İSTANBUL TEKNİK ÜNİVERSİTESİ
BİLGİSAYAR ve BİLİŞİM FAKÜLTESİ

MESAJLARIN ŞİFRELENMESİNDE YENİ BİR YÖNTEM VE ANDROİD UYGULAMASI

,

Bitirme Ödevi

Arzu Çakmak

040070233

Bölüm: Bilgisayar Mühendisliği
Anabilim Dalı: Bilgisayar Bilimleri

Danışman : Prof. Dr. Eşref ADALI

Aralık 2012

Özgünlük Bildirisi

1. Bu çalışmada, başka kaynaklardan yapılan tüm alıntıların, ilgili kaynaklar referans gösterilerek açıkça belirtildiğini,
2. Alıntılar dışındaki bölümlerin, özellikle projenin ana konusunu oluşturan teorik çalışmaların ve yazılım/donanımın benim tarafımdan yapıldığını bildiririm.

İstanbul, 10.01.2013

Arzu ÇAKMAK

MESAJLARIN ŞİFRELENMESİNDE YENİ BİR YÖNTEM VE ANDROİD UYGULAMASI

(ÖZET)

Gelişen teknoloji, artan bilgi birikimi ve trafiği ile bilgilerin güvenliğini sağlamak kaçınılmaz bir gereksinim haline gelmiştir. Akıllı telefonların varlığı ile tüm bilgilerimiz ve iletişimimiz artık telefonlar üzerinden yapılmaktadır. Bu anlamda bilişim etiği önemli bir kavram olarak karşımıza çıkmaktadır. Bilişim etiği açısından da önemli olan mahremiyet konusunda, bilgilerin 3. şahıslar tarafından paylaşılması istenilmemektedir.

Bu amaç doğrultusunda çok karmaşık olmaması şartı ile yapılan bir şifreleme yöntemi geliştirilmiş ve günlük kullanımda var olması amacı ile android uygulaması olarak gerçekleştirilmiş ve sınanmıştır.

Bu şifreleme yöntemi, ham metni şifrelemek için bir matris yapısı ve aynı zamanda şifreyi çözmek için de anahtarı bir matris yapısı olarak kullanmaktadır. Şifrelemek için de yine anahtara göre 12x12 boyutlu bir matris doldurulduktan sonra; anahtar matris saat yönünde her 90 derecede bir döndürülerek, şifrelenmiş matris ile bu anahtar matrisin kesişen alanları okunarak bu alanlara ham metinin karakterlerinin yazılması yoluna gidilmiştir. Tüm şifreleme işlemleri gerçekleştirildikten sonra, elde edilen matrislerdeki karakterlerin ASCII kod karşılıkları alınarak *bitmap* resim formatına çevrilmektedir. Alıcı bu resmi aldığında karma karışık bir resim görmektedir.

Şifrelenmiş metin *bitmap* resim formatında alıcıya aktarıldıktan sonra, şifrelenmiş metni çözmek için; öncelikli olarak *bitmap* resim formatındaki bilgilerin ASCII kodları karakterlere çevrilmektedir. 12x12 boyutlu matrise matrislere karakterler yerleştirilerek, anahtar matrisi 90 derece saat yönünde döndürülüp karakter matrisi okunarak şifrelenen metnin çözümü sağlanır.

Şifreleme yöntemi kullanım alanı açısından çok zor olmasına gerek duyulmamıştır. Yapılan çalışmanın amacı, günlük hayatta iletmek istediğimiz özel mesajların şifrelenerek gönderilmesini sağlaması için yeni bir yöntem geliştirilmesidir. Bu yöntem, şifrelemenin kullanımına daha çok ihtiyaç duyulan akıllı telefonlarda kullanılmasına yönelik olarak android işletim sisteminde bir uygulama olarak geliştirilmiştir.

A NEW METHOD FOR MESSAGE ENCRYPTION AND ANDROID APPLICATION

(SUMMARY)

Day by day; the technology, information and information transition are getting bigger. And also, smart phones are so popular. People use these smart phones to communicate and for a lot of other things. Under these conditions, privacy is the natural right. So; the cyriptography is a necessery technich in these days for information security.

In this way a new cyriptographic algorithm are applied. This algorithm is carried out by developing an Android Application.

Same definations about the cryptography;

Plain text: the un-encrypted, clearly readable form of a message.

Cipher text: the encrypted form of the plaintext, readable only with the key from sender.[1]

This algorithm uses a matrix in order to encyript the messeage by rotating the key matrix 90 degrees clockwise for three times. After each rotate the key matrix 90 degrees clockwise, the intersection boxes of key matrix and message matrix are represent the original characters' position in the encrypted text.

After performing all cryptographic operations, the resulting matrixes' characters are converted into ascii code.

Than that, it creates a bit map image to send it to the receiver. Then the receiver loads the image to the application in order to retrieve the plain text from the encrypted image. Then the application decrypts the image with the key supplied by the user. The key in hexadecimal base represents the chosen box in the text matrix and the ending character position.

The key can cause confusions about understanding which boxes are chosen in the matrix, if the key is represented in the decimal base. Because when the key is following as;

Key: 1245630108211…

The chosen box: **[1][2]-[4][5]-[6][3]-[0][1]-[0][8]**

or

The chosen box: **[1][2]-[4][5]-[6][3]-[0][10]-[8][2]**

To decrypt the image via the key, the key matrix in 90 degrees rotated in a clockwise is used. The image bits are representing the “1” and “0” which are ascii codes of the characters.

After converting these ascii codes to character, the characters are located into 12x12 matrix’s by controlling the ending position that are obtained via the key.

Then, the intersection of the key matrix and the character matrixes represents the plain text. Each character matrixes is processed in the order.

This crypto algorithm is implemented as an android mobile application. In this application, crypto consist all the components that represented above.

In this project, there was no need to use encryption methods very difficult in terms of use space. This cyrpto method is suitable for use in daily life.

İÇİNDEKİLER

TABLOLAR

ŞEKİLLER

1 GİRİŞ

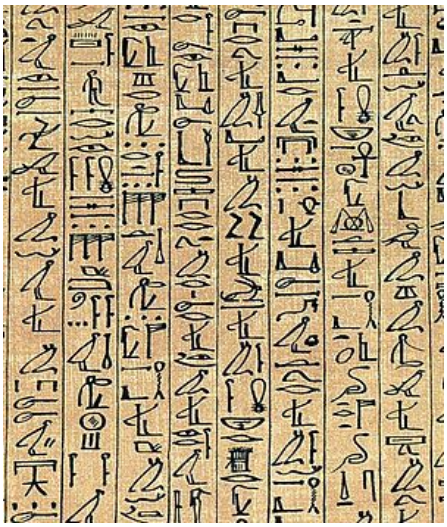
Kişiler veya kurumlar arası haberleşmede gizli tutulması gereken bilgiler olabilmektedir. Özellikle askeri alanda çok eski çağlardan beri iletişimde gizlilik önemli bir konu olmuştur. İletinin gizli tutulması konusunda günün sağladığı teknik imkanlara göre gizliliği sağlayacak yöntemler araştırılmış ve kullanılmıştır.

Eski Mısır'da, Mısır hiyeroglif yazı ile metinlerin şifrelendiği bilinmektedir. Yine bilinen bir gizleme yöntemi; ulağın kafasını tıraş edip, kafasına iletiyi yazmak ve saçları uzadıktan sonra karşı tarafa göndermektir. Bir diğer yöntem ise belli çaptaki sopanın üzerine sarılı kurdele üzerine iletiyi yazmak; kurdelede boş kalan yerleri anlamsız harfler ile doldurmak ve sadece kurdeleyi karşı tarafa göndermektir. Modern şifreleme yöntemlerinden önce kullanılmış bilinen şifreleme yöntemlerinden bir başkası "Sezar Şifresi" dir. Aşağıdaki kısımda, geçmiş dönemlerde ve günümüzde kullanılan bazı şifreleme yöntemleri anlatılmıştır:

1.1 Şifreleme Tarihçesi

Şifrelemenin tarihçesini üç dönem halinde inceleyebiliriz:

1. Makine ya da Bilgisayar kullanmayan yöntemler
2. Makine kullanan yöntemler
3. Bilgisayar kullanan yöntemler



Şekil-1: **Hiyeroglif yazı örneği**

1.1.1 Makine ya da Bilgisayar Kullanmayan Yöntemler

Eski Mısır'da gizlenecek olan belgelerin değişik hiyeroglif yöntemler ile şifrelendiği tarihi belgelerden görülmektedir. Sıradan insanların anlamayacağı hiyeroglif karakterler iletileri gizlemek amacıyla kullanılmıştır.

Yine Eski Yunan'da belirli çaptaki silindir biçimindeki sopa üzerine bir kurdele sarılmaktadır. Ardından kurdele üzerine bir satır halinde iletilmek istenen metin yazılmaktadır. Daha sonra kurdele açılır ve kurdele üzerindeki boş yerlere anlamsız harfler eklenmektedir.

Kurdeleyi alan kişide aynı çapta bir sopa bulunması halinde yazılmış olan yazı okunabilmektedir.

Daha yakın çağlara gelindiğinde "yerine koyma"ya dayalı şifreleme yöntemleri kullanılmıştır. Bu yöntem iki türlü kullanılmaktadır.

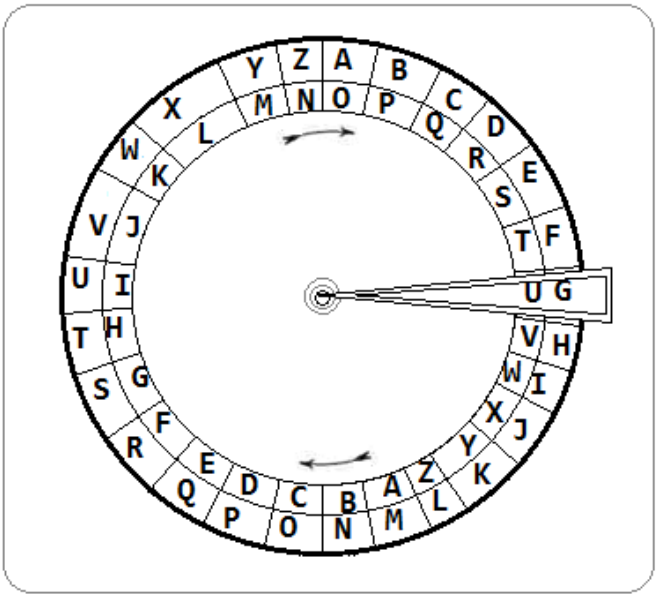
Yöntem-1 ;

Yazılı tarihin başladığı dönemden itibaren bilinen ve yaygın olarak kullanılan ilk şifreleme algoritması olarak bilinmektedir. Bu algoritmanın ana hatları şöyledir:

- Bir alfabeye dayanır (Fenike, Latin, Arap alfabesi vb.).
- Şifrelenecek metin de her bir harf yerine alfabedeki sırasından n adım ilerideki veya gerideki harf ile yer değiştirir. Alfabe bir tekerlek gibi düşünülerek son harften sonra tekrar başa dönülmektedir.

"Sezar" algoritması olarak da bilinen bu yöntemin daha eski çağlarda, Arap alfabesinden türetilmiş olan İbrani alfabesi ile yazılmış belgelerde uygulandığı bilinmektedir.

Anlatılanlardan anlaşılacağı gibi Sezar Şifreleme algoritmasının temeli bir harf yerine belli uzaklıktaki bir başka harf koymaktır. Bu yöntemde gizli tutulan asıl harf ile yerine konulan harf arasındaki uzaklık yani **n** sayısıdır. Şekil-2'de bu yönteme ilişkin bir örnek gösterilmiştir.



Şekil-2: Sezar Şifreleme yönteminin temelinin gösterimi

Örnek; Sezar şifreleme algoritması için,

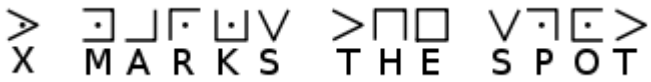
```
n                   : 3
Ham metin:  Arzu Cakmak
Şifrelenmiş metin : ofnı qoyaoy
```

Bu şifreleme algoritmasında gizli tutulan n sayısıdır ve n sayısı gönderen ile alıcı arasında mesaj gönderilmeden önce karar verilen bir sayıdır. Bu anahtar alıcı ve verici arasında gizli tutulmaktadır.

Sezar şifreleme algoritmasının zayıf yönü; örnek ile açıklanırsa, ‘a’ harfi yerine ‘o’ harfinin kullanılması ile tekrar eden harflerden yola çıkılırsa bir süre sonra harflerin karşılıkları bulunabilir.[2]

Yöntem-2;

Alfabedeki harflere karşı sırasız şekil, harf veya sayı ile karşılık vererek ham metni bu şekil, harf veya sayılar karşı düşürülmektedir. Şekil-3’te bu yönteme ilişkin iki örnek gösterilmiştir.



A	B	C	Ç	D	E	F	G	Ğ	I	İ	H	J	K
1	20	30	40	700	500	2	50	4	600	800	3	70	60

L	M	N	O	Ö	*P*	R	S	Ş	T	U	Ü	V	Y	Z	boşluk
1000	50	200	300	80	400	8	6	9	7	10	900	5	90	100	2000

Şekil-3: Yerine koyma ile şifreleme yöntemine ilişkin iki örnek

Ham metin: Arzu okula gidecek

Şifrelenmiş metin :

181009002000300601010001508007005003050060

Ebced hesabı benzeri bir uygulama Osmanlı İmparatorluğunda kullandığı düşünülmektedir.

Bu yöntemler bir makine ya da bilgisayar kullanmayan tekniklerdir.

Yerine koyma yönteminin zayıf noktası bir karaktere karşı hep aynı karakteri üretmesidir.

n:1

Ham metin: Ayşe Ali

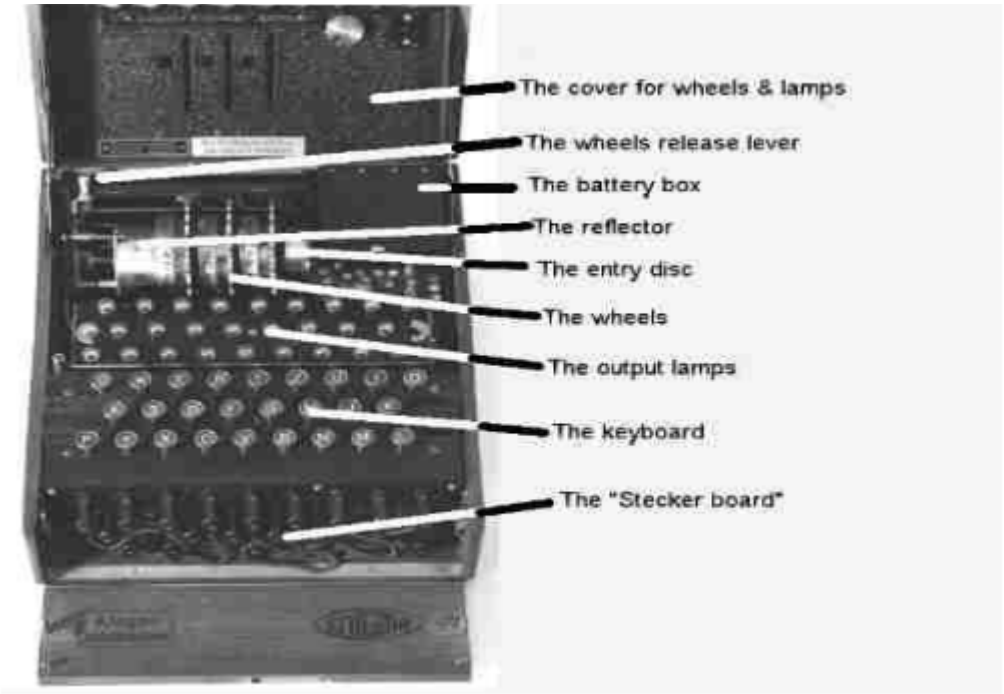
Şifrelenmiş metin :Bztf Bmh

Her iki kelimenin şifrelenmiş hallerinin ilk harflerinin aynı olduğu kolayca söylenebilir.

Metnin hangi dilde yazıldığı bilinirse şifrelenmiş metnin çözülmesinin kolay olacağı açıktır. Bu şifreleme yöntemlerinin kullanıldığı dönemlerde bilgisayarların olmadığı düşünülürse; belli ölçüde gizliliğin korunduğu söylenebilir. Bilgisayarların kullanıldığı dönemde bu algoritmaların basit oldukları açıktır.

1.1.2 Makine Kullanan Yöntemler

Bir araç kullanarak gerçekleştirilen şifreleme yöntemlerinin en bilineni "Enigma"dır. Enigma mekanik olarak yapılmış bir şifreleyicidir. Parolanın düzenlendiği konumlandırılan 4 çark ve bir tuş takımından oluşan bir makina ile şifreleme yapılmaktadır. Şekil-4'te Enigma şifreleme makinesi görülmektedir.

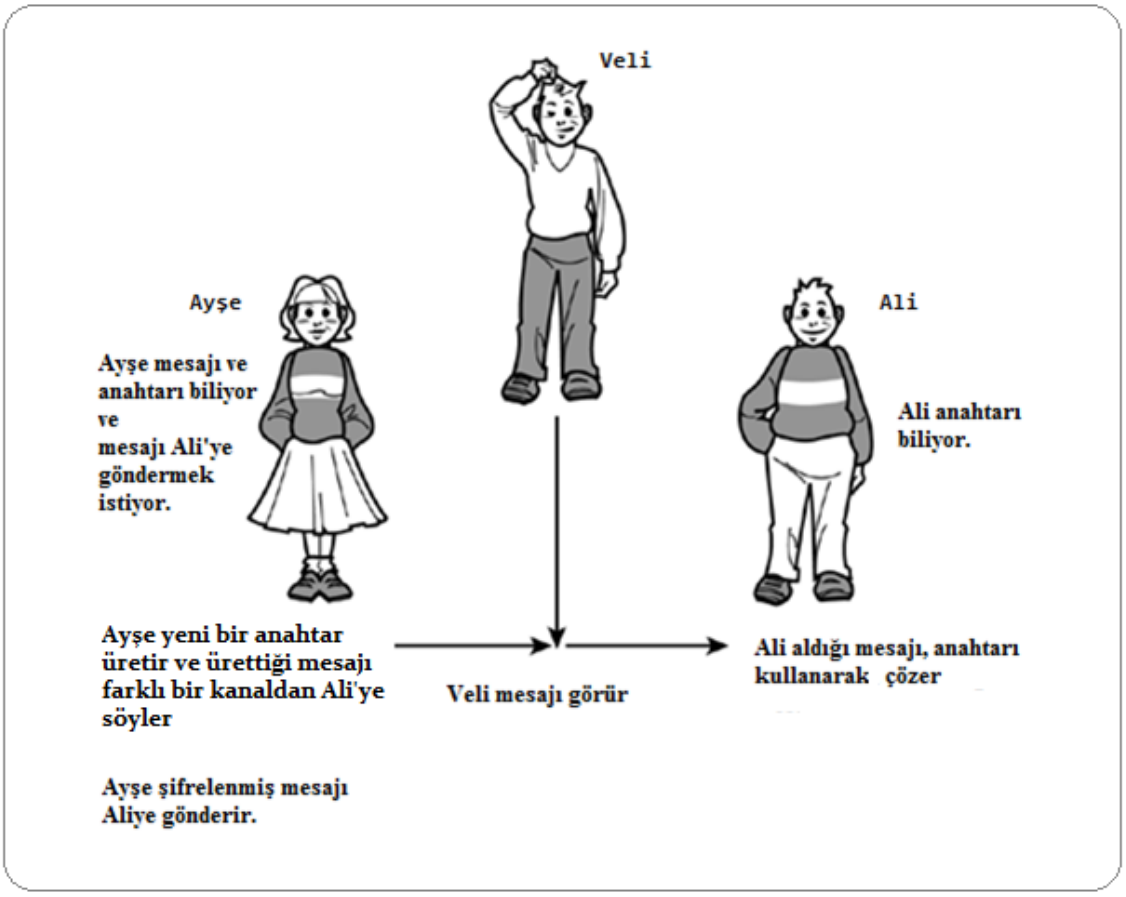


Şekil-4: Enigma şifreleme aygıtı [4]

Çarklar konumlandırılarak parola belirlenmiş olur ve bunun arkasından tuş takımında yazılan her metin şifrelenmiş metne dönüştürülür. "Enigma" 2. Dünya Savaşı sırasında Alman silahlı Kuvvetleri tarafından kullanılmıştır. Enigma'nın şifreleme yöntemini çözmek üzere 2000 dolayında bilim adamının iki yıl boyunca çalıştıkları ve çözemedikleri bilinen bir hikayedir. Ancak Enigma aygıtının ele geçirilmesi sonucunda tüm sırları çözülmüştür. Enigma şifreleme aygıtından öğrenilen ders şöyledir: Şifreleme yönteminin gizli tutulması yanlıştır; doğru olan parolanın gizlenmesidir. Şifreleme algoritmasının açık olması, şifreleme yönteminin sağlamlığını ölçmek için fırsat oluşturmaktadır.

1.1.3 Bilgisayar Kullanan Yöntemler

Bilgisayarlı ya da bilgisayarsız şifreleme yöntemleri temel olarak, simetrik ve asimetrik şifreleme yöntemleri olarak sınıflandırılırlar. Simetrik şifrelemeye ilişkin durum Şekil-5'te gösterilmiştir. Bu örnekte Ali ile Ayşe iletilerini başkalarından saklamak istemektedirler. Bu nedenle, iletilerini şifrelemeden önce, kendi aralarında bir parola belirlerler. Daha sonra gönderecekleri iletileri bu parola ile birbirlerine gönderirler. Şifrelenmiş metin aynı parola ile çözülür. Bu nedenle simetrik şifreleme adını almıştır.



Şekil-5: Simetrik şifreleme yöntemleri senaryosu

Bundan sonraki dönemde şifreleme algoritmaları bilgisayar destekli şifreleme yöntemleri olarak geliştirilmiştir. Bu dönem geliştirilmiş olan yöntemlerden en çok bilineni DES (Digital Encription Standart), 3-li DES , AES (Advaced Encription Standart) dir. Bu

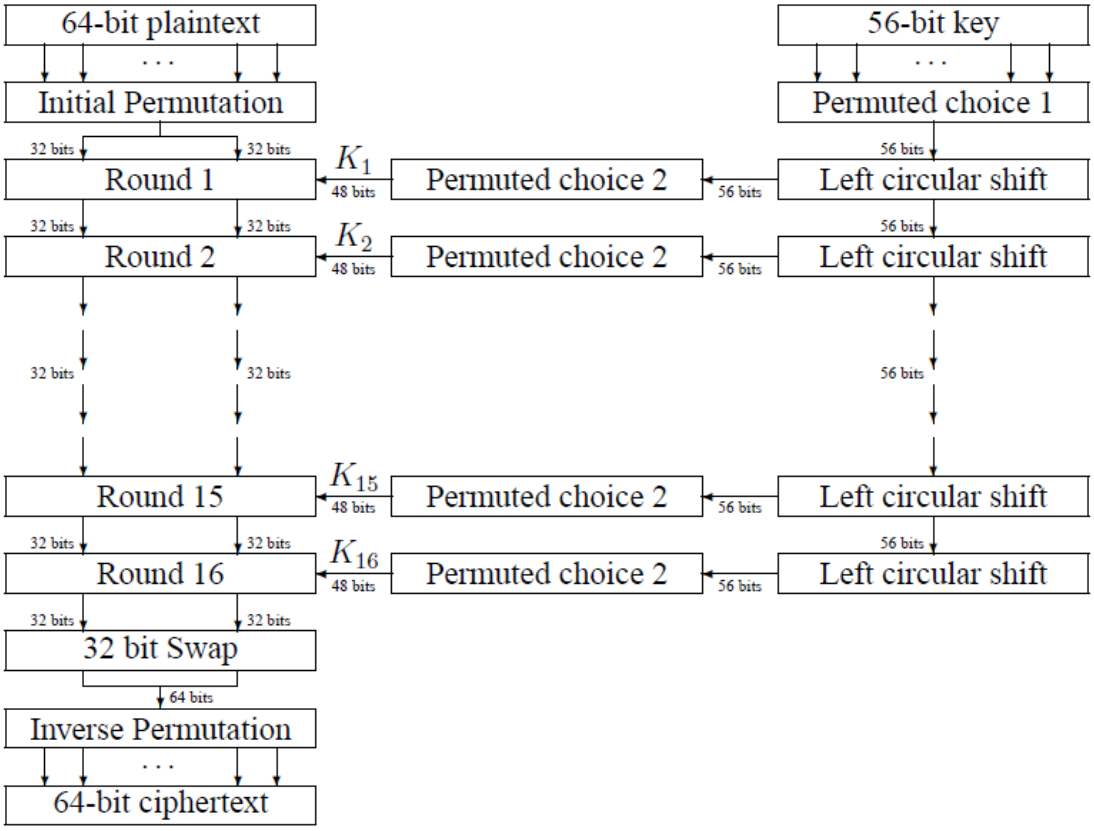
şifreleme yöntemleri simetrik şifreleme yöntemi olarak bilinmektedir. Asimetrik olarak bilinen ise şifreleme yöntemi ise RSA'dır. Bu şifreleme yöntemleri ile ilgili ayrıntılar ikinci bölüm içerisinde verilecektir.

Şifreleme algoritmaları sadece metinleri şifrelemek ile sınırlı değil sesli konuşmaları da şifrelemek üzere kullanılabilmektedir. Örneğin DES algoritması sesi şifreleyebilecek özelliğe sahiptir. Bir sesin şifrelenebilmesi için; şifreleme algoritmasının sesi işleyebilecek kadar hızlı olması gerekir. RSA daha yavaş çalışan ve yazılım temelli olduğu için ses şifrelemede kullanılamaz.

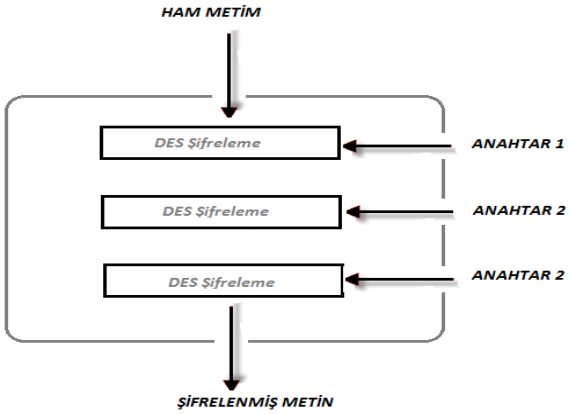
DES algoritmasının sağladığı en önemli özelliklerden bir tanesi bir karaktere karşılık hep aynı karakteri üretmemesidir.[5]

DES şifreleme yöntemi 64 bit blok şifreleyici kullanmaktadır. Şifrelenmiş metin, şifrelenmiş 6 bitlik bir anahtar ile üretilir. Şifrelenen metnin her byte'nın en düşük anlamlı biti eşlik biti olarak kullanılmaktadır. Eğer mesaj biti sayısı 64'e bölünebilir değil ise; son blok doldurulur. Şifrelemeyi daha da zorlaştırmak için permütasyonlar ve yerine koyma yöntemleri de dahil edilmiştir. İlk olarak 64 bitlik şifrelenmiş metin üzerinde bir permütasyon yaparak; 32 bitlik L_i ve R_i biçiminde iki parçaya bölünür. DES şifreleme yönteminde seçilen 16 bit şifrelenmiş metin ile ham metin arasındaki korelasyonu ortadan kaldırmayı garanti etmektedir. Şekil-5'te DES şifreleme algoritmasının ana hatları gösterilmiştir.

DES algoritması 1990'lı yıllarda bilinen en güçlü algoritma idi. Ancak bilgisayarların hızlarının ve yeteneklerinin artması ile kırılmazlık özelliğini yitirmiştir. Bunun için 3'lü DES yöntemi kullanılmaya başlamıştır. Bu şifreleme yöntemi DES algoritmasını aynı metin bloklarına 3 kere uygulamaktadır. Bu nedenle 3 tane DES anahtarı içermektedir. Anahtarlar farklı da olabilir aynıda olabilir. Fakat anahtarların farklı olması şifrelemeyi daha da güçlendirir. Şekil-6'da üçlü DES şifreleme algoritması gösterilmiştir.



Şekil-6: DES şifreleme algoritmasının ana hatları[6]



Şekil-7: Üçlü DES şifreleme algoritmasının ana hatları

Bu yöntemler ile ilgili çok sayıda yayın bulunmaktadır. Bunlardan bir kaçı kaynakçada yer almaktadır.

RSA Şifreleme Yöntemi

Asimetrik şifreleme yöntemidir. Bu yöntemde iki anahtar bulunur. Bunlardan birine açık diğerine özel anahtar denir. Açık anahtar ile şifrelenen bir metin ancak o açık anahtarı üretenin elinde bulunan özel anahtar ile çözülebilir.[3]

RSA algoritmasının yaygın kullanıldığı bir uygulama internet bankacılığıdır. Bu örnekte, bankaya açık adı (müşteri numarası) ile bağlanan müşteriye, banka kendi ürettiği açık anahtarını müşteriye gönderir. Müşterinin gönderdiği her mesaj bu açık anahtarla şifrelenir. Şifrelenmiş metni ancak banka çözebilir.

AES Şifreleme Yöntemi

Bilgisayarların hızlarının artması sonucunda DES algoritması ile şifrelenmiş metinlerin çözülme süreleri kısalmıştır. Bu nedenle şifreleme gücü daha yüksek olana algoritma arayışlarına gidilmiş AES böyle geliştirilmiştir.

Android'in açık kaynak kodlu işletim sistemi olması ve mobil platformlara uygulama

geliştirmek isteyen insanlar için bir kolaylık sağlaması ile de geliştirilen şifreleme yöntemi Android uygulaması olarak gerçekleştirilmiştir.

Şifreleme algoritmaları tek kullanımlık parola üretiminde de kullanılmaktadır.

1.2 Tez Kapsamı

- Giriş bölümünde, konunun genel tanıtımı yapılmış, şifreleme ile ilgili ayrıntılar verilmiş ve çalışmaya yardımcı olan yöntemler anlatılmıştır.
- İkinci kısımda, projenin amacı, kapsamı, risk yönetimi ve zamanlama yer almıştır.
- Proje Kapsamı bölümünde, projede kullanılan terimler tanıtılmış ve önerilen şifreleme yöntemi adım adım açıklanmıştır.
- Analiz ve modelleme bölümünde, şifreleme yönteminin nasıl gerçekleştirileceği açıklanmış, anahtar yapısının ayrıntılı analizi yapılmıştır.
- Daha sonra, şifrelemenin Android ile gerçekleştirilmesi hakkında bilgi verilmiş ve arayüz görüntüleri konulmuş ve kullanımı açıklanmıştır.

- Sonraki bölümde ise, şifreleme yöntemi hakkında yorumlar yer almakta ve proje çıktıları anlatılmaktadır.

2 PROJENİN TANIMI VE PLANI

Bu bölüm projenin tümü ile ilgili genel çalışma bilgisinin içermektedir.

2.1 Projenin Amacı

Hedefimiz kısa metinlerin (mesajların, iletilerin) kısa süre için şifrelenmesidir. Bu nedenle çok kuvvetli bir şifreleme algoritması geliştirmeye gerek olmadığını kabul ediyoruz. Dolayısı ile algoritmamızın programlanmış halinde çok kısa ve hızlı olmasını hedefliyoruz. Şifreleme algoritması uzmanlarca değil de, uzman olmayanların çözemeyeceği şekilde kullanılmaktadır. Böyle bir hedef basit şifreleme algoritmalarının neler yapabileceğini göstererek çok basit bir algoritma gerçekleştirecektir. Cep telefonlarının yaygınlaşması ile telefonlar ile kısa mesaj gönderimi hayatımıza girmiştir. Cep telefonun üzerinden algoritma ve parola bildirilmeksizin şifrelenmiş metin ve ses gönderilmesi de kamu yönetimi tarafından istenmemektedir. Tez kapsamında belirlenen hedef askeri bilgilerin şifrelenmesinde kullanılacak çok güvenlikli şifreleme algoritması geliştirmesi değildir.

2.2 Projenin Kapsamı

Proje kapsamının ilk kısmında öncelikle şifreleme yöntemlerinin incelenmesi yapılmıştır. Bunun için öncelikle kaynak araştırması yapılmıştır. Mevcut şifreleme yöntemlerinin üstünlük yöntemleri değerlendirilmiş ve cep telefonu üzerinde kullanılabilecek bir algoritma tarafımızdan oluşturulmuştur. Bundan sonraki aşamada mantıksal tasarımı yapılmış olan şifreleme algoritmasının yazılması ve sınanmasıdır. Mesajın ya da metnin yazılmasında gerekli olan “metin işleyici” tarafımızdan yazılacaktır. Bu metin işleyicide hazırlanmış olan mesajlar şifreleyiciye aktarılacak ve şifrelenmiş dosya bir resim formatında alıcıya gönderilecektir. Mesajın alındığı tarafta ise şifre çözücü resim dosyasını çözümleyecek ardından bunu metin göstericiye aktaracaktır.

Yukarıda anlatıldığından da görüldüğü gibi şu iş paketleri yer alacaktır:

- Metin işleyici
- Şifreleyici
- Şifre çözücü

- Metin gösterici

Mantıksal tasarımı yapılmış şifreleme yöntemi ana hatları ile ;

1. Her bir karakter bit temelinde şifrelenecektir.

2. Birinci aşama sonunda üretilmiş olan karakterler girilen metin mesajının harflerini sırası ile alacaktır. 12x12 boyutundaki matrise kutucuklar, her 90 derece döndürüldüğünde seçilen hiçbir kutucuk üst üste çakışmayacak biçimde yerleştirecektir. Yerleştirdikten sonra yerleştirilen yerler işaretlenecektir. İşaretlenen kutucuklar saat yönünde 90 derece döndürülecektir. Döndürüldükten sonra gelecek **n** harf işaretli yerlere yerleştirilecektir. Bu kutucuk şekilleri en baş haline dönünceye kadar döndürülerek tekrarlanacaktır. Daha sonra 12x12 boyutlu kutucuk matrisinde boş kalan 144-(4*n) kutu rastgele üretilen karakterler ile doldurulacaktır. Şifrelenecek metnin, bu şifreleme yöntemi ile elde edilen matris alanlarına sığmaması durumunda, artan sayıda matris kullanımına devam edilecektir.

Elde edilen harfler sırası ile ASCII kodlarına çevrilecektir. Çevrilen kodlar kendi içinde çeşitlendirildikten sonra *bitmap image* çevrildikten sonra karşı tarafa gönderilecektir. Daha sonra kutucuklardaki işaretli alanların şifrelenmiş sayıları da parola olarak program ile karşıya gönderilecektir. Alıcı tarafta ilk aşamada *bitmap* şeklinde gelen dosya şifreleyicinin anlayacağı şekle döndürülecek ardından şifre çözücü şifreleme aşamasındaki adımları ters yönde izleyerek düz metni üretecektir.

2.3 Risk Yönetimi

Risk yönetimi zamanlama yönünden değerlendirilmiştir:

Proje için yeterli ön araştırmalardan ve hazırlıklardan sonra var olabilecek riskler listelenmiştir. Risk yönetimi ile ilgili analiz yapılmıştır.

Risk yönetimi var olan risklerin minimize edilmesi üzerinde odaklanmıştır.

Proje süresince oluşabilecek riskler şu şekildedir;

A: Dersler ve sınavlar dolayısıyla oluşabilecek zamanlama engelleri

B: Projede gerçekleşecek olan değişikliklerin beklenen dışı bir planla gerçekleşmesi

C: Proje araçları hakkında bilgi eksikliği oluşması

D: Proje amacının gerçekleştirilememesi

E: Projenin çalınması, fiziksel engeller oluşması

Raporlamalar ile kontroller sağlanacaktır.

Zamanlama garantisi gereği ve olası sorunlara karşı, resmi proje bitiş tarihinden önce

Bitimine planlanarak herhangi bir gecikmenin sorun yaratmaması planlanmıştır.

Proje sürekliliğinde oluşabilecek bir soruna karşı her gelişimde proje yedeğinin alınması hedeflenmiştir.

Tablo 1 : Risk Yönetimi

RİSK YÖNETİMİ					
ETKİ \ OLASILIK	A (%10)	B (%10)	C (%10)	D (%20)	E (%20)
5				X	X
4					
3		X	X		
2	X				
1					

2.4 Zamanlama

Proje zamanlama planlamasında, oluşabilecek değişiklikleri minimize etmek için uzun süreçli araştırma yoluna gidilmiştir.

Projede yapılması planlanan ya da yapılmış adımların listesi ve gantt diyagramı verilmiştir. Hesaplama adımları ve sonuçları aşağıda gösterilmiştir.

1. adım : Proje planı

2. adım : Şifreleme yöntemlerinin araştırılması

3. adım : Şifreleme yönteminin analizi

4. adım : Yazılım modelleme ve tasarımı

5. adım : Metin düzenleyicinin gerçekleştirilmesi

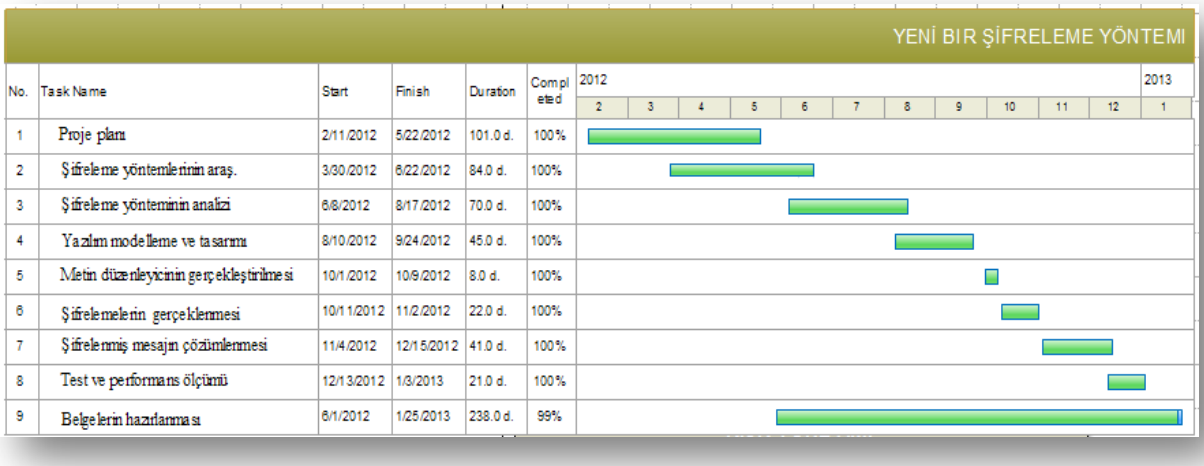
6. adım : Şifrelemelerin gerçekleştirilmesi

7. adım : Gelen şifrelenmiş mesajın çözümlenmesi

8. adım : Sınama ve performans ölçümü

9. adım : Belgelerin hazırlanması

Tablo 2: Zamanlama Tablosu



2.5 Proje Kaynakları

Danışman kontrolünde internet ve kütüphane araştırması ile proje sürdürülmüştür.

Kullanılan kaynaklar aşağıda sıralanmıştır:

- Eclipse
- Android Development Tool Bundle android 4.2.1
- JDK 1.6
- WolframAlpha hesaplama motoru
- Edraw Max 6.8
- SmartDraw 2012

3 KURAMSAL BİLGİLER

Tez kapsamında kullanılmış olan bazı tanımlar aşağıda verilmiştir:

Ham metin: Şifrelenecek metin.

Anahtar / Parola : Şifreleme ve şifrelenmiş metni çözmede kullanılacak bilgi

Eşlenik: Seçilen her bir kutunun her 90 derece döndürüldüğünde matriste karşılık geldiği hücre.

Sayfa Numarası: Şifrelenmiş metnin oluştuğu matris sayısında, her bir matrisin numarasının o matrise sayfa numarası olarak eklenmesi

3.1 Önerilen Şifreleme Yöntemi

- Şifrelenmesi istenen ham metin 12x12 boyutlu matrise ya da matrislere yerleştirilecektir.
- Şifrelenecek ham metnin harfleri; 12x12 boyutlu matrise ayrıntıları daha sonra anlatılacak kurala göre seçilen n tane kutuya yerleştirilecektir.
- Daha sonra matriste harflerin yerleştirildiği kutucuklar belirli olmak üzere, matris saat yönünde 90 derece döndürülecektir.
- Döndürmeden sonra ham metinden sırası ile yine harfler önceden belirlenen kutulara yerleştirilecektir. Daha önceden yazılmış bir harfi ezmemek için de seçilen tüm kutucukların; 90 derece döndürüldüğünde üst üste gelmemesi gerekmektedir, yani eşleniğinin kendisi ile çakışmaması için eşlenik kutulardan sadece bir tanesi seçilebilir.
- Anahtar matris; ilk konumunu alana kadar, yani 4 defa saat yönünde 90 derece ötelenecektir.
- Ham metnin bir 12x12 matrisine sığmaması durumunda bir sonraki karakterler, yeni bir matrise yerleştirilecektir.
- 4 kere 90 derece döndürme işleminden sonra ham metnin harfleri ile rastgele doldurulan matrisin **(12*12)-4n** tane matris kutucuğu boş kalmıştır. Bu boş kutular anlamsız harfle, noktalama işaretleri ve boşluk ile doldurulacaktır.

- Tüm ham metnin bir matrisin yarısında sonlanması ve seçilen kutuların da rastgele seçilmiş karakterler ile doldurulması durumunda; şifre çözümü sırasında sorun oluşmasını önlemek için, ham metnin matriste bittiği son karakterin yeri de anahtara bilgi olarak eklenmiştir.

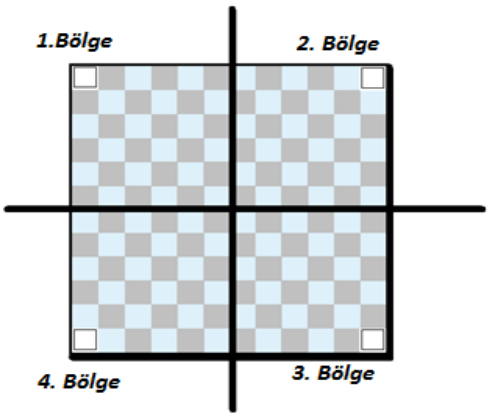
Ayrıntıları ile adım adım şifreleme;

İlk olarak ham metnin 12x12 boyutlu matrislere yerleştirilmesinde, ham metinin yerleştirileceği matris kutucukları seçilmelidir.

Seçilecek matris kutularının her 90 derece döndürmede üst üste gelme durumunda yeni yazılacak harf önceden yazılmış olan harfi ezecektir. Bu nedenle; ham metnin yazılacağı kutular seçilirken mutlaka seçilen bir kutunun eşlenikleri bir daha seçilmemelidir.

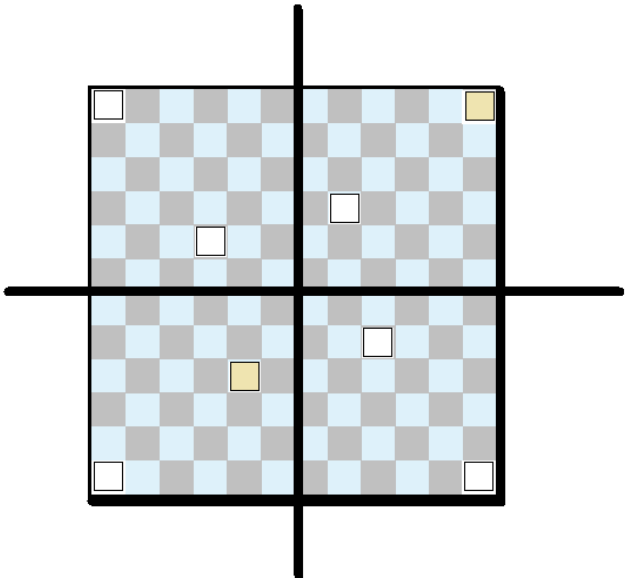
Bu kurala uygun olarak ham metni yerleştirmek için sırası ile;

Matrisin bütünündeki kutucuk seçimi için öncelikle eşlenikleri birbiri ile çakışmayacak olan kutuları 1.bölge'den seçiyoruz. Seçtiğimiz her bir kutucuğun eşleniğini de 2. Bölgeden, 3. Bölgeden ve 4. Bölgeden eşlenikleri bulunur. Durum Şekil- 8 ve Şekil-9'de gösterilmiştir



Şekil-8: Geliştirilen şifreleme algoritmasında ilk anahtar seçimi

Her bölgeden seçilen eşlenik kutulardan bir tanesi rastgele seçilerek, diğerleri elenerek; ham metinin ilk harfi bu kutucuğa yerleştirilir



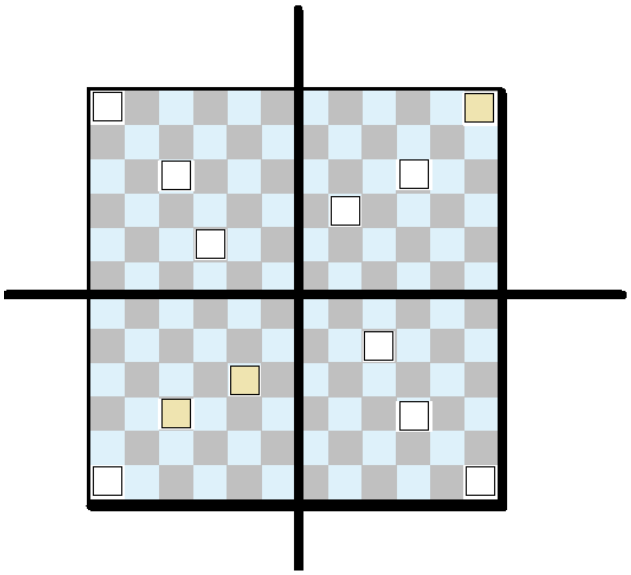
Şekil-9: Geliştirilen şifreleme algoritmasında ikinci anahtar seçimi

Şekildeki gibi rastgele 2. Bölgeden kutucuğu seçtikten sonra yine aynı şekilde 1. Bölgeden daha önce seçilmemiş rastgele bir kutu seçiyoruz.

Seçilen kutunun 1. Bölgede, 2. Bölgede, 3. Bölgede ve 4. Bölgede eşleniklerini buluyoruz ve bu eşleniklerden birini ham metnin ikinci karakterini koymak için seçiyoruz. Böylece 12x12 boyutundaki matrisin 90 derece döndürülmeden önce yazılacak ola n karakterden ikisini matrise yerleştirmiş oluyoruz.

İki karakteri yerleştirdikten sonra; üçüncü karakteri yerleştirmek için;

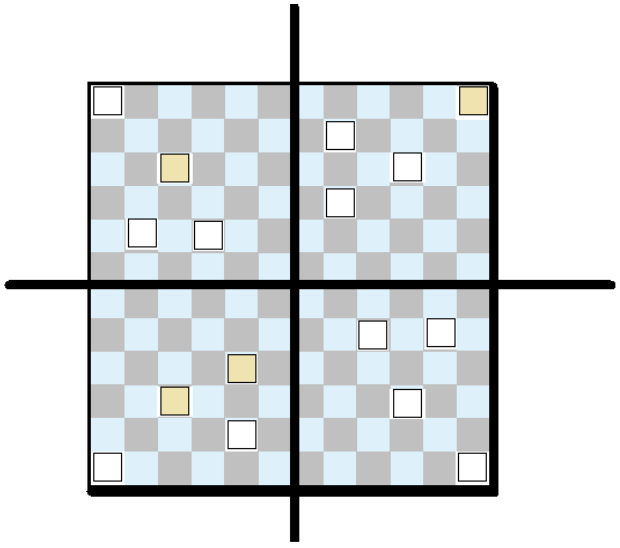
- 1. Bölgeden daha önce hiç seçilmemiş olan bir kutucuk seçilir.
- Seçilen kutucuk için; 2. Bölgede, 3. Bölgede ve 4. Bölgede eşlenik kutular bulunur.
- Bulunan kutular arasından rastgele bir tanesi seçilir.
- Seçilen bu kutuya ham metinin üçüncü karakteri yerleştirilir.



Şekil-10: Geliştirilen şifreleme algoritmasında üçüncü anahtar seçimi

Üç karakteri yerleştirdikten sonra; dördüncü karakteri yerleştirmek için;

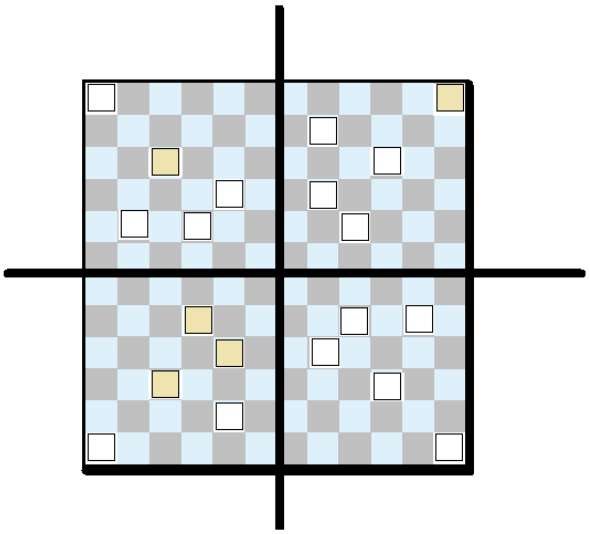
- 1.Bölgeden daha önce hiç seçilmemiş olan bir kutucuk seçilir.
- Seçilen kutucuk için; 2. Bölgede, 3. Bölgede ve 4. Bölgede eşlenik kutular bulunur.
- Bulunan kutular arasından rastgele bir tanesi seçilir.
- Seçilen bu kutuya ham metinin dördüncü karakteri yerleştirilir.



Şekil-11: Geliştirilen şifreleme algoritmasında dördüncü anahtar seçimi

Dört karakteri yerleştirdikten sonra; dördüncü karakteri yerleştirmek için;

- 1.Bölgeden daha önce hiç seçilmemiş olan bir kutucuk seçilir.
- Seçilen kutucuk için; 2. Bölgede, 3. Bölgede ve 4. Bölgede eşlenik kutular bulunur.
- Bulunan kutular arasından rastgele bir tanesi seçilir.
- Seçilen bu kutuya ham metinin beşinci karakteri yerleştirilir.

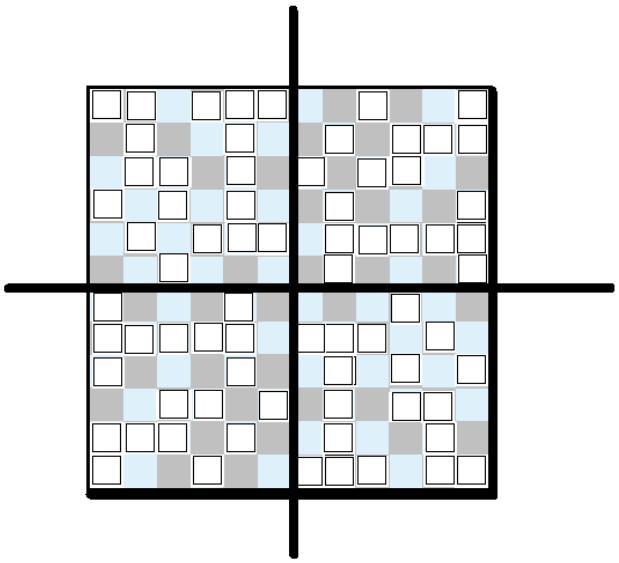


Şekil-12: Geliştirilen şifreleme algoritmasının ana hatları

12x12 matrisinden seçilecek olan n kutunun seçimi bu yöntem n kere tekrarlanarak bulunur. Bu yöntem ile matris 90 derece saat yönünde döndürüldüğünde seçilen hiç bir kutu birbirini ezmeyecektir. Bu; şifre çözme yönteminde şifrelenmiş metni karakter kaybı olmaksızın çözmek için önemlidir. Çünkü şifrenin çözümlenme aşamasında tüm matris, merkezi etrafında 90 derece saat yönünde çevrilerek okunacaktır.

Anahtar olarak gönderilecek olan bilgi, 12x12 kutucuk matrisinde hangi kutulara harf yerleştirileceğinin bilgisi ve son karakterin son matrisin hangi kutucuğuna yerleştirildiğidir.

Her bir yerleştirmeden sonra matris saat yönünde 90 derece döndürüldükten sonra cümlenin devamındaki harfler matrisin [0][0] kutucuğundan itibaren seçili kutucuklara yerleştirilecektir. Sağa 3 devir dönmeden sonra başa dönecek olan kutucuk şekli kullanılmış olacak daha sonraki bir cümlede yeni versiyon üretilecektir.



Şekil-13: Geliştirilen şifreleme algoritmasının ana hatları

Üretilen versiyondan sonra 12x12 matris simetrik olarak bilgi ile doldurulmuş olacaktır.

Harflerin üst üste ezme olasılığı kutucuklar seçilirken kullanılan algoritma ile engellenmektedir.

12x12 matrisinde n=18 seçilirse eğer; 144 kutucuktan her bir döndürmede 18 tane karakter yerleştirilecektir.

1. Bölgeden 36 kutucuktan 18 tanesi eşleniği ile rastgele seçilecektir.

Tüm yerleştirmelerden sonra ise elde edilen matrislerin karakterlerinin ASCII kodları ile bir *bitmap* elde edilecektir. Bu resim alıcı ile paylaşılacaktır.

Ayrıntıları ile adım adım şifreleme;

Gelen *bitmap* formatı ikilik dizi (binary string) olarak alındıktan sonra; sırası ile 12x12 yapısındaki matrislere karakterler doldurulur. Doldurulan karakterler, daha önceden bilinen anahtar ile çözülecektir.

Anahtar: matrisin hangi kutucuklarının seçildiği bilgisini ve ham metnin karakterinin hangi kutucukta sonlandığı bilgisini tutmaktadır.

Eğer ham metin matrisin tüm kutucuklarını dolduracak kadar uzun değil ise; anahtar için seçilen kutucuklar rastgele karakterler ile doldurulacağından; matrisin hangi karakter ile sonlandığı bilgisi önemlidir. Eğer ki; bu bilgi kullanılmaz ise şifresi çözülmüş metinde fazla karakterler yer alacaktır.

12x12 matrisi üzerinden hangi kutuların seçildiği bilgisi anahtar üzerinde gönderilir iken; hangi kutuların seçildiği bilgisi direkt gönderilemeyecektir. Çünkü anahtarın okunması ile ilgili aşağıdaki gibi bir sorun oluşmaktadır.

Anahtar: 1234459811212...

Anahtar bu şekilde gönderildiğinde okunmak istenirse;

(1,2), (3,4), (4,5), (9,8), (1,1), (2,1)... şeklinde okunacak ve (11,2) olarak gönderilmek istenen kutucuk (1,1) olarak algılanacaktır. Bu şekilde yanlış çözümlemeyi engellemek için anahtar kutucuklarının tek basamaklı kullanılması sorunu çözmektedir. Bunun için de ;

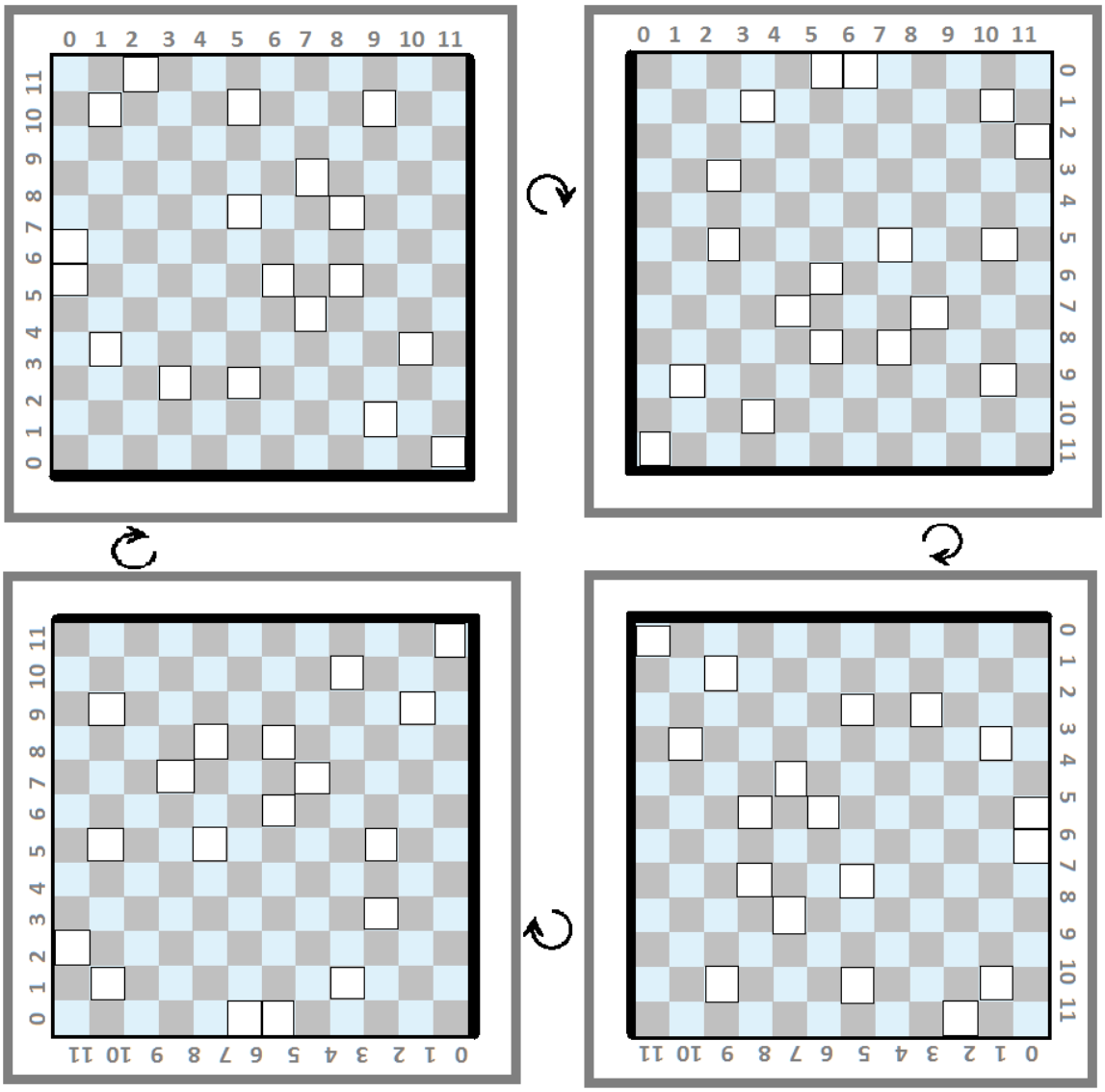
anahtar **onaltılık** tabanda seçilmiştir. Örnekteki anahtarın yeni şekli;

Anahtar: 12344598b2c... şeklindedir.

Anahtar çözüldükten sonra da; *bitmap*'ten elde edilen matrisler için sırası ile;

- Anahtar öncelikle hangi kutucuklardan karakter okumamız gerektiğini söylemektedir. Anahtar ile öncelikle ilk matristen okuduğumuz karakterleri alırız.
- Daha sonra matrisi 90 derece saat yönünde çevirerek elde edilen yeni matrisi, anahtarımız ile okuruz ve yeni bilgileri elde ederiz.
- Elde edilen bilgilerden ilk iki karakter onaltılık tabanda sayfa numarasıdır. Bunu çözülen metne eklemiyoruz.
- 2. tur için ilk matristen karakterleri okumak için; matrisi tekrar 90 derece saat yönünde çevirerek elde edilen yeni matrisi, anahtarımız ile okuruz ve yeni bilgileri elde ederiz.
- 3. tur için ilk matristen karakterleri okumak için; matrisi tekrar 90 derece saat yönünde çevirerek elde edilen yeni matrisi, anahtarımız ile okuruz ve yeni bilgileri elde ederiz

- İlk matrisin okuması gerçekleştirilir.
- Bu işlemleri elde ettiğimiz tüm matrisler için yapıyoruz.
- Son matris için hangi kutucuktan itibaren okumayı bırakacağımız kontrolünü, anahtarın en sonunda gelen bilgi ile yapıyoruz.



Şekil-14: Şifrelenmiş metnin çözümü

Geliştirilen bu şifreleme yönteminin kodlamasının gerçekleştirilmesi için ilk adım olarak bir metin düzenleyici gerekmekteydi. Bunun için belirtilen teknolojiler ile bir *android*

virtual machine ile metin düzenleyici uygulaması geliştirilmiştir.[7] Girilen metin "Encyript" düğmesi ile şifrelenecek bir *bitmap* resme çevrilecek ve alıcıya telefon üzerindeki *whataapp* ya da *mms* kullanılarak gönderilecektir. [8]

4 ANALİZ VE MODELLEME

Şifreleme ve şifre çözme yöntemlerinin ayrıntılar verilmektedir.

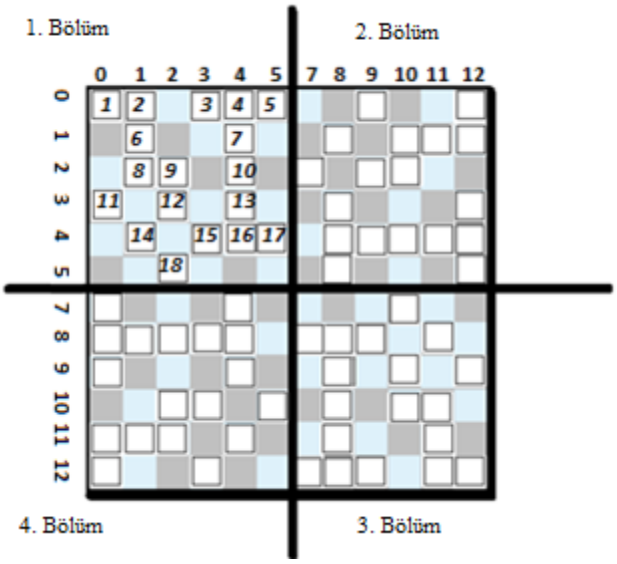
4.1 Şifreleme Yönteminin Analizi

Şifreleme yöntemi şifreleme ve şifrelenmiş metnin alıcıya gönderildikten sonra şifresinin çözülmesi olarak iki temel kısımdan oluşmaktadır.

4.1.1 Şifreleme

Öncelikle 12x12 boyutlu matris üzerinde 1.bölümden olası anahtar adayları seçildikten sonra, bir anahtar adayının 2. bölüm, 3. bölüm ve 4. bölümden eşlenikleri bulunur.

Bunun nedeni yazılacak olan mesajın 1.bölümü doldurduktan sonra diğer kısımlara sıra ile geçmesini, yani mesajın ¼ kısmının 1. Bölümde, 2. ¼ kısmının 2. Bölümde, 3. ¼ kısmının 3. Bölümde ve 4. ¼ kısmının 4. Bölümde olması engellenecektir.



Şekil-15: Şifreleme için anahtar seçimi

1 numaralı hücrenin yansımaları →[0][0], [0][12], [12][0], [12][12]

2 numaralı hücrenin yansımaları →[0][1], [1][12], [12][11], [11][0]

3 numaralı hücrenin yansımaları →[0][3], [3][12], [12][9], [9][0]

4 numaralı hücrenin yansımaları →[0][4], [4][12], [12][8], [8][0]

5 numaralı hücrenin yansımaları →[0][5], [5][12], [12][7], [7][0]

6 numaralı hücrenin yansımaları →[1][1], [1][11], [11][11], [11][1]

7 numaralı hücrenin yansımaları →[1][4], [4][11], [11][8], [8][1]

8 numaralı hücrenin yansımaları →[2][1], [1][10], [10][11], [11][2]

9 numaralı hücrenin yansımaları →[2][2], [2][10], [10][10], [10][2]

10 numaralı hücrenin yansımaları →[2][4], [4][10], [10][8], [8][2]

11 numaralı hücrenin yansımaları →[3][0], [0][9], [9][12], [12][3]

12 numaralı hücrenin yansımaları →[3][2], [2][9], [9][10], [10][3]

13 numaralı hücrenin yansımaları →[3][4], [4][9], [9][8], [8][3]

14 numaralı hücrenin yansımaları →[4][1], [1][8], [8][11], [11][4]

15 numaralı hücrenin yansımaları →[4][3], [3][8], [8][9], [9][4]

16 numaralı hücrenin yansımaları →[4][4], [4][8], [8][8], [8][4]

17 numaralı hücrenin yansımaları →[4][5], [5][8], [8][7], [7][4]

18 numaralı hücrenin yansımaları →[5][2], [2][7], [7][10], [10][5]

Her 18 hücre listesinin her birinden bir tane hücre seçerek anahtar elde edilmiş olacaktır. Bu ezilmeleri de önceleyecektir. Örnek anahtar seçimi yapılırsa;

Anahtar hücreleri:

[12][12] -- [1][12] -- [12][9] -- [8][0] -- [0][5] -- [1][11] -- [8][1] -- [10][11] -- [2][10] -- [2][4] -- [0][9] -- [10][3] -- [4][9] -- [8][11] -- [3][8] -- [8][8] -- [7][4] -- [10][5]

Seçilen bu yapı için de ham metin eğer doldurulursa sırası ile 4 turda doldurulacaktır.

Sırası ile her turda harflerin yazılacağı hücreler:

1.Tur : [12][12] -- [1][12] -- [12][9] -- [8][0] -- [0][5] -- [1][11] -- [8][1] -- [10][11] -- [2][10] -- [2][4] -- [0][9] -- [10][3] -- [4][9] -- [8][11] -- [3][8] -- [8][8] -- [7][4] -- [10][5]

2.Tur : [0][0] -- [2][11] -- [9][0] -- [0][4] -- [5][12] -- [11][11] -- [1][4] -- [11][2] -- [10][10] -- [4][10] -- [9][12] -- [3] [2] -- [9][8] -- [11][4] -- [8][9] -- [8][4] -- [4][5] -- [5][2]

3.Tur : [0][12] -- [11][0] -- [0][3] -- [4][12] -- [12][7] -- [11][1] -- [4][11] -- [2][1] -- [10][2] -- [10][8] -- [12][3] -- [2][9] -- [8][3] -- [4][1] -- [9][4] -- [4][4] -- [5][8] -- [2][7]

4.Tur : [12][0] -- [0][1] -- [3][12] -- [12][8] -- [7][0] -- [1][1] -- [11][8] -- [1][10] -- [2][2] -- [8][2] -- [3][0] -- [9][10] -- [3][4] -- [1][8] -- [4][3] -- [4][8] -- [8][7] -- [7][10]

Bu matrislerin kutucukları sırası ile ham metnin harfleri ile doldurulacaktır.

Eğer ki ham metin bu kutuya sığmaz ise başa dönülecek ve aynı durumda yeniden aynı matris doldurulacaktır. Sayfa numaraları her metrisin ilk karakterine eklenecektir. Şifreleme gerçekleştirilmiş olacaktır.

4.1.2 Anahtar Yapısı Analizi

Anahtarın çözülme olasılığı şifreleme yönteminin gücünü gösterecektir.

Anahtarın Çözülme Olasılığı;

Toplamda 12x12 matrisinde 4'e böldüğümüzde bir alanda 36 kutucuk bulunmaktadır.

Bu 36 kutucuktan n tanesi seçilecektir.

$P=\binom{36}{n}$ farklı kutu seçilme olasılığı mevcuttur.

Seçilen bu **P** farklı kutu içinden de her biri için anahtarımızı seçebileceğimiz 4 farklı matris bölmesi olduğunda olasılık her bir kutu için 4 farklı olasılık mevcuttur.

Seçilen P farklı kombinasyon ile seçilen n anahtar içinde, genel matristeki yer seçimi için;

4^n farklı anahtar kombinasyonu mevcuttur.

Bu demektir ki ;

Anahtar sayısı : **A**

Seçilecek kutucuk sayısı: **n**

Belirli seçilen bir n değeri için;

$$A = 4^n P$$

Tüm üretilebilecek anahtar sayısı, [9]

$$\mathbf{A} = \sum_{n=0}^{36} \binom{36}{n} * 4^n$$

n=1 → 36*4 = 144

n=2 → 630*16=10080

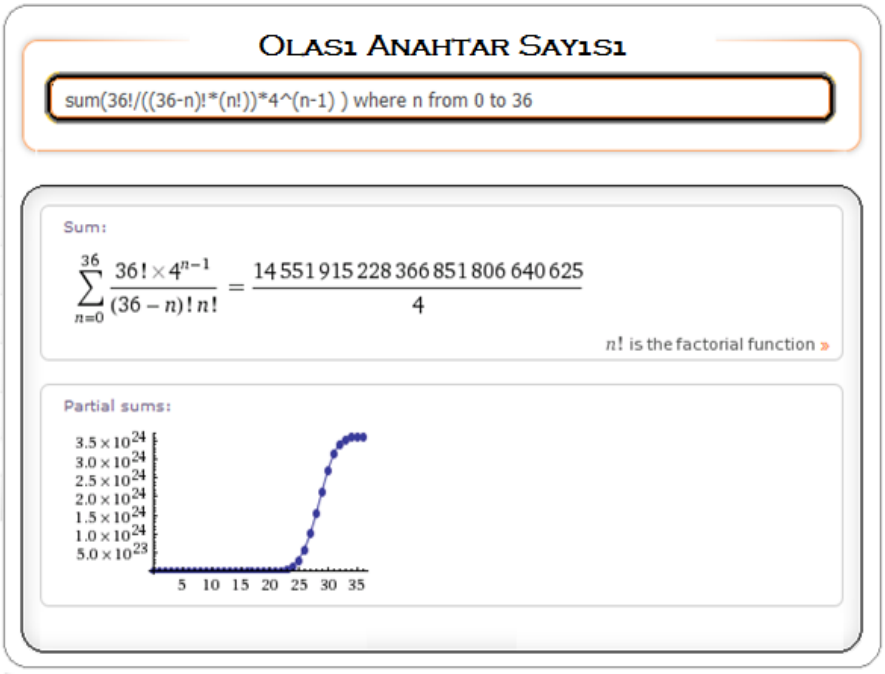
n=3 → 7140*64=456960

n=4 → 58905*256=15079680

n=5 → 376992*1024=386039808.....

Olası tüm anahtar sayısı;[10]

Tablo 3: Şifre yöntemindeki anahtar sayısı



Hesaplama WorlframAlpha hesaplama motoru ile yapılmıştır.

4.1.3 Şifre Çözme

Şifreleme işlemi yapılıp ASCII kodları *bitmap* image'e çevrildikten sonra şifre çözme gerçekleştirilecektir.

- *Bitmap image'in* bitleri ASCII kodlarını temsil ettiğinden bu kodlar öncelikle 8 bit olarak alınıp her biri karakterlere çevrilmektir. Çevrilen karakterler 12x12 boyutlu matrislere sırası ile doldurulmaktadır.
- Daha sonra anahtar yapısından matris oluşturulmaktadır.
- Anahtar saat yönünde 90 derece çevrilecektir.
- Her 90 derece döndürmeden sonra anahtar matris ile karakter matrisin kesişiminden elde edilen karakterler ham metnin karakterlerini vermektedir.
- Bu işlem 2 tur tekrarlandıktan sonra, 3. turda anahtarın sonunda gönderilen sonlanma karakterine kadar karakter matrisi okunacaktır.

- Tüm matrisler için bu işlemin gerçekleştirilmesi ile şifre çözülmüş olacaktır.

4.1.4 Şifrelemede Önemli Noktalar

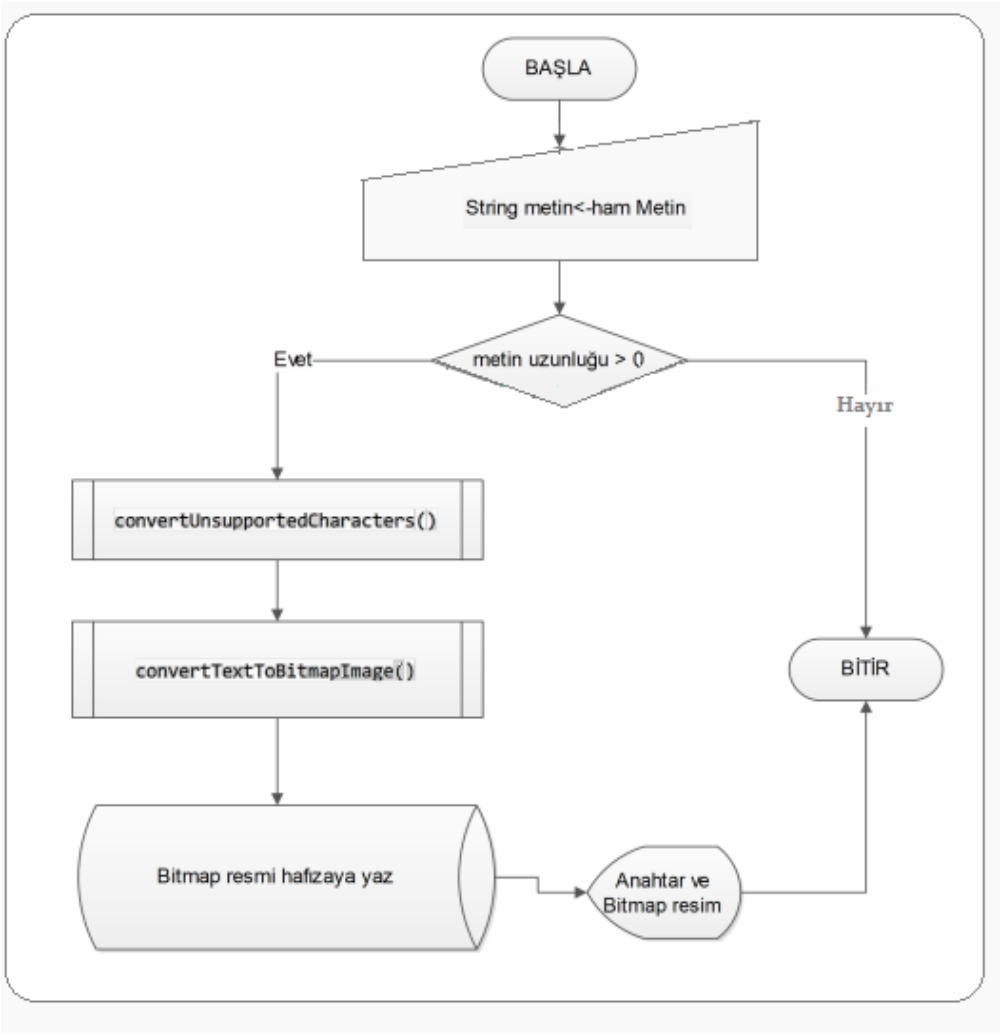
- Şifreleme yönteminin sağlıklı çalışması için **nxn** boyutlu seçilecek matris için n sayısı çift olması gerekmektedir.
- Bu sayının çok büyük seçilmesi halinde gereksiz boyutta bilgi gönderimi gerçekleşeceğinden en uygun sayının seçilmesi gerekmektedir. Daha küçük seçilen bir sayı da ise; çözüm içim üretilecek anahtar sayısı azaldığından anahtarın bulunması ve böylece şifrenin çözülmesi kolaylaşacaktır.
- Bütün matris saat yönünde 90 derece döndürüldüğü için; her 90 derece döndürüldükten sonra simetrik bir yapı elde etmenin yolu ancak kare şeklinde bir matris seçmektir.
- Bir matrise kaç harf yerleştirileceği ise; kullanıcı tarafından şifrelemenin düşük, yüksek ya da orta seviyede olması ile belirlenecektir.
- Tüm karakterlerin yerleştirilmesinden sonra ise matris ya da matrisler oluşacaktır.
- Oluşan matrisler *bitmap* resme çevrilecektir. Çevrildikten sonra ise girilen anahtar kullanılarak resim şifre çözücü ile çözülecektir.
- Anahtar yapısı onaltılık tabanda gönderilmektedir.

4.2 Modelleme

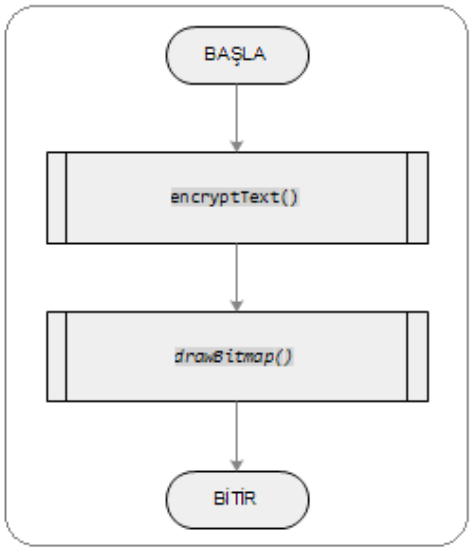
Önerilen şifreleme yönteminin uygulamada nasıl modelleneceği UML diyagramları ile anlatılmaktadır.

4.2.1 Akış Diyagramı

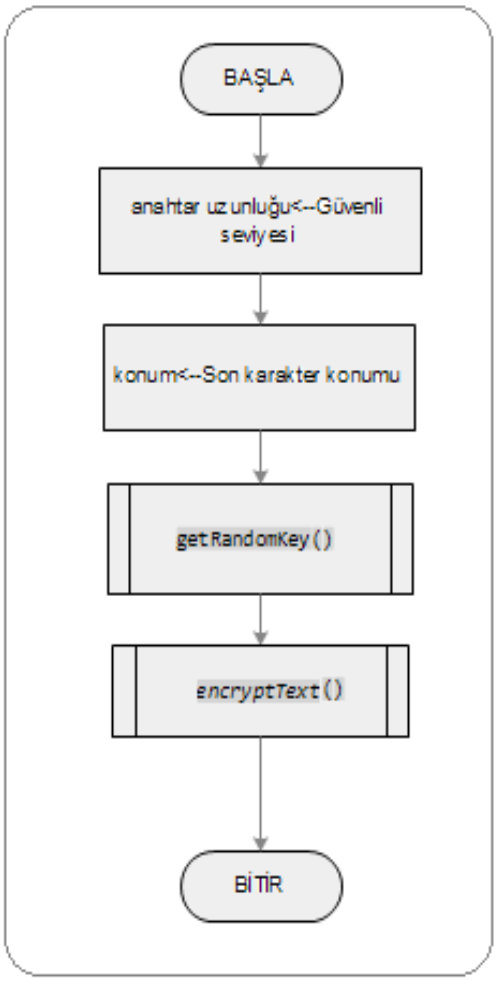
Şifreleme ve şifre çözme, alt metotları ile akış diyagramları ile gösterilmiştir.



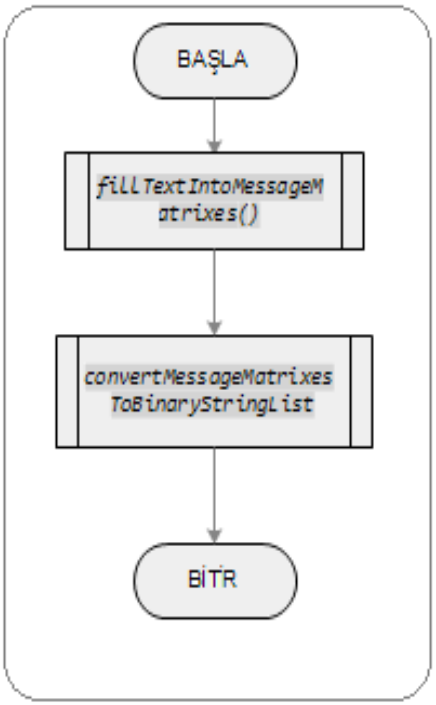
Şekil-16: Şifreleme Modellemesi Akış Diyagramı



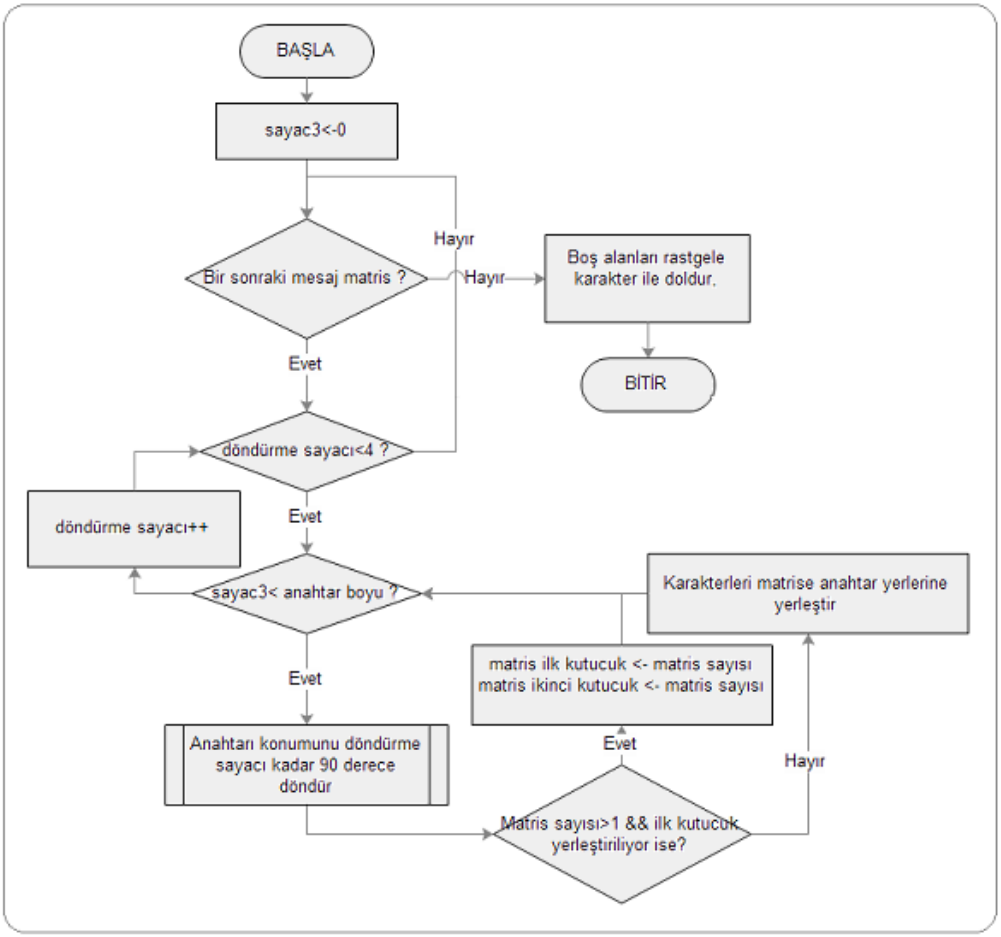
Şekil-17: Şifreleme Modellemesinde "convertTextToBitmapImage()" Akış Diyagramı



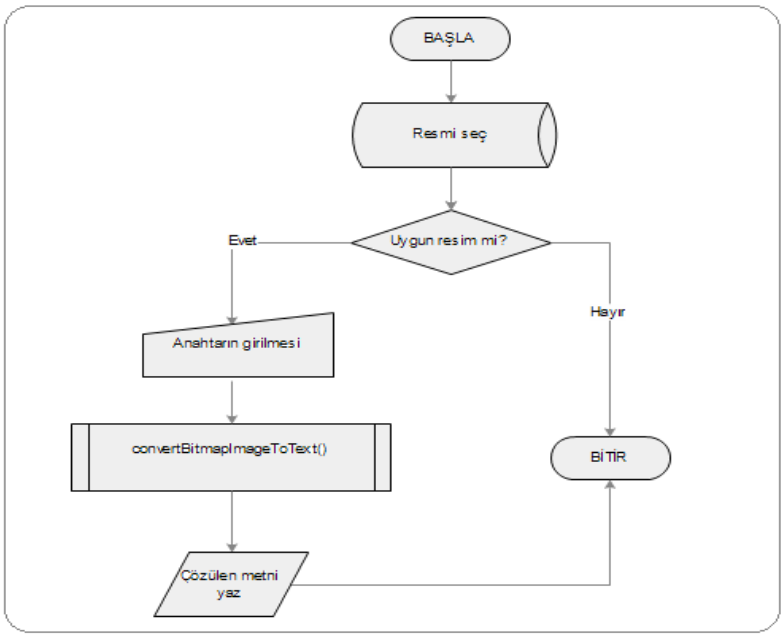
Şekil-18: Şifreleme Modellemesinde "encryptText()" Akış Diyagramı



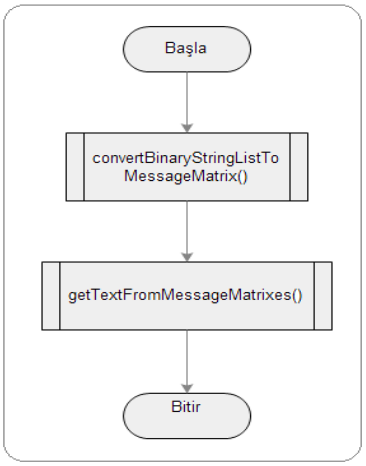
Şekil-19: Şifreleme Modellemesinde "commonController.encryptText()" Akış Diyagramı



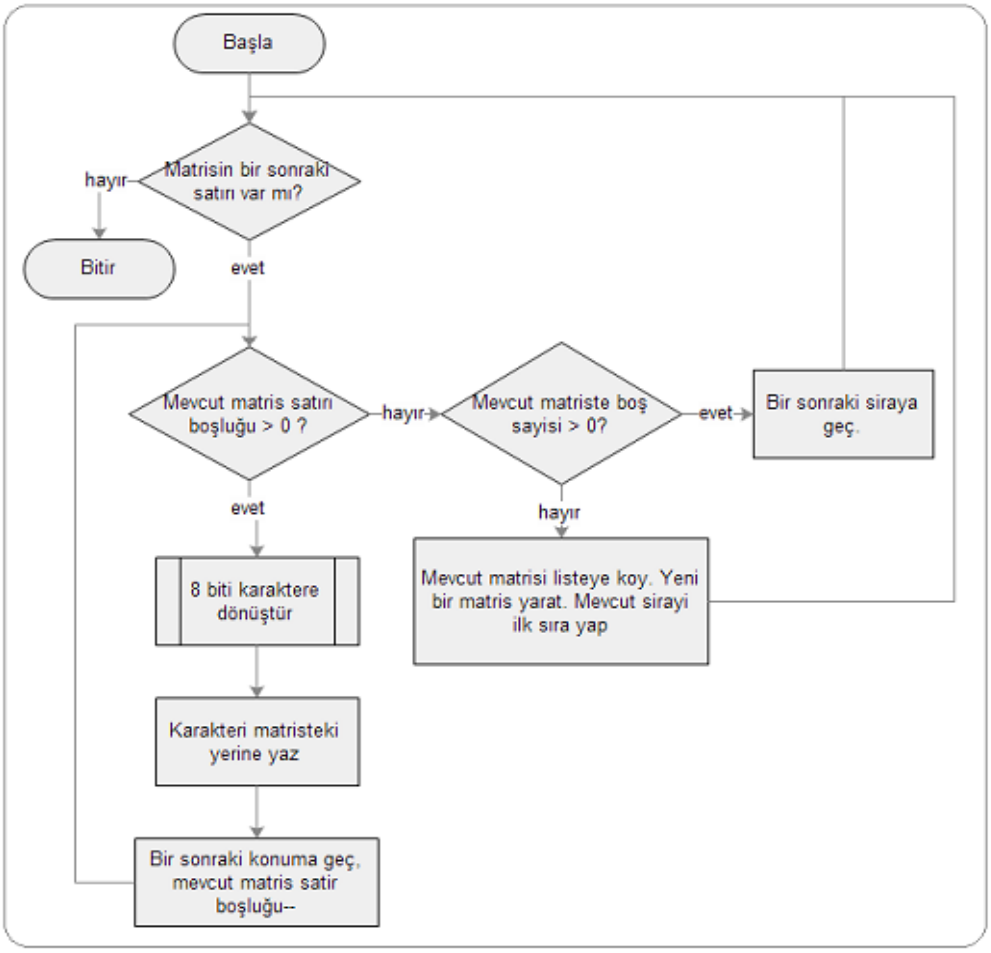
Şekil-20: Şifreleme Modellemesinde "fillTextIntoMessageMatrixes" Akış Diyagramı



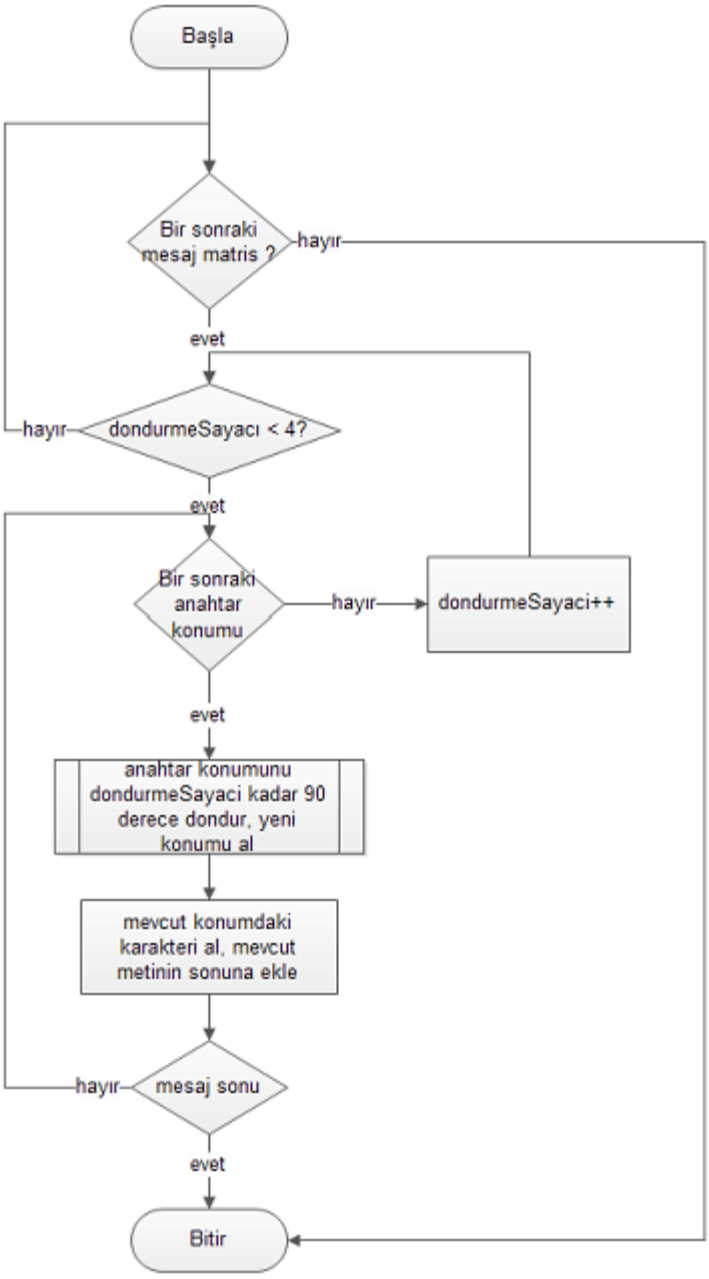
Şekil-21: Şifre Çözümü Akış Diyagramı



Şekil-22: "convertBitmapImageToText"alt metodu Akış Diyagramı



Şekil-23: "convertBinaryStringListToMessageMatrix" Akış Diyagramı

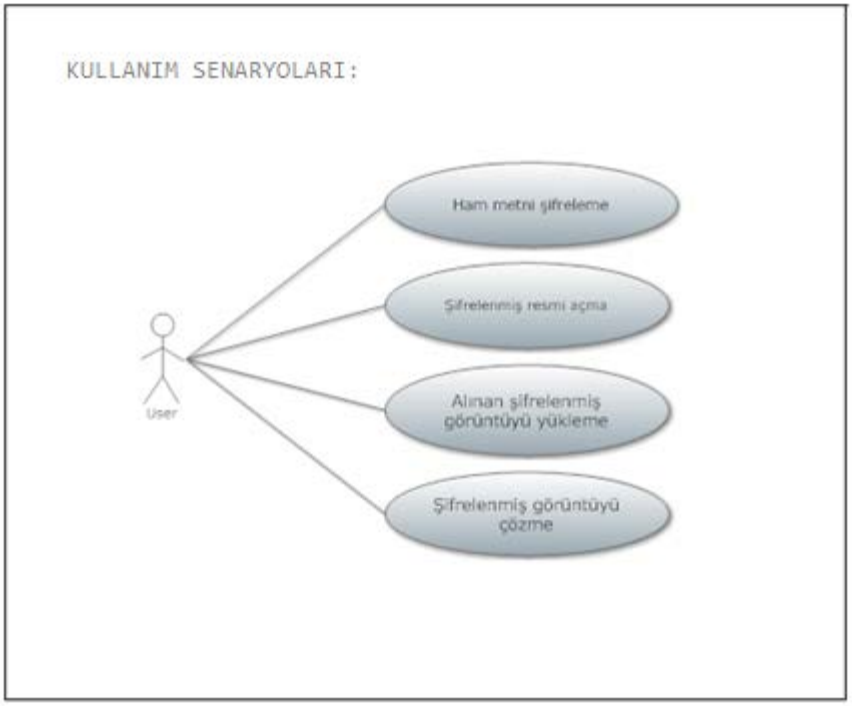


Şekil-24: "getTextFromMessageMatrixes" metodu akış diyagramı

4.2.2 Kullanım Senaryoları

Bir android uygulamasına dönüştürülen bu şifreleme yönteminde bir kullanıcı rolü mevcuttur. Bu rolün sahibi kullanıcı uygulamadaki tüm arayüzleri görebilmektedir. Kendi bir ham metni uygulamaya şifreleyip bir alıcıya gönderebildiği gibi, bir alıcı olarak kendisine de şifrelenmiş bir resim geldiğinde bildiği anahtar ile uygulamayı kullanarak

şifrelenmiş metni çözmekte ve görüntüleyebilmektedir. Şekil-13 te kullanım senaryoları örnek olarak verilmiştir.

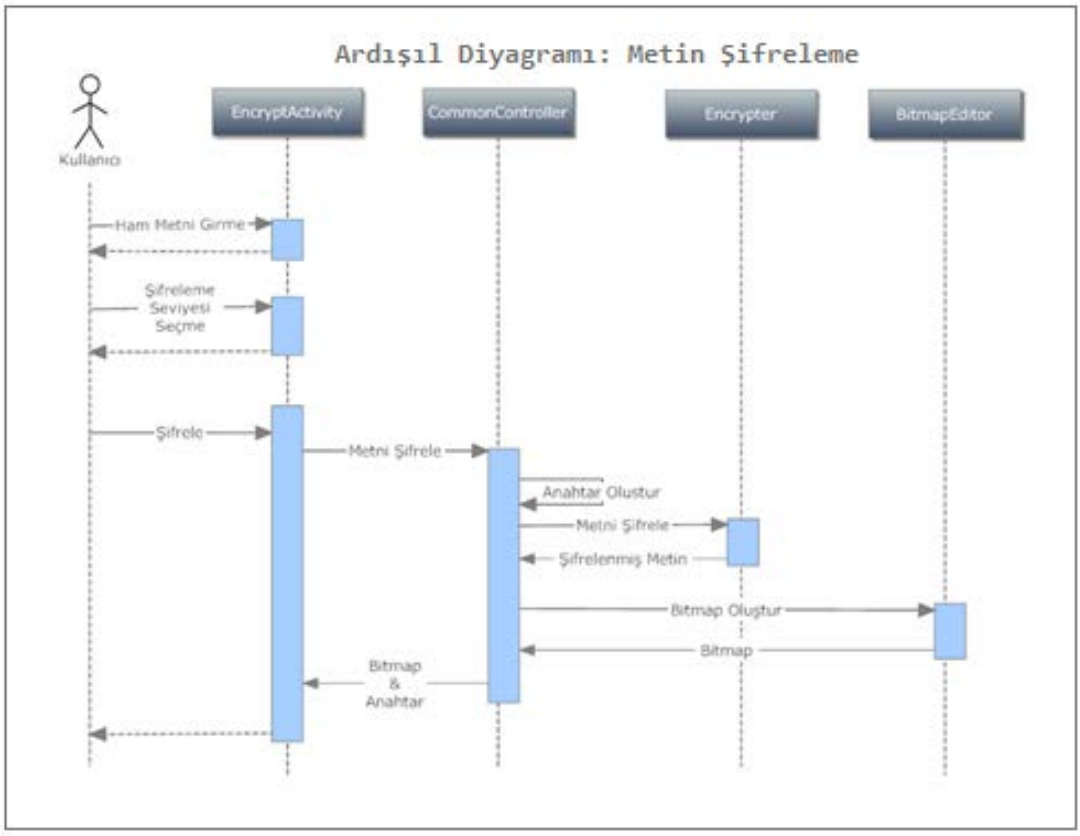


Şekil-25: Kullanım senaryoları

4.2.4 Ardışıl Diyagram

Metin Şifreleme

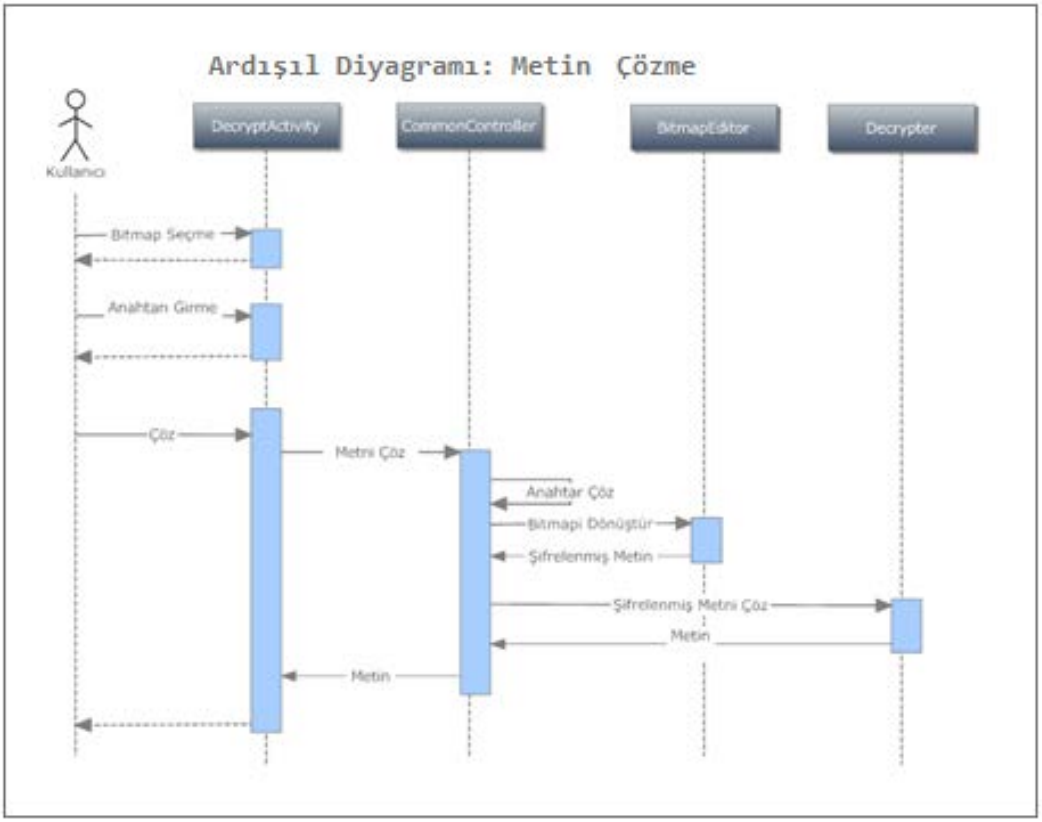
- Kullanıcı gelen arayüzden metin işleyicisine şifrelenmesinin istediği ham metni girecektir.
- Arayüzden şifreleme seviyesi seçebilecektir. Bu şifreleme seviyesinin "Yüksek", "Orta" ve "düşük" olmasına göre 12x12 matrisinden kaç tane kutucuğa ham metin karakteri girilmesine karar verecektir.
- "Encryp" tuşuna bastığında arka planda şifrelenecek ve şifrelenen metin yine arka planda *bitmap* resme döndürüldükten sonra anahtar ile birlikte kullanıcıya gösterilecektir.
- Aynı zamanda telefonun resimler dizinine kaydedilecektir.



Şekil-26: Ardışıl diyagramı

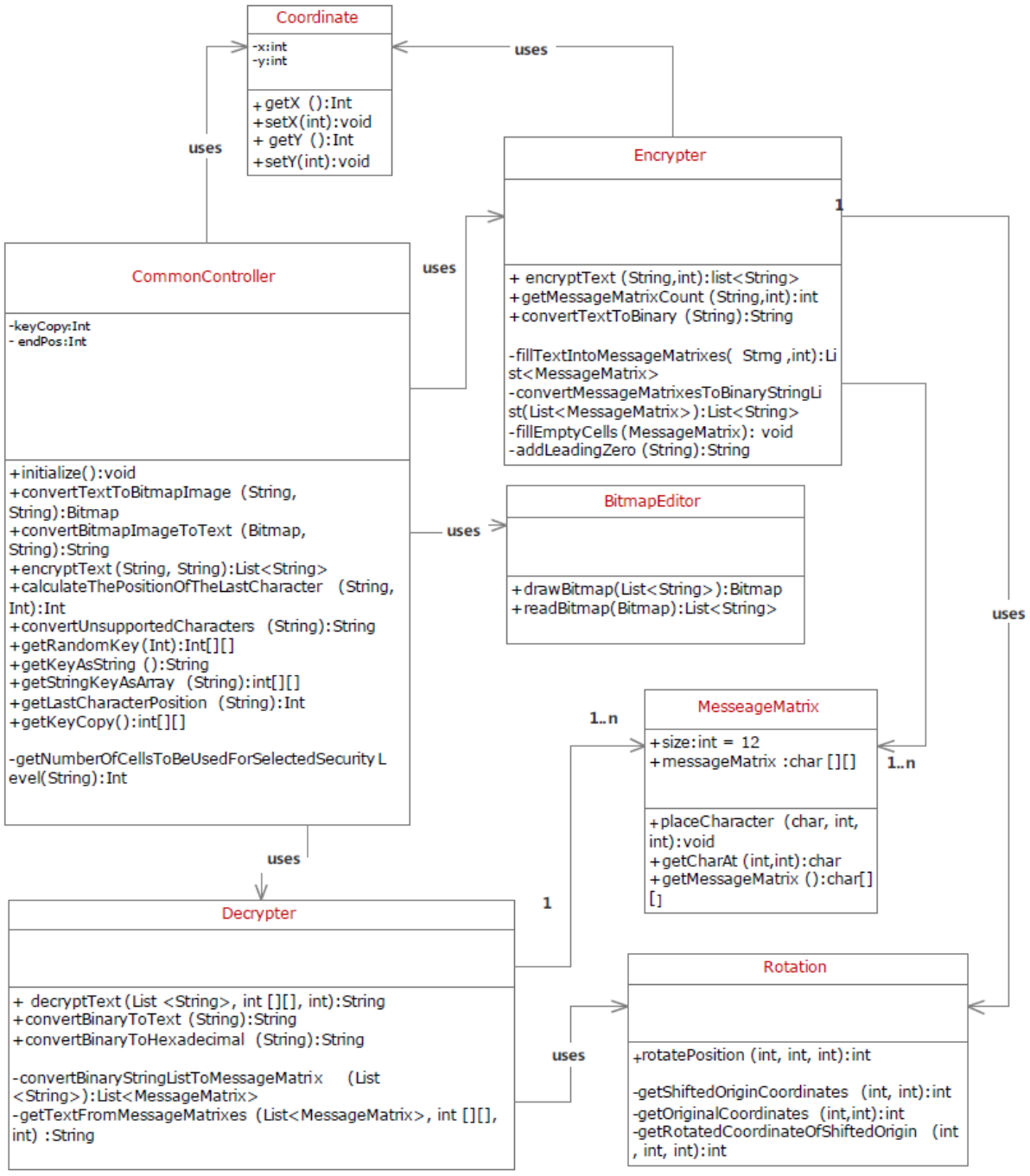
Şifre Çözme

- Kullanıcı kendisine "*whatsapp*" ya da *mms* olarak gelen *bitmap* resmi anahtar ile birlikte uygulamaya girecektir.
- Sonra "Decrypt" tuşuna basılacaktır ve şifre çözme işlemi başlatılacaktır.
- Önce anahtar çözülecektir.
- Bitmap resim matris haline çevrilecektir.
- Elde edilen matris anahtar ile anlatıldığı gibi çözülecektir.
- Çözülen metin yine tasarlanan bir metin görüntüleyici ile gösterilecektir.



Şekil-27: Ardışıl diyagramı

4.2.5 Sınıf Diyagramı



Şekil-28: Sınıf diyagramı

5 TASARIM, GERÇEKLEŞTİRME VE SINAMA

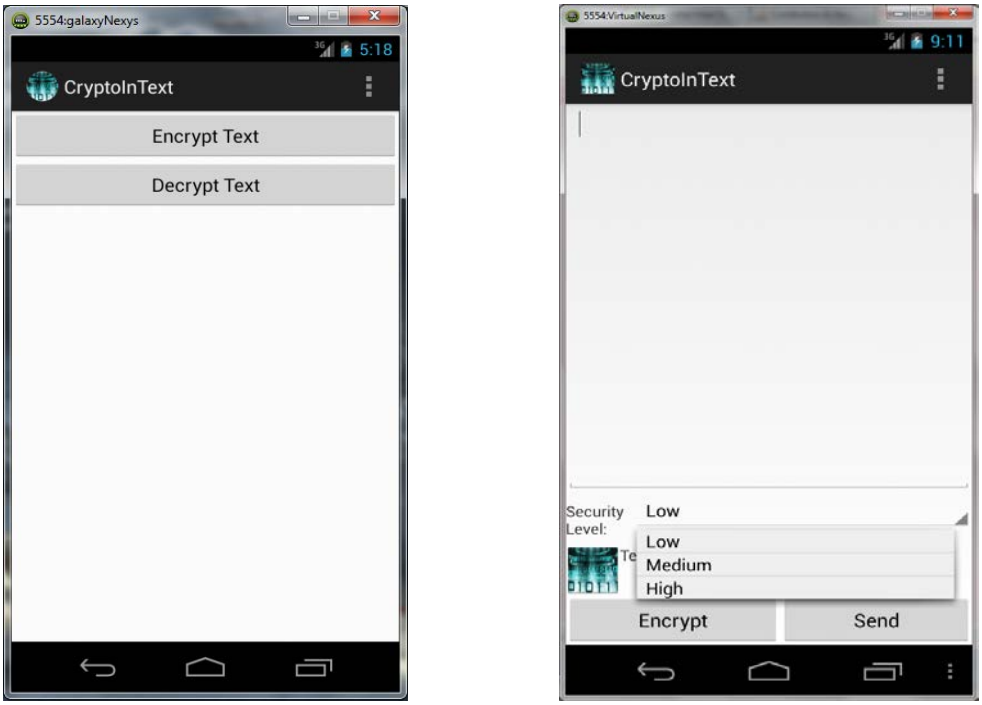
5.1 Gerçekleştirme

Geliştirilen şifreleme yöntemi tasarlanan yapı ile Android 4.2.1 de gerçekleştirilmiştir. Bir *activity* uygulaması olarak tasarlanmıştır.

5.2 Arayüz

Kullanıcının metni girebileceği bir alan bulunmaktadır. Ayrıca kullanıcı öncelikle bir şifreleme seviyesi seçtikten sonra da "Encrypt" tuşuna basarak şifreleme isteğini uygulamaya göndermiş olacaktır. Şeki-29'de arayüz verilmiştir

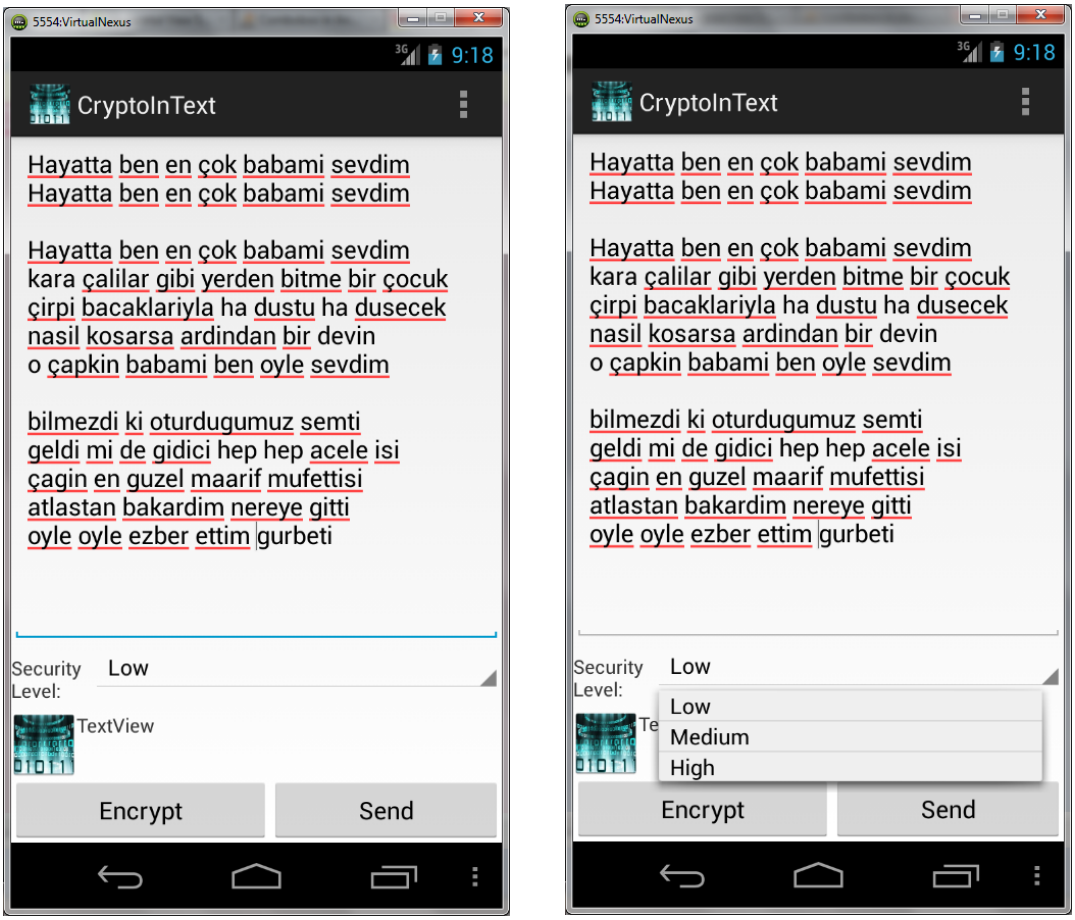
Kullanıcını belirlediği bir şifreleme seviyesi ile anahtarın uzunluğu da belirlenmiş olacaktır. Anahtar ne kadar kısa olursa o kadar zor şifreleme gerçekleştirilecektir. Şifreleme seviyesine göre 12x12 matristen 26, 18 ve 12 kutucuktan oluşan anahtar üretilecektir.



Şekil-29: Çoktan seçmeli yapı

İlk olarak ana ekranda yapmak istediğimiz işlem seçilmektedir.

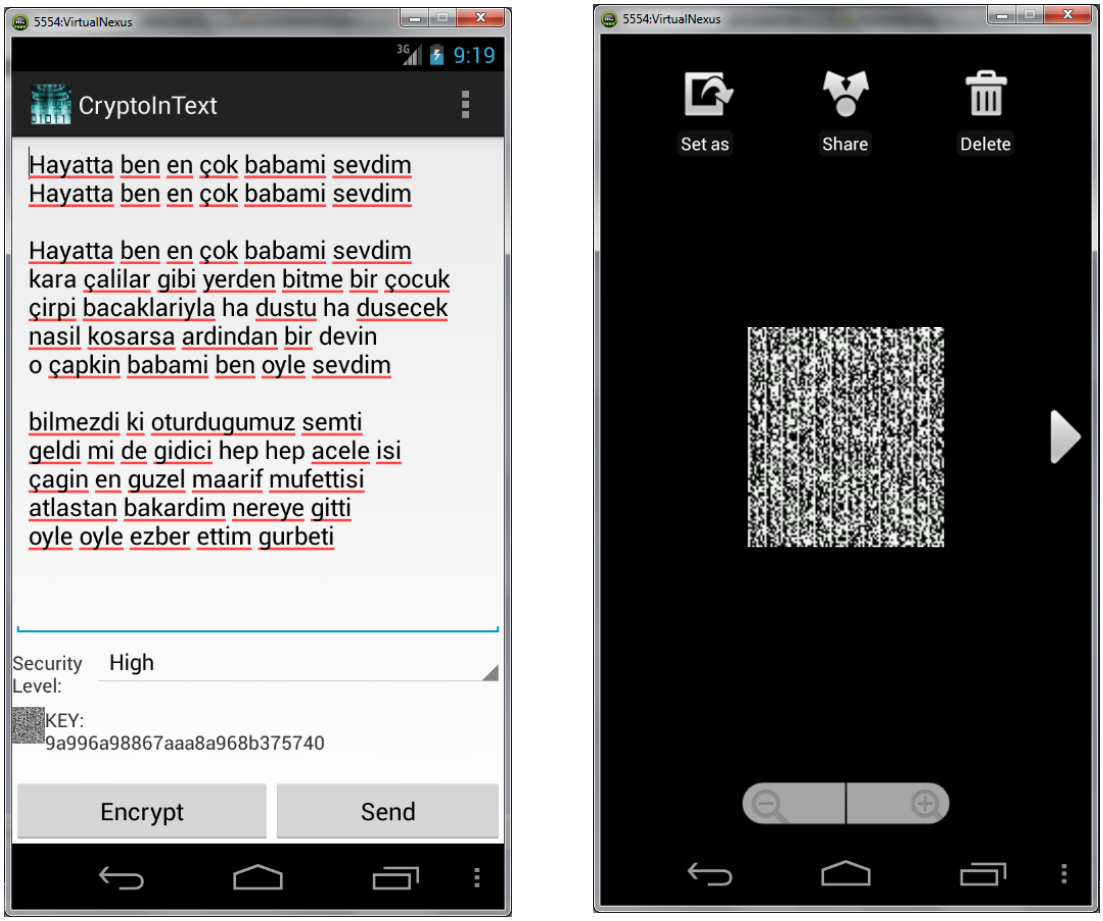
Şifrelenmesi istenen metine arayüzde daha fazla alan ayrılmıştır. Metin şekildeki gibi bir metin editöre girilmektedir.



Şekil-30: Metin yazılması

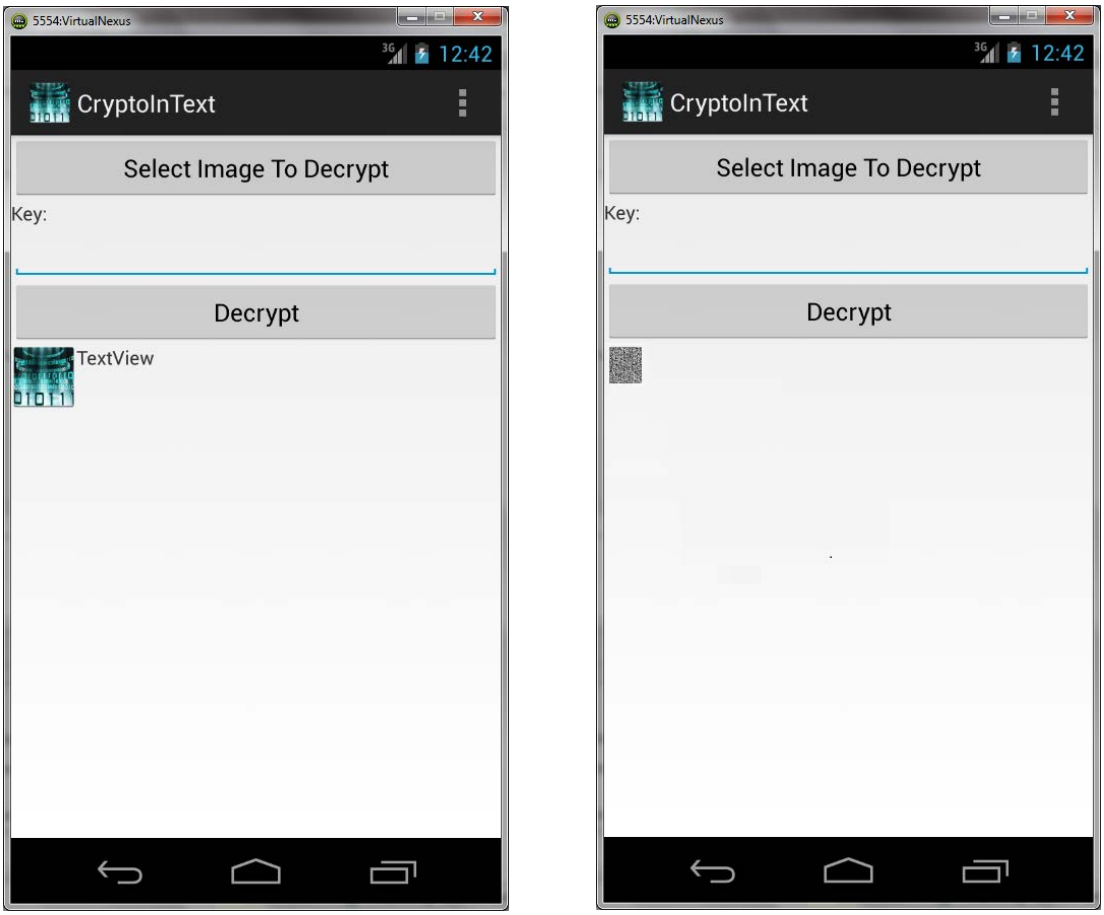
Şifrelenmesi istenen ham metin girildikten sonra, metin düzenleyici hemen alt kısmında yer alan birçok seçenekli "combo box" yapısı ile şifrelenmesi istenen seviye seçilmektedir.

Şifrelenmesi istenen metin girildikten sonra, şifreleme seviyesi girildikten sonra da **"Encrypt"** tuşuna basılarak metnin şifrelenmesi sağlanır. Şifrelenen metin *bitmap* resme dönüştürülür ve anahtar ile birlikte ekranın alt kısmına *bitmap* resim ve anahtar kullanıcıya gösterilecektir.



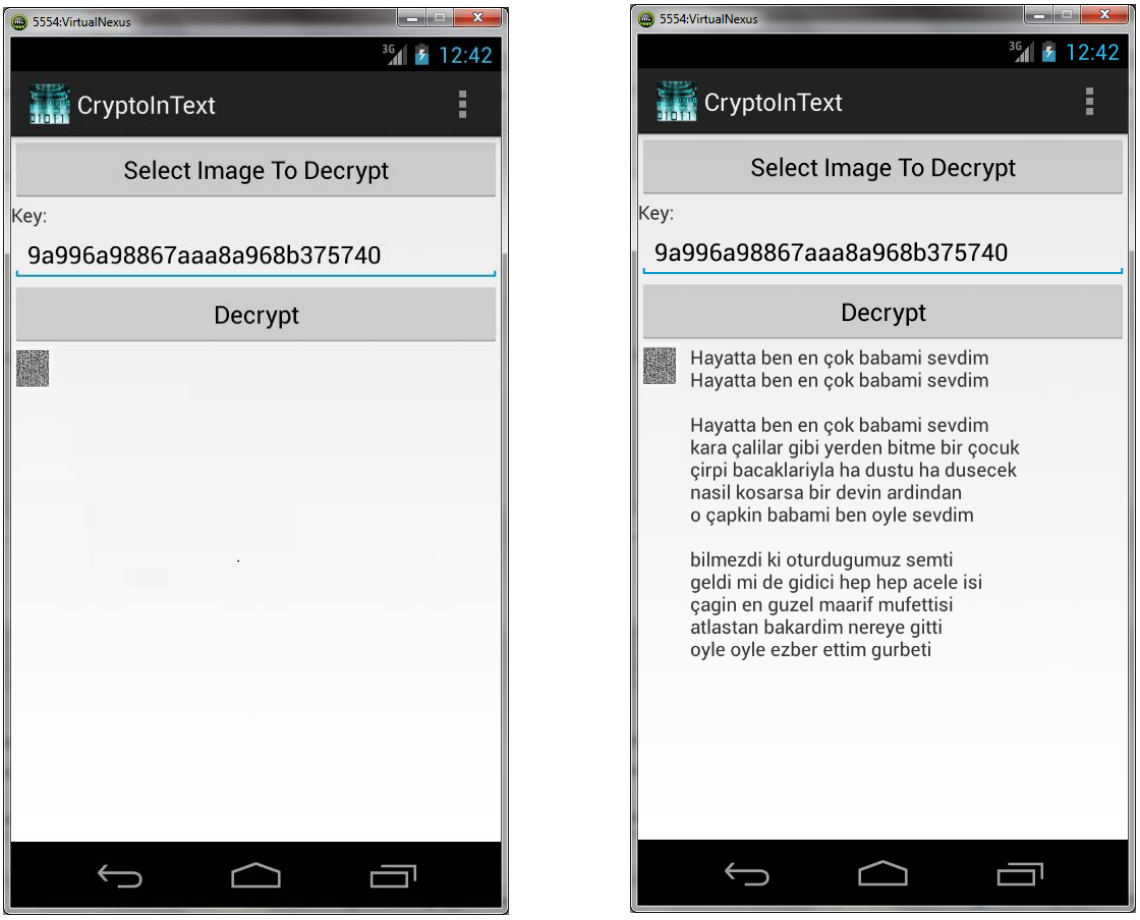
Şekil-31: Şifreleme sonrası

Gösterilen *bitmap* resim aynı zamanda "Galery" dizinine kaydedilecektir. Metin düzenleyici altında gösterilen *bitmap* resme tıklandığında "Galery" dizininden resim açılacaktır ve istenilen yol ile alıcıya gönderilecektir.



Şekil-32: Şifreleme seviyesinin belirlenmesi

Şifresin çözülmesi istenen *bitmap* resim "Select Image To Decrypt" tuşuna basılıp telefondaki mevcut resimlerden bir seçilir. Resim uygulama tarafından şifre çözülmeye uygun resim mi kontrol edilir. Seçilen resim Şekil-32' deki gibi kullanıcıya gösterilir. Bu aşamadan, şifre çözülmesinin gerçekleşebilmesi için kullanıcıdan, resimden farklı bir kanalla iletilen anahtar beklenmektedir.



Şekil-33: Şifrelenmiş resim

Şekil-33' deki gibi onaltılık tabandaki anahtar girildikten sonra, "*Decrypt*" tuşuna basılarak şifre çözülmesi başlatılır. Bu aşamada, "*bitmap*" resmin yanına çözülen metin yazılacaktır.

5.3 Sınama

Yazılımın sınama edilmesi kodun geliştirilmesiyle paralel olarak yürütülmüştür.

Yazılım aşamasında sınama için;

- Junit library kullanılmıştır. Birim testler yapılmıştır.
- Şifreleme aşamasında gerçekleştirilen matris için "rotate" yapısı 1 kere, 2 kere ve 3 kere yapılan döndürmeler için sınanmıştır.
- Aynı zaman da "**ConvertTextToBinary**" ve "**Encrytp**" ve "**Decrytp**"

Tasarımı gerçekleştirildikten sonra, metinler gönderilerek ve şifre çözümleri yapılarak bütünleştirme sınanması yapılmıştır.

5.3.1 Performans Sınaması

Yazılım Performansı

- Nesneler arası denetçi bulunmaktadır.[11]
- Sınıflar arası bağımlılık azdır
- Az bağımlı modüllerden oluşmaktadır.
- Methotlar ile yazılım karmaşıklığı azaltılmış, okunabilirlik artırılmıştır.

6 DENEYSEL SONUÇLAR

Şifreleme aşamalarında “ş”, “ı”, “ğ” ve “I” harfleri ASCII kodları 8 bite sığmadığı için desteklenmemektedir. Onun yerine “s”, “i”, “g” ve “i” harfleri kullanılmaktadır.

Anahtar şifresi ne kadar kısa ise şifre o kadar karışık ve çözülmesi zor olmaktadır.

Anahtarın her şifrelemede değişiyor olması ile anahtarın kullanım süresi azaltılmış ve bu sayede şifrenin çözülmesi için önemli bir zaman kısıtlaması getirilmiştir.

Kaba kuvvet yöntemi ile şifre anahtarı çözülmek istenirse; 3 septilyondan daha fazla anahtar denemesi yapılmak istenmektedir ki; bu büyük bir rakamdır.

Şifrelenen metnin direkt gönderilmesi yerine; resim olarak gönderilmesi tercih edilmiştir. 3. Kişiler tarafından anlamsız bir resim formatı ile kafa karıştırma yoluna gidilmiştir.

Şifreleme algoritmasının donanımda ve yazılımda hızlı olması, daha kolay uygulanabilir olması ve çok fazla hafızaya gerek duymaması olumlu yönleri olarak söylenebilir.

7 SONUÇ ve ÖNERİLER

Hızlı çalışan ve başarılı bir şifreleme yöntemidir.

Şifreleme yöntemi çok karışık düzeyde olmamakla birlikte, askeri ve siyasi amaçlarla kullanılması önerilmeyen bir şifreleme tekniğidir.

Proje sonucunda şifreleme yöntemleri hakkında bilgi edinilmiş, şifreleme yöntemi analizi öğrenilmiş ve Android işletim sistemi için *activity* uygulaması geliştirilmesi öğrenilmiştir.

Proje ilerletilmek istenirse; oluşturulan resim için görüntü şifreleme yöntemleri de uygulanabilir. Hatta akıllı telefonlardaki gelişmiş teknoloji ile, resime görsel kriptografi uygulanabilir ve bu amaç ile oluşturulan iki farklı resmin üstüste getirilmesinde, bir resim telefona bir kanaldan gönderilir iken resmin diğer parçası kamera ile işlenebilir.

Arayüz iyileştirilerek kullanıcılara daha çok hitap eden hale getirilebilir.

8 KAYNAKLAR

[1] J. Robert Buchanan , "An Introduction to Cryptography, Spotlight on Science", http://banach.millersville.edu/~BobBuchanan/presentations/Spotlight.pdf, 2008

[2] B. Schneier, *Applied Cryptography*, John Wiley & Sons, Inc., 1996.

[3] Mike Knee, "The Basic of Cryptography", *http://www.snellgroup.com/documents/white-papers/white-paper-Good-Old-Mathematics.pdf ,2008.*

[4] The components of the Enigma machine, http://www.codesandciphers.org.uk/enigma/enigma2.htm

[5] İTÜ/BİDB, "Şifreleme Yöntemleri", http://www.bidb.itu.edu.tr/?d=1002, 2009.

[6] Sourav Mukhopadhyay,http://www.facweb.iitkgp.ernet.in/~sourav/DES.pdf

[7] Android Development with Eclipse – Tutorial http://www.eclipse.org/resources/resource.php?id=516, 2012.

[8] An Adroid Developers, http://developer.android.com/index.html, 2012.

[9] R. L. Schaffer, M. Mulekar and J. T. Mcclave, *Probability and Statistics for Engineers*, 2010, pp. 170-172.

[10] WolframAlpha Computational Knowledge Engine, http://www.wolframalpha.com/ , 2012.

[11] Feza Buzluca, "Lecture Notes of Object Oriented Modelling and Design", http://ninova.itu.edu.tr/tr/dersler/bilgisayar-bilisim-fakultesi/2097/blg-468e/ekkaynaklar?g197952, 2012.