Kullanıcı Kayıt ve Giriş Sistemi

Uyguluma 8 sınıftan oluşmaktadır;

MainActivity	:Giriş yapılarak erişilmek istenen boş aktivite sınıfı.
RegisterActivity	:Kullanıcı kayıt işlemini yaptığı sınıf.
LoginActivity:	:Kullanıcıların giriş işlemini yaptığı sınıf.
User	:Kullanıcı parametrelerini tutulduğunu sınıf.
UserRules	:Kullanıcı kayıt ve giriş işlemleri için koyulmuş kurallar.
Encode	:Kullanılan veritabanına uyum kullanılan karakter değiştirici.
MyHash	:Hash işleminin yapıldığı sınıf.
ConvertBlocks192	:Hash işlemi için string ifadenin byte değer dizilerini oluşturan sınıf.

Uygulama Android projesi olarak mobil platforma göre hazırlandı. Kısaca özetlemek gerekir ise; belirli kurallar çerçevesinde kullanıcıların kayit olduğu ve giriş yaptığı bir sistem. Veri tabanı olarak Google'ın firebase teknolojisi kullanıldı. Üye kayıt sistemi için daha kullanışlı olmasına rağmen hash fonksiyonlarını kendi kullandığı için Authentication türü veritabı tercih edilmedi. Bunun yerine Realtime Database tercih edildi.

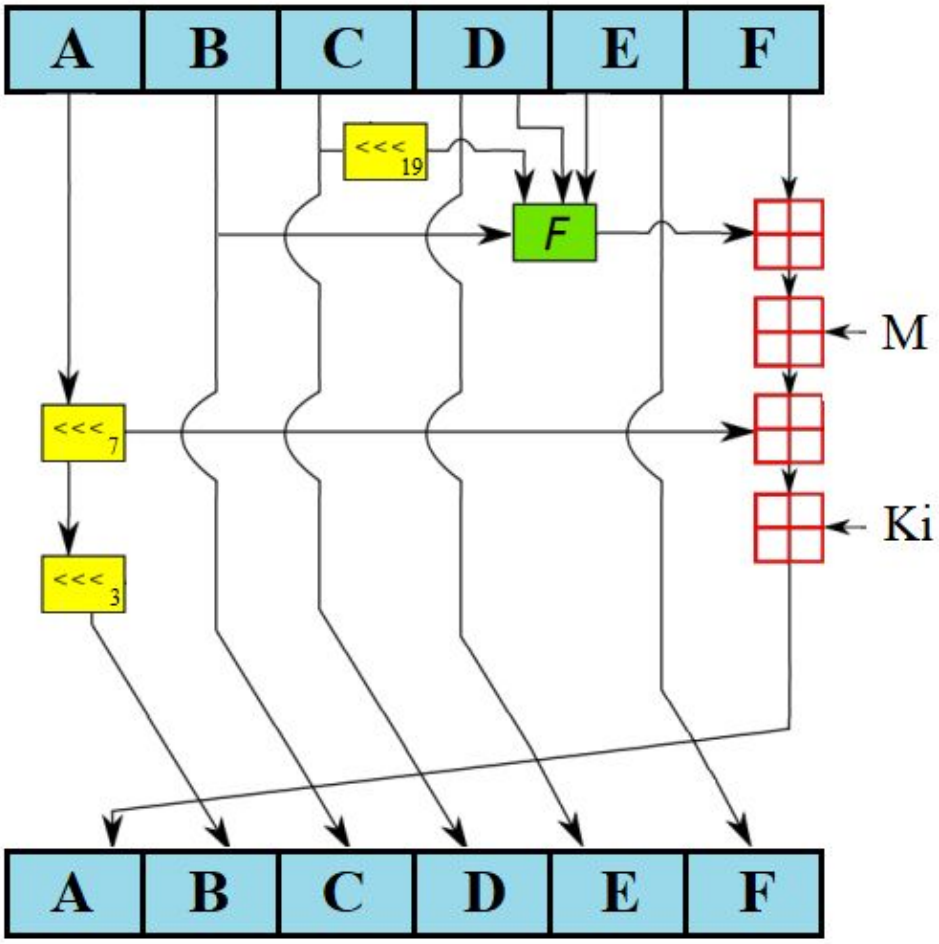
Hash Fonksiyonu

Hash alma işlemi 2 adımda oluşmaktadır. İlk adımı hash işlemi için girilen string türündeki verinin, byte değerlerini elde etme işlemidir. ConvertBlocks192 adındaki sınıfın üstlendiği bu görevde girilen string byte dizisine dönüştürüldü. (Her byte aslında 8bitlik uuzunluğunda integer bir değer)

Veri Yapısının Tasarımı: Gelen veri ister 1 bit olsun ister 1 terabyte olsun sonuç olarak 192 bitlik veri çıktısı almak istenmekte. Bunun için byte dizisi 24 byte'ın (8x24=192bit) tam katı olacak şekilde genişletildi yani padding eklendi. Sonrasında her terimi 4 byte yani 32 bitlik veri olacak şekilde bir diziye çevrildi. Burada 32 bitlik bloklar oluşturulmasının iki sebebi var. Birincisi 192 bitlik her bloğun 32 bitlik parçaları arasında hash fonksiyonlarını ve işlemlerini yapmak istenmesi, ikincisi ise 4 adet 8bitin birleşmesi sonucu oluşan değerleri tutmak için byte dizi yerine integer dizisine ihtiyaç duyulması ve 32 bitlik verilerin de integer tipini tam kapasite ile kullanacak oluşu. (integer sınırı 32 bit). Verimiz zaten 192 in yani 24 byte'ın katı olduğundan ve 32 bitlik bloklara ayrıldığından bu 32 bitlik blocklardan 6 tanesini alınması 192 bitlik bloklar oluşturulması anlamına geliyor. Bunun için elimizdeki dizi her elemanı 6 adet 32 bitlik veri tutan çift boyutlu bir dizi haline çevirildi ve hash işlemleri için gerekli veri yapımız kurulmuş oldu.

Hash İşlemi: Her 192 bitlik blok alınarak 32 blokluk kısımlarının bazıları değişikliğe uğrayarak birbiri ile etkileşime sokuldu. Bu etkileşim daha çok son 32 bit üzerinde gerçekleştirildi. Sonrasında 32 bit blocklarımız son 32 bit ilk 32 bit olacak şekilde kaydırıldı. Etkileşim işleminin merkezi olan son 32 bitlik kısım diğer 32 bitliklerin yanı sıra, var ise hash işleminden geçmiş bir önceki 192 bitlik bloğun 32 bitlik blokları ile ve önceden tasarlanmış bir k dizisinin terimleri ile de etkileşime girdi. Bu işlemler 96 kere tekar etti ve her 24 turda 32 blokluk bitler arasında etkileşime giren fonksiyonlar değiştirildi. Sonuç olarak 192 bit yani 16 lık tabanda 48 karakterli bir çıktı elde edilmiş olundu.

Hash işlemlerinin görsel hali aşağıdadır.



for i to 96 ;

M : 192 bitlik blok sayısı = 1 ise işlenen bloğun i%6 ncı 32 bitlik elemanı,
> 1 ise işlemden geçmiş olan bir önceki 192 bitlik bloğun i%6 ncı 32 bitlik elemanı.

Ki : 96 adet tekrarsız rastgele sayilar. (32 bitlik)

Tuzlama İşlemi: Tuzlama işlemi için 16 lik tabanda rastgele 48 karakter üretildi. Hashalanmiş parola ile birleştirildi ve 384 bitlik 96 karakterli bir veri oluşturuldu. Sonrasında bu veri tekrar hashlenerek veri tabanına kullanıcı parolası olarak gönderildi. Kullanılan 48 karakterlik tuz ise giriş işlemlerinde tekrar kullanılmak üzere ayrı bir tabloda veri tabanınana kaydedildi.

Test işlemi için gönderilen dosyadaki .apk uzantılı dosyayı android bir cihaza yükleyebilir veya uygulama klasörünü (UserSignUpSystem) android studio programı ile açabilirsiniz. Uygulamada kullanılan sınıflara ait java dosyaları ise kolay erişim ve inceleme için gönderilen dosyanın içindeki java adlı klasöre kopyalandı. Verilerin kaydedildiği veritabanını ise alttaki url ve hesabı kullanarak görüntüleyebilirsiniz.

url : https://console.firebase.google.com/project/usersignupsystem/database/usersignupsystem/data
e-posta : anonimhesap377@gmail.com
parola : hesapanonim377