**Şifrələmə və Deşifrələmə Layihəsi**

*Məmmədova Aysu*

**İnformasiya Təhlükəsizliyi**

**Azərbaycan Texniki Universiteti**

**Xülasə**

Layihəni yazmazdan əvvəl ilk olaraq c# ilə access bağlantısı araşdırılıb. Daha sonra şifrələmə üsüllarını, tətbiq olunma yolları araşdırılmışdır. Layihədə 6 fərqli form yaradılmışdır. Birinci qeydiyyat, ikinci formda giriş üçncü formda düz mətnin tərsinə çevirmə formatı,dördüncü formda ceaser şifrələmə və deşifrələmə, beçinci formda base64 şifrələmə və deşifrələmə altıncı formda isə düz mətnin md5 formatı göstərilmişdir.

**1.Giriş**

Layihə üzərində çalışarkən şifrələmə və deşifrələmə üsullarını araşdıraraq, üzərində işləyərək təcrübə yığılmışdır. İlk öncə qediyyat formu yaradılmışdır. Ad və şifrə yazaraq giriş edildikdə düz yazılmazsa mesaj qutusu ilə xəta verdiyi vurğulanacaq. Əgər ad və şifrə düz yazılarsa ikinci form açılacaq və ilk şifrələmə üsulu qarşımıza çıxacaq. Beləliklə növbəli şəkildə şifrələmə üsüllarını tətbiq edirik.

**2.Təməl Biliklər**

**MD5**

MD5 (Message-Digest algorithm 5) – Verilənlərin tamlığını yoxlamaq üçün istifadə olunan alqoritm. 1991-ci ildə Massaçusets Texnologiya İnstitutunda Ron Rivest tərəfindən yaradılmışdır. 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. MD5 şifrlərinin qırılması nəzəri olaraq qeyri mümkündür. Ancaq bəzi MD5 Verilənlər Bazaları ilə bruteforce üsulu ilə 16 simvola qədər olan şifrlər qırıla bilir. Bu cür sistemlər daxil edilən MD5 şifrini öz bazasında əvvəlcədən daxil MD5-lər içərisində axtarır. Amma şifr nə qədər mürəkkəb və uzun olarsa onun qırılmasıda bir o qədər çətinləşir.

**BASE64**

Proqramlaşdırmada Base64 ikili verilənləri (daha dəqiq desək, 8 bitlik bayt ardıcıllığı) məlumatları radix-64 təsvirinə çevirməklə ASCII sətir formatında təmsil edən ikili-mətnə ​​kodlaşdırma sxemləri qrupudur. Base64 termini xüsusi MIME məzmun ötürmə kodlaşdırmasından yaranır. Hər bir yekun olmayan Base64 rəqəmi tam olaraq 6 bit məlumatı təmsil edir. Beləliklə, üç bayt (yəni, cəmi 24 bit) dörd 6 bitlik Base64 rəqəmi ilə təmsil oluna bilər.

Bütün ikili-mətnə ​​kodlaşdırma sxemləri üçün ümumi olan Base64 ikili formatlarda saxlanılan məlumatları yalnız mətn məzmununu etibarlı şəkildə dəstəkləyən kanallar arasında daşımaq üçün nəzərdə tutulmuşdur. Base64 xüsusilə Ümumdünya Şəbəkəsində geniş yayılmışdır, burada onun istifadələrindən biri HTML və CSS faylları kimi mətn aktivlərinin içərisinə şəkil faylları və ya digər ikili aktivləri yerləşdirmək imkanıdır.

Base64 elektron poçt əlavələrini göndərmək üçün də geniş istifadə olunur. Bu tələb olunur, çünki SMTP – öz orijinal formasında – yalnız 7 bitlik ASCII simvollarını daşımaq üçün nəzərdə tutulmuşdur. Bu kodlaşdırma 33-36% əlavə yükə səbəb olur (kodlaşdırmanın özü ilə 33%; daxil edilmiş sətir fasilələri ilə 3%-ə qədər daha çox).

**Ceaser**

Dünyada ən qədim bəlli olan şifrələrdən biridir. Məşhur Roma sərkərdəsi Yuli Sezar öz yazışmalarında indi onun adını daşıyan şifrdən istifadə edirdi. Adi latın əlifba yazılırdı, sonra onun altında həmin əlifba, lakin sola hərf dövri sürüşmə ilə yazılırdı. Sezar şifrəsini yerini dəişmə (əvəz etmə) şifrə kimi təsnif etmək olur. Şifrənin mükəmməlləşdirilmiş formasına Vijiner şifrəsi deyilir. Müasir kriptoqrafiyada Sezar şifrəsi dözümsüz kimi sayılır.

**Reverse**

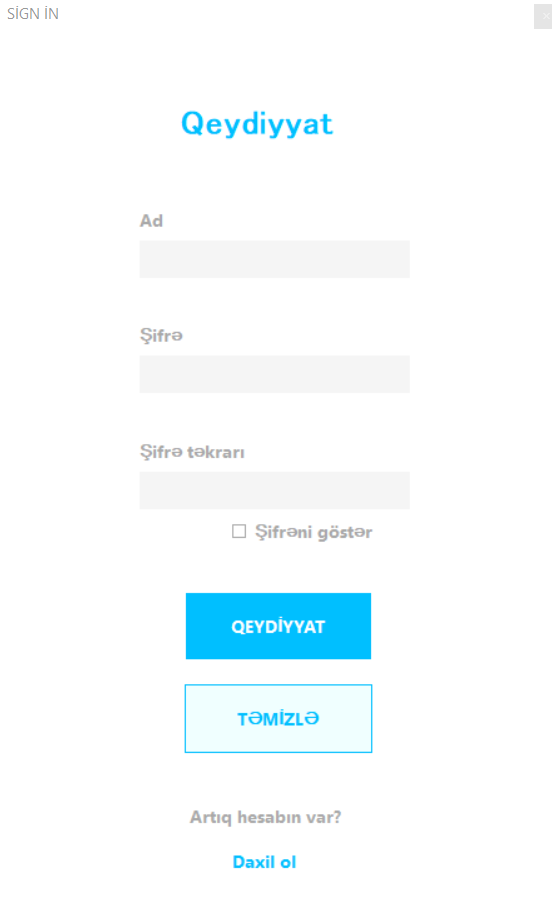
Reverse Cipher, şifrə mətni kimi çevirmək üçün düz mətn sətirini tərsinə çevirmək nümunəsindən istifadə edir.Şifrələmə və şifrənin açılması prosesi eynidır.Şifrə mətninin şifrəsini açmaq üçün istifadəçi sadə mətni əldə etmək üçün sadəcə olaraq şifrə mətnini tərsinə çevirməlidir.

**4.Qarşılaşılan problemlər və həll yolları**

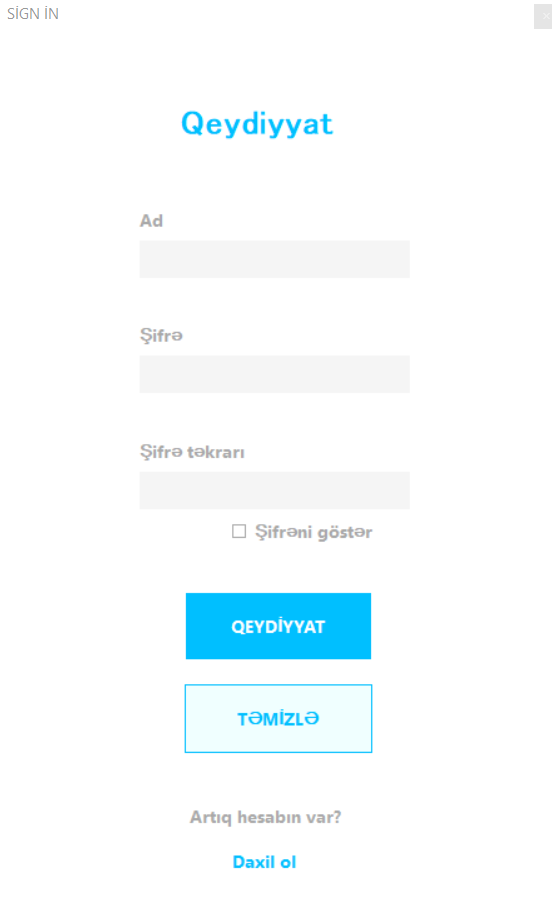
**Problem:** C# ilə access arasındakı bağlantının yaranması

**Həlli:** String connection ilə app.config eyni olmalıdır

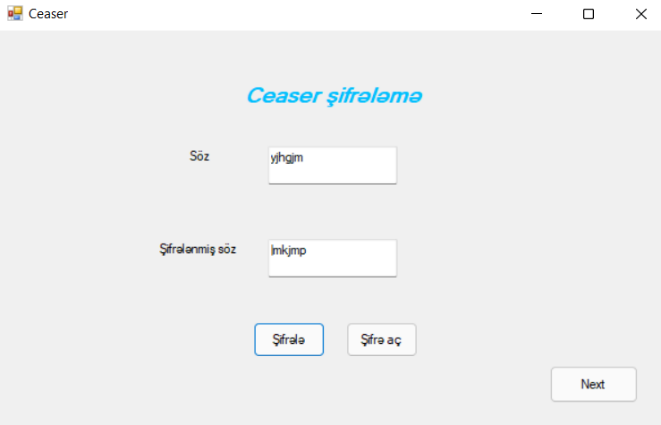
**5.İstifadəçi katalogu**



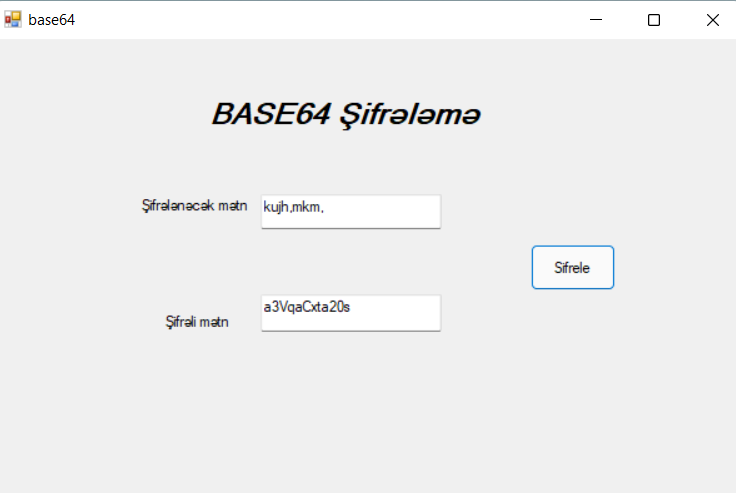
Layihə açıldığında qarşımıza ilk çıxan qeydiyyat formudur. Burada adımızı və şifrəmizi qeyd etmekle qeydiyyatdan keçirik.



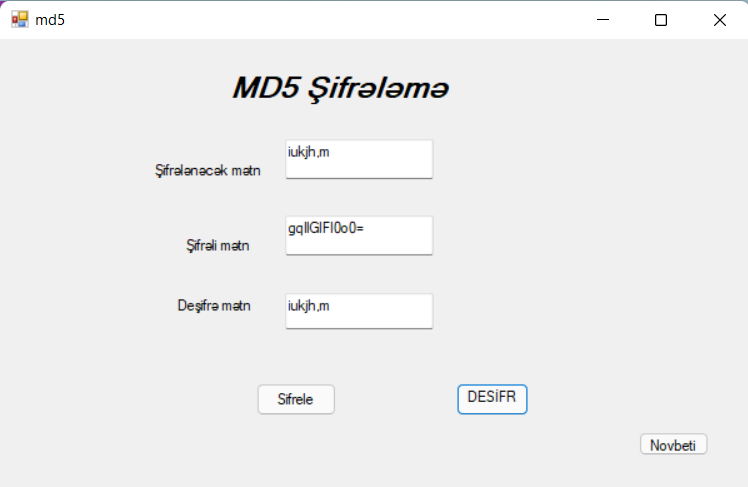
Daha sonra giriş formuna daxil oluruqşGiriş etdikdən sonra əgər ad və şifrə düz yazılmışsa üçüncü form açılacaqdır. Burada tərsinə şifrələmə əməliyyatını etdikdən sonra növbəti buttona klikləyərək digər şifrələmə üsuluna keçid ediləcəkdir.



Burada SEZAR şifrələmə və deşifrələmə üsulu edilir. Sonra növbəti buttona klikləyərək digər şifrələmə üsuluna keçid ediləcəkdir.



BASE64 şifrələmə üsulunda verilən sözün şifrələnməsi və şifrələnmiş sözün açılması göstərilmişdir.



Burada MD5 şifrələmə və deşifrələmə üsulu göstərilmişdir.

**6.Ədəbiyyat**

**1.** [**https://az.wikipedia.org/wiki/MD5**](https://az.wikipedia.org/wiki/MD5)

**2.** [**https://az.wikipedia.org/wiki/Sezar\_%C5%9Fifr%C9%99si**](https://az.wikipedia.org/wiki/Sezar_%C5%9Fifr%C9%99si)

**3.https://www.tutorialspoint.com/cryptography\_with\_python/cryptography\_with\_python\_reverse\_cipher.htm**

**4.** [**https://az.wikipedia.org/wiki/MD5**](https://az.wikipedia.org/wiki/MD5)

**7.Sonluq**

Son olaraq şifrələmə üsullarını, tətbiq olunma yollarını, kodları araşdırıraraq və üzərində işləyərək yeni biliklər öyrənildi və təcrübə olundu.