# MOBİL PLATFORMADA AZKRİPT LAYİHƏSİNİN REALLAŞDIRILMASI

*1.Mirməhəmməd MANSUROV, 2.Murad ŞƏFİYEV, 3.Orxan ƏKBƏRZADƏ*

İnformasiya Təhlükəsizliyi Fakültəsi
Dövlət Gömrük Komitəsinin Akademiyası

**Xülasə**

**Layihəni inkişaf etdirərkən Java proqramlaşdırma dili, Java-da kriptoqrafik alqoritmlər və Firebase ilə bağlı araşdırmalar aparılmışdır. Layihədə istifadəçilər ilk öncə qeydiyyatdan keçir və daha sonra giriş edirlər. Əgər giriş uğurlu alınarsa, o zaman istifadəçilər interfeysdə yerləşdirilmiş kriptoqrafik alqoritmlərdən istifadə edərək şifrələmə və deşifrələmə prosesini həyata keçirə bilərlər. İstifadəçi istədiyi mətni və ya şifrələnmiş mətni daxil edərək, onu uyğun olaraq şifrələyə və ya deşifrələyə bilər.**

## 1. Giriş

Mobil platformada müxtəlif şifrələmələrdən istifadə edən tətbiq inkişaf etdirilərək həm Java proqramlaşdırma, kriptoqrafik alqoritmlər və Firebase ilə bağlı araşdırmalar aparılmış və işlər görülmüşdür, həm də Java-da kriptoqrafik alqoritmlərin və Firebase-in necə işlədiyi barəsində təcrübə qazanılmışdır. İstifadəçi interfeysə daxil olduğu zaman ilk öncə qeydiyyatdan keçir, sonra giriş edir. Bundan sonra istifadəçinin qarşısına MD5, ROT13, Sezar, Base64 və Tərs alqorimtlər çıxır, Bu alqorimtlər hər biri fərqli şifrləməni yerinə yetirir. İstifadəçi istədiyi birini seçib, mətni şifrələyə və ya şifrələnmiş mətni deşifrələyə bilər. İstifadəçi şifrləmə və ya deşifrələmə butonuna kliklədikdən sonra cavab uyğun hissədə və Textview widget`də göstərilir.

## 2. Təməl Biliklər

**Java proqramlaşdırma dili**
Java açıq mənbəli, obyekt yönümlü, yerdən müstəqil, yüksək effektiv, çoxfunksiyalı, yüksək səviyyəli, addım-addım strukturlaşdırılmış dildir, Sun Microsystems-in mühəndisi James Gosling tərəfindən hazırlanmışdır.

Java-da proqram birbaşa başa düşülən koda çevrilmir. O, JVM (Java Virtual Maşın) tərəfindən şərh edilən bayt koduna (.class faylı) çevrilir. Bu səbəbdən, tərtib edildikdə, hər yerdə işlədilə bilən bir bayt kodu faylı yaradır. Bir dəfə yazın və istədiyiniz yerə qaçın təbiətini buradan alır.

Android / İOS üçün mobil proqramlar inkişaf etdirə bilərsiniz, veb saytlarda istifadə edə bilərsiniz, masaüstü proqramlar hazırlaya bilərsiniz, oyunlar inkişaf etdirə bilərsiniz.

**Firebase**
Firebase bir xidmət kimi arxa tərəfdir. (Baas). O, tərtibatçılara keyfiyyətli proqramlar hazırlamağa, istifadəçi bazalarını böyütməyə və qazanc əldə etməyə kömək etmək üçün müxtəlif alətlər və xidmətlər təqdim edir. O, Google infrastrukturu üzərində qurulub. Firebase, məlumatları JSON kimi sənədlərdə saxlayan NoSQL verilənlər bazası proqramı kimi təsnif edilir. Bəzi əsas xüsusiyyətləri mövcuddur:
1. Doğrulama
2. Real vaxt verilənlər bazası
3. Hostinq
4. Sınaq laboratoriyası
5. Bildirişlər

**Android Studio**

Android Studio, Google tərəfindən 16 may 2013-cü ildə Google I/O tədbirində təqdim edilmiş rəsmi İnteqrasiya edilmiş İnkişaf Mühiti (IDE) kimi tanınır və o vaxtdan Android proqramlarının hazırlanmasında istifadə olunur. Bütün növ Android cihazlarında işləyir. O, yüksək keyfiyyətli, səmərəli nəticələrlə tətbiqləri inkişaf etdirmək üçün ən sürətli alətləri təqdim edir.

Android Studio IntelliJ IDEA-a əsaslanır və xüsusi olaraq Android proqramlarının hazırlanması üçün nəzərdə tutulub. Android Studio istifadəçilərin proqramların hazırlanması üçün ehtiyaclarını ödəyə bilən bir çox funksiyaları, o cümlədən ağıllı kod redaktoru və sazlayıcı, performans təhlili alətləri, emulyatorlar və daha çoxunu ehtiva edir.

## 3. İnkişaf etdirilən struktur

### 3.1. İstifadə olunan alqorimtlərin və funksiyaların qısa açıqlamaları

MD5 - MD5 (Message-Digest algorithm 5) – Verilənlərin tamlığını yoxlamaq üçün istifadə olunan alqoritmdir. Tək istiqamətli şifrləmə alqoritmidir. Daxil edilən verilənlərin ölçüsündən asılı olmayaraq onları 128 bitlik hexadecimal simvollara çevirir. MD5-dəki hər bir verilənin eyni olması mümkün deyildir, çünki generasiya edilən yekun verilən nəticədə 128 bitlik informasiyadır. Mobil platformada MD5 alqoritminin java-da hazır "md5" kitabxanası istifadə edilmişdir.

ROT13 - ROT13 hərfi əlifbada özündən sonra 13-cü hərflə əvəz edən sadə hərf əvəzetmə şifrəsidir. ROT13 qədim Romada işlənib hazırlanmış Sezar şifrəsinin xüsusi halıdır. Əsas Latın əlifbasında 26 hərf (2×13) olduğundan, ROT13 öz tərsidir, yəni ROT13-ü ləğv etmək üçün eyni alqoritm tətbiq edilir, buna görə də eyni hərəkət kodlaşdırma və dekodlaşdırma üçün istifadə edilə bilər. Veb platformasında ROT13 alqoritminin java kodunda uyğun əlifbaların çevrilməsi funksiyasından istifadə edilmişdir.

Sezar - Sezar şifrəsi dünyada ən qədim bəlli olan şifrələrdən biridir. Sezar şifrəsini yerini dəyişmə (əvəz etmə) şifrə kimi təsnif etmək olur. Şifrənin mükəmməlləşdirilmiş formasına Vijiner şifrəsi deyilir. Müasir kriptoqrafiyada Sezar şifrəsi dözümsüz kimi sayılır. Mobil platformada Sezar alqoritminin javascript kodunda "charsMap", "currentChar" və "charIndex" funksiyalarından istifadə edilmişdir.

Base64 - Base64 ikili məlumatların yalnız ASCII simvollarından istifadə edən mühitlərdə ötürülməsinə və saxlanmasına imkan verən kodlaşdırma sxemidir. Kodlaşdırma zamanı 3 baytlıq məlumat 6 bitlik dördlü qruplara paylanır. Hər 6 bitlik qrup 0 ilə 63 arasında bir ədəd yaradır (26=64). Hər bir nömrə uyğun olaraq ASCII çap simvoluna çevrilir. Veb platformasında Base64 alqoritminin java kodunda "atob" və "btoa" funksiyalarından istifadə edilmişdir.

Əks - Əks şifrə mesajı tərs qaydada çap edərək şifrələyir. Şifrəni açmaq üçün orijinal mesajı əldə etmək üçün sadəcə tərsinə çevrilmiş mesajı geri qaytarırsınız. Şifrələmə və deşifrləmə addımları eynidir. Mobil platformada Əks şifrə alqoritminin java kodunda "split" (simvolları əksinə çevirmə funksiyası) funksiyasından istifadə edilmişdir.

### 3.2. Qarşıya çıxan problemlər və həlləri

**Problem:** Mobil platformada alqoritmlərin java-da yazılmış kodlarının implementasiyası/ tətbiqi.
**Həll:** Mobil platformada java kodlarının necə işlədiyini aradırmaq. Alqoritmlərin java kodlarını tapmaq və kodlaşdırmağa başlamaq.

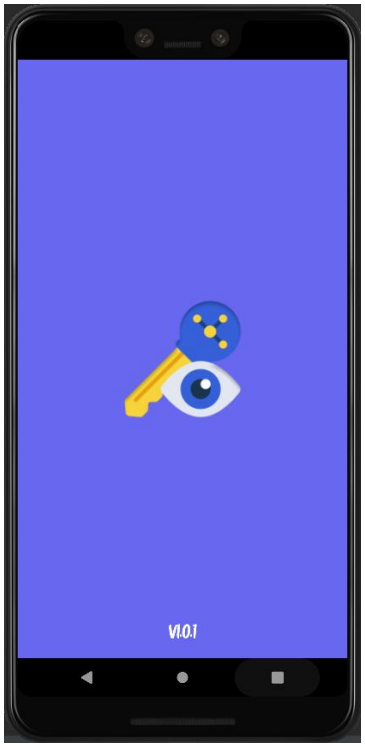
**Problem:** Mobil platformada girişin və qeydiyyatın aparılması.
**Həll:** "Log In" və "Register" funksiyalarının necə işlədiyini araşdırmaq və Firebase-də hesab açmaq. Verilən Firebase-in verdiyi API-ni tətbiqə bağlamaq və kodlaşdırmağa başlamaq.

### 3.3. İnterfeysin yaradılması üçün sərf olunan vaxt (şəxs və saat əsasında)

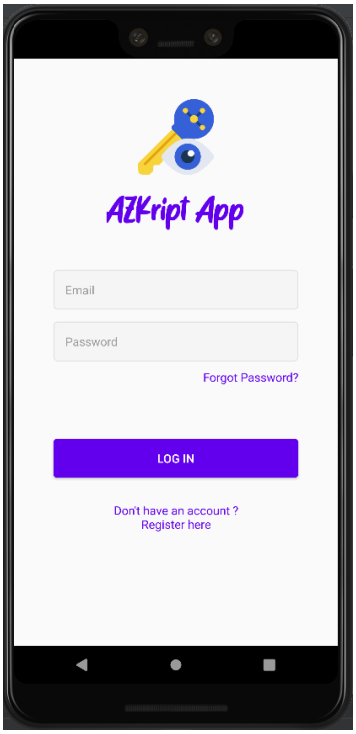
- Mirməhəmməd Mansurov: 4 gün, gün ərzində 1-2 saat
- Murad Şəfiyev: 12 gün, gün ərzində 1-2 saat
- Orxan Əkbərzadə: 4 gün, gün ərzində 1-2 saat

## 4. İstifadəçi İnterfeysi

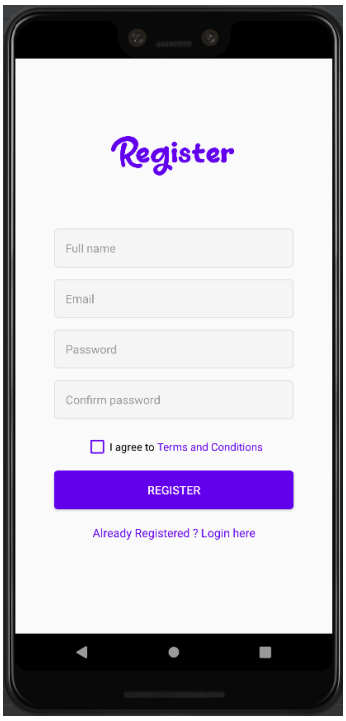
Tətbiq ilk işə düşdükdə tətbiq loqosu və versiyası əks olunan bir “SplashScreen” ekrana gəlir.




Ardınca istifadəçinin qarşısına çıxan login page səhifəsi. Burada "Log In", "Register" və "Forgot Password" bölümləri mövcuddur.

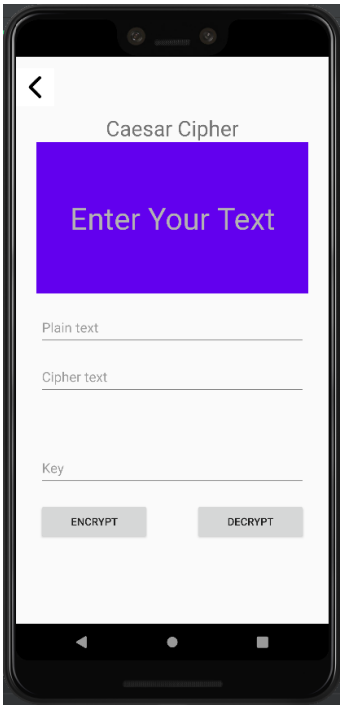



Növbəti görüntüdə isə istifadəçi qeydiyyatının aparıldığı səhifə göstərilib.

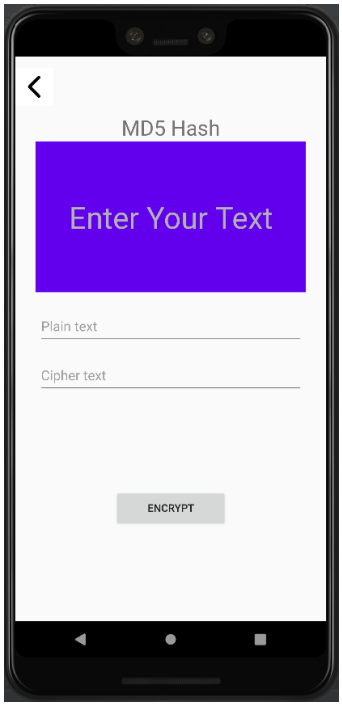


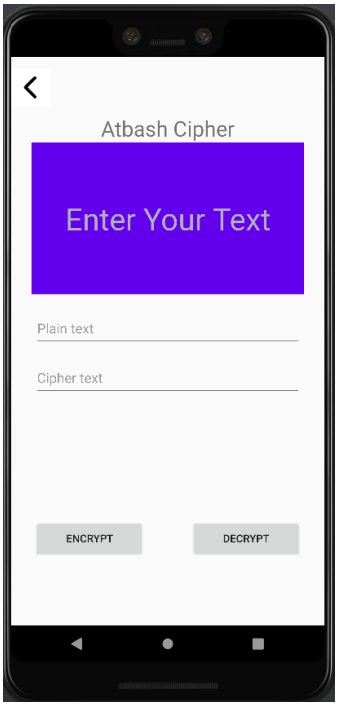

İstifadəçi qeydiyyatdan keçib hesaba daxil olduqdan sonra “Dashboard” əsas menyusuna yönləndirilir. Burada onun istifadə edə biləcəyi bir neçə şifrələmə alqoritmi mövcuddur.

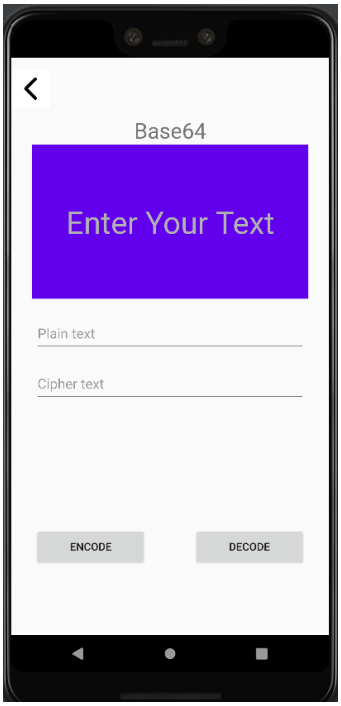
İstifadəçi Caesar bölümünə keçdikdən sonra bu səhifə açılacaq. İstifadəçi istədiyi mətni və açarı daxil edərək "ENCRYPT" butonuna klikləyir və onu Sezar alqoritmi ilə şifrələyir. Nəticə isə uyğun hissədə və Textview widget`də göstərilir.

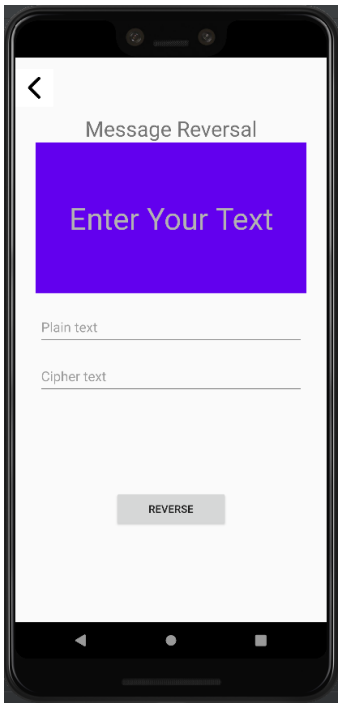



İstifadəçi MD5 bölümünə keçdikdən sonra bu səhifə açılacaq. İstifadəçi istədiyi mətni daxil edərək "encoder" butonuna klikləyir və onu MD5 alqoritmi ilə şifrələyir.

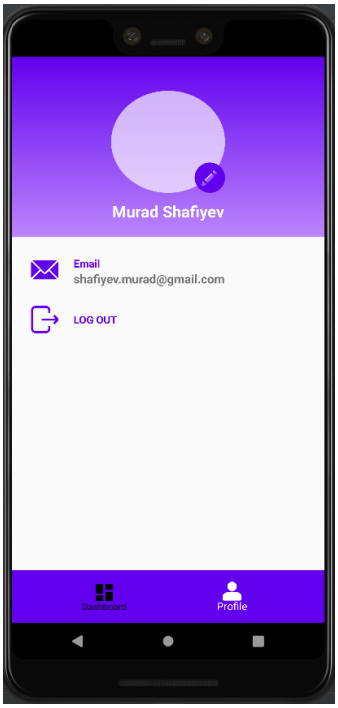



Tətbiqdə həmçinin istifadəçi adının, e-mail adresinin və "Log Out" butonunun olduğu "profil" hissəsi də vardır. İstifadəçi adı və e-mail adresləri Firebase`də depolanır. Növbəti görüntü həmin bu səhifəni təsvir edir.




## 5. Nəticələr

Nəticədə mobil platformada istifadə olunan proqramlaşdırma dilləri, texnologiyaları və kriptoqrafik alqorimtlər haqqında edilən araşdırmalar əsasında yeni biliklər qazanıldı. Firebase ilə mobil platformanın necə əlaqəli şəkildə işlədiyi və istifadəçi məlumatlarının bulud (cloud) mühitində necə saxlandığı öyrənildi. Bu layihədə arzu olunan nəticə əldə olunmuşdur.

## 6. İstinadlar

[1] https://www.w3schools.com/
[2] https://stackoverflow.com/
[3] https://www.tutorialspoint.com/index.htm
[4] https://github.com/
[5] https://codereview.stackexchange.com/
[6] https://www.youtube.com/c/SmallAcademy