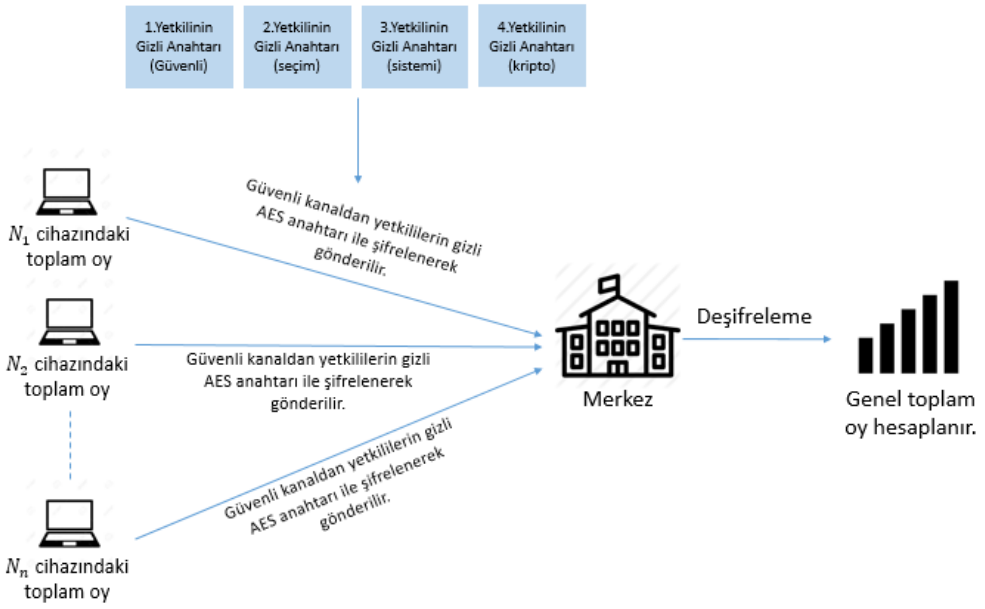



Şekil 5.18.Oylama sonuçlarının yetkililer tarafından doğrulanması.

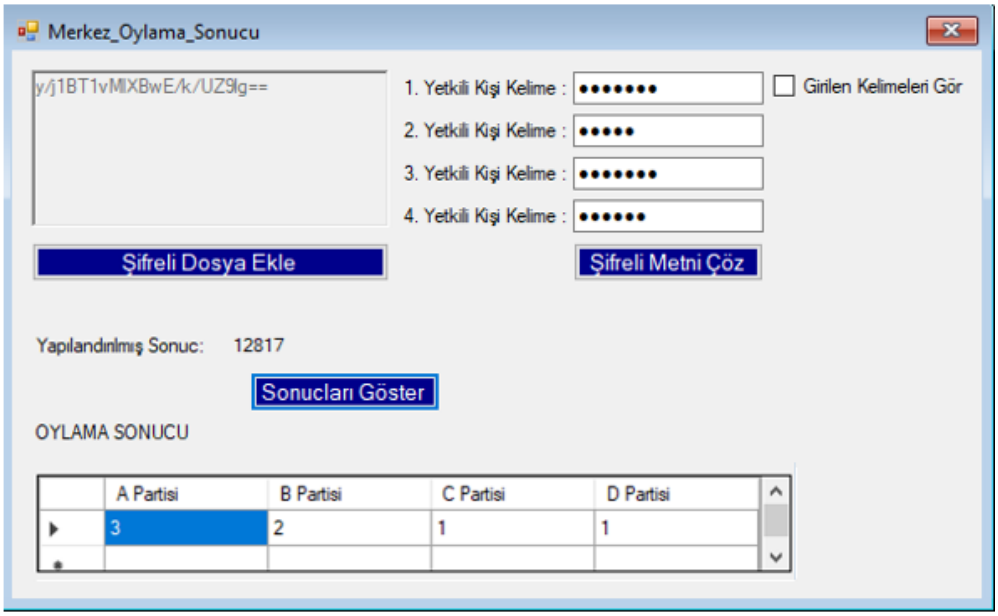



Şekil 5.19.Oylama sonuçlarının şifrelenmesi için yetkililer tarafından anahtar değerlerinin girilmesi.

Sonra Şekil 5.20'de görüldüğü gibi 4 yetkili için konuşacak olursak, oylama cihazındaki doğruluğu yetkili kişilerce onaylanan toplam oy sonucu yetkili kişilerin elindeki kısmi gizli anahtarlar birleştirilerek (belirli düzende) AES ile şifrelenip güvenli kanaldan merkeze gönderilir. Merkezdeki yetkililer de aynı şekilde Şekil 5.21'de görüldüğü gibi ellerindeki gizli anahtarları birleştirerek gelen toplam oyları çözer ve genel toplam oylar hesaplanır.

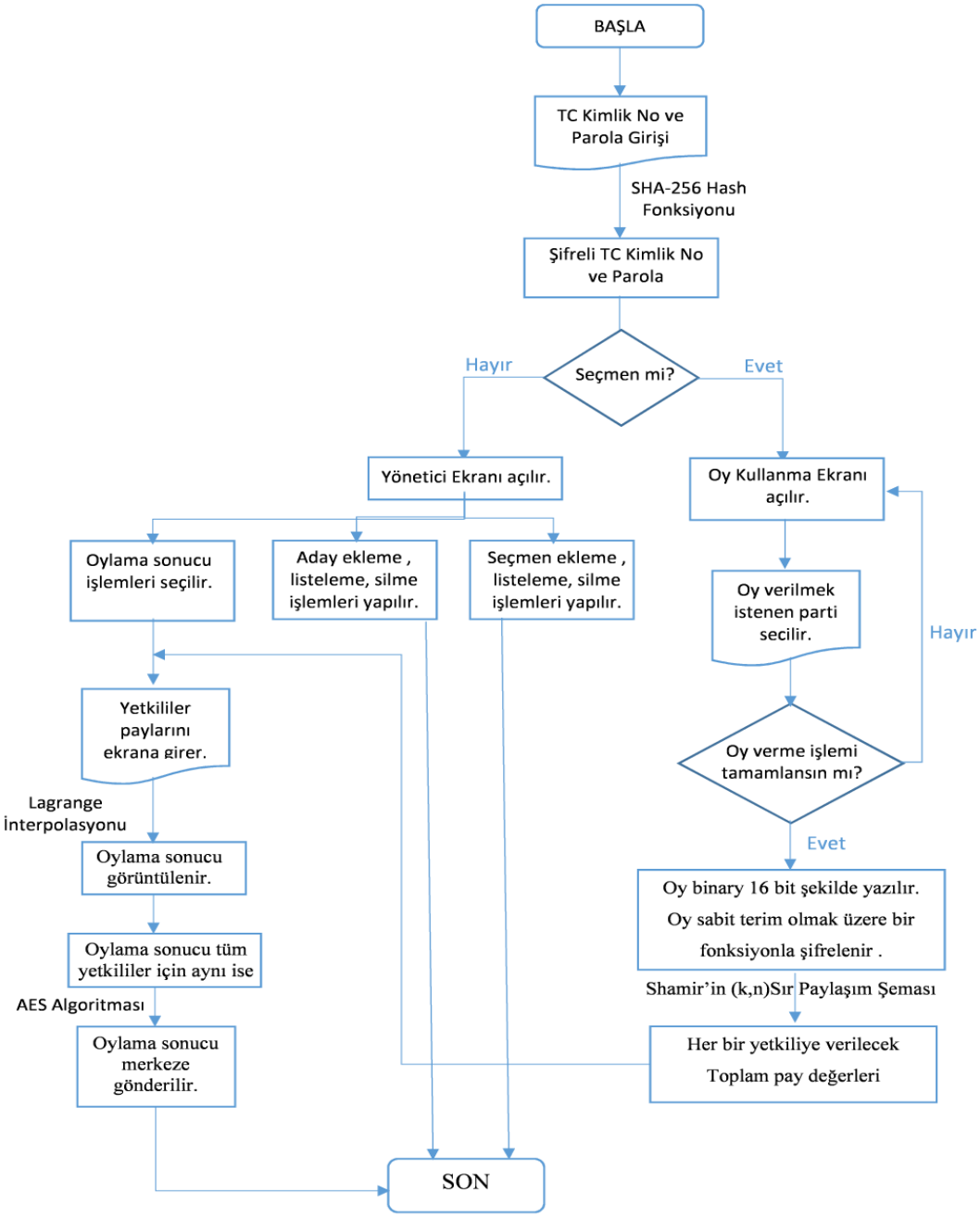



Şekil 5.20. Her bir N oylama cihazındaki toplam oy sonucunun AES ile şifrelenerek merkeze gönderilmesi ve toplam oyun hesaplanması süreci.




Şekil 5.21. Merkezdeki yetkililerin gizli anahtarlarını birleştirerek şifreli toplam oyu AES ile çözerek sonucu görüntülemesi.

Güvenli bir e-seçim özellikle güvenli oylama için önerdiğimiz sistemin akış şeması aşağıdaki Şekil 5.22'de detaylı bir şekilde verilmiştir.




Şekil 5. 22. Önerilen e-seçim siteminin akış şeması.

# BÖLÜM 6

# SONUÇLAR VE TARTIŞMA

Geçersiz oy kaybını engellemek, oy sayımındaki hız ve sistemin güvenilirliği gibi konuları amaç edinerek geliştirilen elektronik oylama sistemlerinin önemli getirilere sahip olacağı düşüncesi ile çalışmalar gün geçtikçe artmaktadır. Bu nedenle teknolojinin gelişmesi ve bilgisayar kullanımının artması ile çeşitli ülkelerde elektronik seçimlerin bir bilgisayardan ya da tasarlanan elektronik cihazdan daha hızlı, daha güvenilir ve daha az maliyetle yapılması fikri kabul görmektedir. Ancak her teknolojik gelişme ile gelen birçok soru işareti ve olumsuzluk bu sistemler için de geçerli olup, tartışmalar ve çalışmalar özellikle sistemin güvenilirliğini artırmak üzerine yoğunlaşmaktadır. İçinde yaşadığımız mevcut pandemi koşulları da göz önünde bulundurulduğunda ve bilgisayar okuryazarlığının artmakta olduğu dijitalleşen dünyada e-seçim sisteminin de güvenilirliğini kanıtlanmış elektronik sistemler ile yapılması araştırılmaya değer bir problem olarak karşımıza çıkmaktadır.

E-seçim sisteminin en önemli ve hassas noktası güvenlik ihtiyacıdır. Bu güvenlik ihtiyaçları içerisinde seçmenin gizliliği, kanunlara göre oyunu kullanabilmesi, sistemin güvenilirliği, oyların değiştirilememesi, oyların kime kullanıldığının anlaşılamaması gerekliliği, oyların doğru sayılması ve sistemin saldırılara karşı dayanıklı olması gibi konular sayılabilir.

Bu tezde e-seçim uygulaması için internet bağlantısı olmayan bir bilgisayar veya elektronik cihaz üzerinde farklı kriptografik yapılar kullanılarak oylama yapılmasına imkan veren bir yazılım geliştirildi. Bu yazılım sayesinde yapılacak bir e-seçim dışardan gelecek herhangi bir siber saldırıya karşı korunmaktadır. İlk olarak oy kullanılacak sisteme girişte kimlik doğrulama için SHA256 mesaj özeti algoritması kullanılmıştır. Oylama esnasında her seçmenin oyu bir fonksiyona sokularak oy kodlanmıştır. Oy sayma işlemi

kullanılan cihazın ya da bilgisayarın kendi içerisinde gerçekleşmektedir. Böylece oy kullanma işlemi bittikten sonra yetkili kişiler o cihazdaki oyların sonucunu öğrenmek için kendilerine verilen şifreleri girerek kısmi oy sonuçlarını alabilmektedir.

Daha sonra eşik değerdeki yetkili kişilerin elde ettiği oy sonuçları ile diğer eşik değerdeki yetkililerin elde ettiği oy sonuçları aynı ise toplam oyların doğruluğu onaylanmış olur. Sürecin devamında ise yine yetkililer kendilerine ait kısmi gizli anahtarlarını birleştirerek toplam oy sonuçlarını AES ile şifreleyip seçim sisteminin kullandığı güvenilir internet hattı üzerinden oy toplama merkezine iletir.

Bu tezde özellikle oylama ve sonuçların doğruluğu için kullanılan kriptografik yapıların e-seçim sisteminde güvenliğe etkisi üzerine odaklanılmıştır. İlk olarak seçmenin sisteme giriş yapabilmesine imkan veren kimlik doğrulama için mesaj özeti fonksiyonu olarak SHA256 kullanılmıştır. Oy kullanma esnasında Shamir'in polinom tabanlı sır paylaşım şeması kullanılarak oylama sonucunun doğruluğu sağlanmıştır. Sonuç olarak geliştirilen bu yazılım ile oy kaybının ve kullanılan oyların değiştirilmesinin önüne geçildiğini söyleyebiliriz. Böylece güvenli bir e-seçim sistemi için geliştirilmiş yazılım içerisinde Sır Paylaşım Şemaları'nın kullanılması hem seçmenin mahremiyetini korumakta hem de oylama sonucunun tek bir kişi veya kurumun tekelinde olmasını engellemektedir.

Gelecekte güvenliği kanıtlanmış bitcoin tabanlı bir elektronik seçim sistemi ile farklı kriptografik yapılar bir arada kullanılarak daha güvenli bir elektronik seçim sistemi geliştirilmesi hedeflenmektedir.

# KAYNAKLAR


Akın, M., (2006). Elektronik Oy Verme Sistemlerinde Güvenlik: Deneyimler Ve Türkiye İçin Öneriler. İstanbul Üniversitesi *İktisat Fakültesi Ekonometri Ve İstatistik Dergisi*, 3,

Alemdaroğlu, H. (2014). *Mercuri Modeline Dayalı Örnek Elektronik Seçim Uygulaması*. (Yüksek Lisans Tezi) Beykent Üniversitesi / Fen Bilimleri Enstitüsü, İstanbul.

Al-Saidi, N.M.G. & Abdulhadi, M.M. (2017). E–Voting System based on Secret Sharing Scheme. *Engineering and Technology Journal*, *35*, (Part B, 1), 13-18.

Arda, D., Demirbilek, S., & Kavak, S. (2017). The Effect Of Steganography And Secret Image Sharing Scheme To The Security Of Cryptographic Key. *Journal of International Scientific Publications*, *11*, 474-483.

Arda, D., & Buluş, E. (2009). Çin Kalan Teoremini Kullanan Bir Gizlilik Paylaşım Şeması. *IV.İletişim Teknolojileri Ulusal Sempozyumu*, (s. 23-26). Adana.

Arda, D., Buluş, E., Akgün, F., & Yerlikaya, T. (2008). Secret Sharing Scheme in Cryptographic Key Management Problem. *International Scientific Conference UNITECH*. Gabrovo.

Blakley, G. R. (1979). Safeguarding Cryptographic Keys. *National Computer Conference*, *48*, 313-317.

Çetinkaya, D., & Çetinkaya, O.(2006). E-Seçim Uygulamaları için Gereksinimler ve Tasarım İlkeleri XI. *Türkiye'de İnternet Konferansı*, Ankara, Türkiye.

Çinpolat, A. (2005). *Türkiye'deki Genel Seçimler İçin Bir Elektronik Seçim Modeli Uygulaması*. (Yüksek Lisans Tezi ) Gazi Üniversitesi / Fen Bilimleri Enstitüsü, Ankara..

Daemen, J., & Rijmen, V. (2002). The Desing of Rijndal: AES- The advanced encrption standard. In Information security and crypography. *Springer*.

Daemen, J., & Rijmen, V. (1999). AES Submission Document on Rijndael, Version 2, [PDF belgesi]. 10 Ocak 2021 tarihinde http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael.pdf adresinden erişildi.

Elgamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory, 31*(4), 469 - 472.

Erşen, B. (2017). *Yüksek Performanslı Bitcoin Madenciliği İçin Sha256 Özet Algoritmasının En İyilenmesi*.(Yüksek Lisans Tezi) TOBB Ekonomi ve Teknoloji Üniversitesi / Fen Bilimleri Enstitüsü, İstanbul.

FIPS PUB-197. (2001). Advenced Encryption Standard. [PDF belgesi]. 10 Ocak 2021 tarihinde https://it.ojp.gov/NISS/iepd/443 adresinden erişildi.

Forouzan, B. A. (2008). *Cryptography and Network Security*. New York, USA: McGraw-Hill Inc.

Iftene, S. (2007). General secret sharing based on the chinese remainder theorem with applications in e-voting. *Electronic Notes in Theoretical Computer Science, 186*,67‑84.

Kim, K., & Lee, B. (2005). VOTOPIA – Internet Voting Experience during 2002 FIFA WorldCup. *Int. Conf. on E-voting and Electronic Democracy: Present and the Future*, Korea, Japan.

Kiraz, M.S, Birinci, F. & Boyacı, U.K. (2012). Elektronik Seçim: Norveç'in İnternet Üzerinden Oylama Sistemi ve Kriptografik Altyapısı, Ankara, Türkiye.

Koblitz, N. (1987). Elliptic Curve Cryptosystems. *Mathematics Of Computation*, 203-209.

Mignotte, M. (1983). *How to Share a Secret* (s. 371-375). Volume 149 of LNCS Springer-Verlag.

Nair, D. G., Binu, V. P. &. Kumar, G. S. (2014). An Improved E-Voting Scheme using Secret Sharing based Secure Multi-Party Computation. Cochin University of Science and Technology.

National Institute of Standarts and Technology NIST,(2016). SHA256 Standart.[PDF belgesi]. 10 Ocak 2021 tarihinde https://csrc.nist.gov/csrc/media/publications/fips/180/2/archive/2002-08-01/documents/fips180-2.pdf adresinden erişildi.

Pieters, W. (2006). Internet voting: a conceptual challenge to democracy. *International Working Conference*, Ireland, Springer, pp. 89-103.

Rivest, R. L., Shamir, A., & Adleman, L. M. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM, 21*(2),120-126.

Şahin, M. (2005). *Elektronik Seçim Modellerinin Analizi ve Bir Model Önerisi*. (Yüksek Lisans Tezi) Beykent Üniversitesi / Fen Bilimleri Enstitüsü, İstanbul.

Salman, H. (2016). *Elektronik Seçim Sistemlerinde Güvenlik Amaçlı Algoritma Önerisi*. (Yüksek Lisans Tezi) Beykent Üniversitesi / Fen Bilimleri Enstitüsü, İstanbul.

Saltman, R. G.,(1978). Effective use of computing technology in vote-tallying(Vol.13). *US Department of Commerce,* National Bureau of Standards.

Shamir, A. (1979). How to Share a Secret. *Communications of the ACM, 22,* 612-613.

Schoenmakers, B. (1999). A simple publicly verifiable secret sharing scheme and its application to electronic voting. In *Advances in Cryptology CRYPTO99,* pages 148–164. Springer.

Stinson, D.R. (2002). Cryptography : Theory and Practice. Second Adition, CRC Press.

Telciler, C. (2017). Elektronik Seçim Sistemleri, Sorunlar, Çözüm Önerileri. Nişantaşı Üniversitesi Sosyal Bilimler Dergisi, *5*(2), 106-122.

Tüfekçi, M. (2018). AESX+, AESX, AES-128 ve AES-256'nın Performans ve Güvenlik Açısından Karşılaştırılması. Ege Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi.

USEAC (2005a), "Voluntary Voting System Guidelines, .I.

USEAC (2005b), "Voluntary Voting System Guidelines, II.

Wheaton, S.(2015). Voting Test Falls Victim to Hackers .The NewYork Times.

Yuan, L., Li , M., Guo, C., Hu,W. & Wang, Z. (2017). A Verifiable E-voting Scheme with Secret Sharing. *International Journal of Network Security*, *19*(2), 260-271.

# EKLER

## EK A. Kullanılan Teknolojiler

1. IDE: Microsoft Visual Studio 2019
2. Yazılım Dili: C#
3. Veri Tabanı: Microsoft SQL Server 2017

## EK B. Tez İçin Geliştirilen Uygulamanın Kodlarının Açıklanması

Aşağıda tez akışı sürecinde farklı adımlarda yürütülen kodun ekran çıktıları verilmiştir.

EK B1. Güvenli e-seçim sistemi uygulamasında yer alan login ekranında bulunan tc kimlik ve parola input değerlerinin alınarak veri tabanına SHA256 hash fonksiyonuyla mesaj özetine dönüştürülerek, daha önce mesaj özeti alınmış veri tabanındaki bilgileriyle karşılaştırılıp kimlik doğrulamasından sonra oylama sisteme giriş izni için gerçekleştirilen kod akışı.

```
private void btn_login_Click(object sender, EventArgs e)
{
    //
    SHA256 sha = new SHA256CryptoServiceProvider();
    String tc_sha = Convert.ToBase64String(sha.ComputeHash(Encoding.UTF8.GetBytes(txt_box_tc.Text)));
    String pass_sha = Convert.ToBase64String(sha.ComputeHash(Encoding.UTF8.GetBytes(txt_box_pass.Text)));

    cmd_admin = new SqlCommand();
    cmd_voter = new SqlCommand();
    try
    {
        con.Open();
        cmd_admin.Connection = con;
        cmd_admin.CommandText = "select count(Id) from System_Admin where TC=@tc and Password=@pass and Super_Admin=@super";
        cmd_admin.Parameters.AddWithValue("@tc", tc_sha);
        cmd_admin.Parameters.AddWithValue("@pass", pass_sha);
        cmd_admin.Parameters.AddWithValue("@super", 0);
        system_admin = (int)cmd_admin.ExecuteScalar();


        cmd_voter.Connection = con;
        cmd_voter.CommandText = "select TC,Name,SurName,Telephone,Email,BirthDay,IsVote from Voting_Citizen_List where TC = @tc and Password = @pass";
        cmd_voter.Parameters.AddWithValue("@tc", tc_sha);
        cmd_voter.Parameters.AddWithValue("@pass", pass_sha);
```

EK B2. Seçmenlerin kullanmış olduğu oy bilgisinin binaryden decimale dönüştürüldüğü ve random katsayı üretilerek Shamir'in Polinomsal Sır Paylaşım Şeması formülü ile hesaplanan kısmi oy bilgisini hesaplama

```
Secmen secmen = new Secmen(); //secmen classından yeni bir secmen nesnesi yarattık

secmen.oyVer(name);//radiobuttondaki stringi alıp oyver fonksiyonuna gönderiyor
bool[] secimSonucu = secmen.getOy();//bitini 1 yaptığımız diziyi secimsonucu adlı değişkene attık


if (secimSonucu[3] == true) //eğer dizinin 4.elemanı 1 olursa 2 üzeri 12 yap
{
    secmenDecimal = Math.Pow(2, 12);
}
else if (secimSonucu[7] == true)//eğer dizinin 8.elemanı 1 olursa 2 üzeri 8 yap
{
    secmenDecimal = Math.Pow(2, 8);
}
else if (secimSonucu[11] == true)//eğer dizinin 12.elemanı 1 olursa 2 üzeri 4 yap
{
    secmenDecimal = Math.Pow(2, 4);
}
else if (secimSonucu[15] == true)//eğer dizinin 16.elemanı 1 olursa 2 üzeri 0 yap
{
    secmenDecimal = Math.Pow(2, 0);
}

Random rastgele = new Random();
int randomKatsayi = rastgele.Next(1, 13107); //random değer üret

double secmenCC1 = secmenCC(randomKatsayi, 1, secmenDecimal);//cc1 ürettiğimiz fonksiyon
double secmenCC2 = secmenCC(randomKatsayi, 2, secmenDecimal);//cc2 ürettiğimiz fonksiyon
double secmenCC3 = secmenCC(randomKatsayi, 3, secmenDecimal);//cc3 ürettiğimiz fonksiyon
double secmenCC4 = secmenCC(randomKatsayi, 4, secmenDecimal);//cc4 ürettiğimiz fonksiyon

insertSonuc(secmenCC1, secmenCC2, secmenCC3, secmenCC4);//cc1,cc2,cc3 ve cc4 değerlerini veritabanına atan fonksiyon
```

EK B3. Shamir'in Polinomsal Sır Paylaşım Şeması formülü ile hesaplanan kısmi oy bilgilerinin yetkili kişiler için toplamlarının alınması

```
public void oyToplam() //Yetkililere vereceğimiz kısmi toplamları hesaplamak için veritabanına attığımız Pay bilgilerini toplamamız gerek
{

    SqlCommand cmd;
    cmd = new SqlCommand();
    SqlConnection con1 = new SqlConnection("Data Source=DESKTOP-66VA0FH;Initial Catalog=Elections;Integrated Security=True");
    con1.Open();
    cmd.Connection = con1;

    cmd.CommandText = "Select sum(cc1) as toplam from sonuc"; //veritabanındaki Pay1 sütununu topluyor
    scc1 = Convert.ToDouble(cmd.ExecuteScalar());

    cmd.CommandText = "Select sum(cc2) as toplam from sonuc"; //veritabanındaki Pay2 sütununu topluyor
    scc2 = Convert.ToDouble(cmd.ExecuteScalar());

    cmd.CommandText = "Select sum(cc3) as toplam from sonuc"; //veritabanındaki Pay3 sütununu topluyor
    scc3 = Convert.ToDouble(cmd.ExecuteScalar());

    cmd.CommandText = "Select sum(cc4) as toplam from sonuc"; //veritabanındaki Pay4 sütununu topluyor
    scc4 = Convert.ToDouble(cmd.ExecuteScalar());

    con1.Close();

    textBox1.Text = scc1.ToString();
    textBox2.Text = scc2.ToString();
    textBox3.Text = scc3.ToString();
    textBox4.Text = scc4.ToString();
}
```

EK B4. Lagrange interpolasyon metodu ile mod 65537’ ye göre toplam kısmi değerlerin alınarak hesaplanan yeniden yapılandırılmış toplam oy sonuç değeri kodlarını göstermektedir.

```
public double lagrange() //lagrange interpolasyon yaptığımız fonksiyon
{
    double q01 = (((s1 * (0 - scm2)) / (scm1 - scm2)) + ((s2 * (0 - scm1)) / (scm2 - scm1)));

    return q01 % 65537;


}

double s1, s2, scm1, scm2;


public void check_box_kontrol()
{

    int degisen_toplam = toplamsecim;

    // En az 2 adet parçanın seçilip kontrol edilmesi
    foreach (var item in Controls)
    {
        if (item is CheckBox)
        {
            CheckBox c = (CheckBox)item;
            if (c.Checked)
            {
                string name = c.Name;
                if (degisen_toplam == 2)
                {

                    switch (name)
                    {
```

EK B5. Yeniden yapılandırılmış sonuç değerinin binaryden decimale dönüştürülerek hangi partiye ne kadar oy kullanıldığının hesaplaması kodlarını göstermektedir.

```
if (toplamsecim != 2)
{
    MessageBox.Show("EN AZ İKİ ADET SEÇİM YAPINIZ ! ", "DİKKAT", MessageBoxButtons.OK, MessageBoxIcon.Asterisk);
    return;
}
else
{
    check_box_kontrol();

    double result = lagrange();

    sonucBinary = decimalToBinary(result);
    oylarSonuc(sonucBinary);


    aday1Sonuc = resultAday1.ToString();
    aday2Sonuc = resultAday2.ToString();
    aday3Sonuc = resultAday3.ToString();
    aday4Sonuc = resultAday4.ToString();


    lbl1.Visible = true;
    lbl1.Text = result.ToString();

    DataTable tablo = new DataTable();

    tablo.Columns.Add("A Partisi", typeof(int));
    tablo.Columns.Add("B Partisi", typeof(int));
    tablo.Columns.Add("C Partisi", typeof(int));
    tablo.Columns.Add("D Partisi", typeof(int));
    tablo.Rows.Add(aday1Sonuc, aday2Sonuc, aday3Sonuc, aday4Sonuc);
    dataGridView1.DataSource = tablo;
```

EK B6. Decimale dönüştürülen yeniden yapılandırılmış sonuç değeri için tutulan dizide her 4 bit değerin karşılığı olan oylama sayısının hesaplandığı kodları göstermektedir.

```
public void oylarSonuc(int[] dizi) //hangi adaya oy verilmişse 1 arttıracak
{
    int[] aday1 = new int[4];
    int[] aday2 = new int[4];
    int[] aday3 = new int[4];
    int[] aday4 = new int[4];

    int sayac = 0;
    for (int i = 0; i < 16; i++)
    {
        if (i == 4 || i == 8 || i == 12)
        {
            sayac = 0;
        }
        if (i <= 3)
        {
            aday1[sayac] = dizi[i];
        }
        else if (i >= 4 && i <= 7)
        {
            aday2[sayac] = dizi[i];
        }
        else if (i >= 8 && i <= 11)
        {
            aday3[sayac] = dizi[i];
        }
        else if (i >= 12 && i <= 15)
        {
            aday4[sayac] = dizi[i];
        }
        sayac++;
    }
```

EK B7. Oylama sonuçlarının seçim merkezine gönderilmeden önce AES şifreleme algoritmasıyla şifrelenmesi kısmı.

```
public class Crypto
{

//AES 256 Bit şifreleme algoritması Türkçe karakter içeriği ile şifreleme yapılabilmektedir.

public static string EncryptText(string input, string password)
{
    // Get the bytes of the string
    byte[] bytesToBeEncrypted = Encoding.UTF8.GetBytes(input);
    byte[] passwordBytes = Encoding.UTF8.GetBytes(password);

    // Hash the password with SHA256
    passwordBytes = SHA256.Create().ComputeHash(passwordBytes);

    byte[] bytesEncrypted = AES_Encrypt(bytesToBeEncrypted, passwordBytes);

    string result = Convert.ToBase64String(bytesEncrypted);

    return result;
}
```

EK B8. Oylama sonuçlarının seçim merkezine gönderildikten sonra AES şifreleme algoritmasıyla çözülmesi.

```
public static string DecryptText(string input, string password)
{
    // Get the bytes of the string
    byte[] bytesToBeDecrypted = Convert.FromBase64String(input);
    byte[] passwordBytes = Encoding.UTF8.GetBytes(password);
    passwordBytes = SHA256.Create().ComputeHash(passwordBytes);

    byte[] bytesDecrypted = AES_Decrypt(bytesToBeDecrypted, passwordBytes);

    string result = Encoding.UTF8.GetString(bytesDecrypted);

    if (result=="") return null;
    else
    return result;
}
```

## EK C. Tez İçin Geliştirilen Uygulamanın Algoritmaları

### EK C1. Oy Verme İşlemi Algoritması

**Girdi**: Seçmen login ekranından parolasını ve tc kimlik numarasını girer.

**1. Adım:** Seçmenin tc kimlik numarası ve parolası veritabanında daha önceden SHA256 hash fonksiyonuyla mesaj özeti alınmış haliyle karşılaştırarak oy kullanmaya izin verilir.

**2. Adım:** Seçmen oy vermek istediği partiye oyunu kullanır.

**3. Adım:** Oy onaylama ekranında son kez oy kullanmış olduğu partiye oy vererek işlemini tamamlamak isteyip istemediği sorulur.

**4. Adım:** Seçmen evet butonuna tıkladıktan sonra 4 parti için 4'er bitten oluşturulmuş olan 16 bitlik dizi oluşturulur.

**5. Adım:** Oy verilen partiye ait 4 bitlik dizinin 4.elemanı 1 olur ve kalanı 0 olarak kalır.

**6. Adım:** Binary ifade decimal olarak dönüştürülür.

**7. Adım:** Her seçmen için g(x) = (Random katsayı * $x_i$ + Decimal) Mod 65537 formülü kullanılarak oy şifrelenir ve 4 yetkili için kısmi pay değerleri hesaplanır.

**8. Adım:** 4 yetkili için hesaplanan kısmi pay değerlerinin toplamı alınır ve veritabanına kaydedilir.

**Çıktı**: Yönetici kullanıcısıysa login olunduğunda görüntülenebilen oylama sonucu ekranındaki 1.yetkili, 2.yetkili, 3.yetkili ve 4.yetkili için hesaplanmış olan kısmi pay değerlerinin toplamı görüntülenir.

**EK C2. Oylama Sonucu İşlemi Algoritması**

**Girdi**: Yönetici login ekranından parolasını ve tc kimlik numarasını girer.

**1. Adım:** Sonuçları göster butonuna tıklanır.

**2. Adım:** Oylama sonucu ekranında görüntülenen yetkili kişilerden ikisi seçilir.

**3. Adım:** Oylama sonucunu görebilmek için şifreyi aç butonuna tıklanır.

**4. Adım:** Seçilen yetkililer kısmi oy bilgilerini girerek Lagrange intepolasyonu ile yeniden yapılandırılmış oylama sonucu hesaplar.

**5. Adım:** Tüm yetkililer iki kişi olarak giriş yaparak yeniden yapılandırılmış sonuçlarının aynı olduğunu görüntüler.

**Çıktı**: Oy verilen partilere göre oy sonuçları listelenir.

# ÖZGEÇMİŞ

Selin DEMİRBİLEK AYYILDIZ, 1993 yılında Tekirdağ'da doğdu. 2012 yılında Trakya Üniversitesi Bilgisayar Mühendisliği Bölümü'nde lisans eğitimine başladı ve 2016 yılında tamamladı. Bunun yanında 2012-2016 yılları arasında Anadolu Üniversitesi'nde İşletme lisans eğitimi aldı. 2017 yılında Trakya Üniversitesi Fen Bilimleri Enstitüsü'nde Bilgisayar Mühendisliği alanında yüksek lisansa başladı. Ocak 2018 – Ocak 2021 tarihleri arasında İstanbul'da Ericsson firmasına bağlı outsource olarak Garanti Teknoloji'de Yazılım Test Mühendisi olarak çalışmaya başladı. Şubat 2021 tarihinden itibaren Vakıfbank Dijital Kanallar Uygulama Geliştirme Müdürlüğü'nde Uzman İş Analisti olarak görevini sürdürmektedir.

# TEZ ÖĞRENCİSİNE AİT TEZ İLE İLGİLİ BİLİMSEL FAALİYETLER

**Uluslararası Hakemli Dergilerde Yayınlanan Makaleler**

Arda, D., Demirbilek, S., & Kavak, S. (2017). THE EFFECT OF STEGANOGRAPHY AND SECRET IMAGE SHARING SCHEME TO THE SECURITY OF CRYPTOGRAPHIC KEY. *Journal of International Scientific Publications*, ISSN 1314-7269, Volume 11.