İSÜ | İSTİNYE ÜNİVERSİTESİ İSTANBUL

BIL 008

BIL 008 : Kriptografi Temelleri

28/12/2020

Şifre Saklama ve Giriş Sistemi

Sonbahar 2020

Ahmad Al Khas

1 Giriş:

Bu proje ataması, Hash fonkisyonların ve şifre depolama sistemlerinin temellerini kavramak için sağlanmıştır. Sınıfta öğrendiğiniz kavramları kullanarak bir şifre depolama sistemi oluşturmanız gerekmektedir. Bu dokümantasyon dosyasıyla birlikte, **Passwords.txt** adlı başka bir dosya ekli bulacaksınız. Bu dosyayı projede kullanacaksınız ve kullanım şekli aşağıdaki bölümde açıklanmıştır 2. Aşağıdaki bölüm 3 projede sizden istenen görevleri temsil etmektedir. 4 bölümünde, oluşturduğunuz şifre depolama sistemlerini test etmek için bir oturum açma sistemi oluşturacaksınız.

2 Password.txt:

Bu dosyada kullanıcı adı-soyadı satırlarını ve şifrelerini bulacaksınız. Şifreler, kullanıcılarla ilgili ilişkili bilgilerle birlikte gerçek formunda saklanır. Sizin işiniz, dosyayı satır satır okumak ve 3 bölümünde belirtilen aşağıdaki görevleri yapmaktır.

3 Parola Depolama Sistemleri

Password.txt dosyasında saklanan kullanıcı bilgilerini okumanız ve aşağıdaki görevleri ayrı ayrı yapmanız istenir. Her görev farklı bir parola depolama sistemini temsil eder.

3.1 İlk görev:

1. Bir **Veritaban1.txt** dosyası oluşturun.
2. Her kullanıcıya **BIL008-2020xxxxx** biçiminde bir kimlik atayın, **x** ile etiketlenmiş son beş basamak rastgele seçilir. **Not: Oluşturulan her kimlik, şifre ile birlikte son bölümde sisteme giriş yapmak için kullanılacaktır** 4.
3. Şimdi, oluşturulan her bir kimliği, oluşturulan **Veritaban1.txt** dosyasında parola ile birlikte saklayacaksınız. **Not: Her kimlik ve parola tek bir satırda ve şu biçimde saklanmalıdır: Kimlik, Parola**

3.2 İkinci görev:

1. Bir **Veritaban2.txt** dosyası oluşturun.
2. Her kullanıcıy 3.1 öncesindeki görevde yaptığınız gibi **BIL008-2020xxxxx** biçiminde bir kimlik atayın.
3. Parolayı saklamadan önce digestini hesaplamalısınız. **Bu görevde hashing için MD5 algoritması kullanmanız gerekecek**.
4. Şimdi oluşturulan her bir kimliği, şifre digesti ile birlikte oluşturulan **Veritaban2.txt** dosyasında saklayacaksınız. **Not: Her kimlik ve şifre tek bir satırda ve şu biçimde saklanmalıdır: Kimlik, Digest**.

3.3 Üçüncü görev:

1. Bir **Veritaban3.txt** dosyası oluşturun.
2. Her kullanıcıy 3.1 öncesindeki görevde yaptığınız gibi **BIL008-2020xxxxx** biçiminde bir kimlik atayın.
3. Aşağıdaki 20 basamaklı dizeyi sisteminizde **salt** olarak kullanmanız gerekecektir.
   Salt = '9ahd37dn4hd82jdlf753'.

4. Oluşturulan **salt** şifresiyle 'XOR' işlem yapmanız gerekir.
5. Şimdi XORun çıktısının digestini bulunuz. **Bu görevde hashing için SHA224 algoritması kullanmanız gerekecek**.
6. Şimdi oluşturulan her bir kimliği, şifre digestı ile birlikte oluşturulan **Veritaban3.txt** dosyasında saklayacaksınız. **Not: Her kimlik ve şifre tek bir satırda ve şu biçimde saklanmalıdır: Kimlik, Digest**.

3.4 Dördüncü görev:

1. Bir **Veritaban4.txt** dosyası oluşturun.
2. Her kullanıcıy 3.1 öncesindeki görevde yaptığınız gibi **BIL008-2020xxxxx** biçiminde bir kimlik atayın.
3. 20 basamaklı rastgele bir **salt** dizesi oluşturun.
4. Oluşturulan **salt** şifresiyle 'XOR' işlemi yapmanız gerekir.
5. Şimdi XORun çıktısının digesti bulunuz. **Bu görevde hashing için SHA256 algoritması kullanmanız gerekecek**.
6. Şimdi, oluşturulan her bir kimliği, şifre digesti ve **salt** ile birlikte oluşturulan **Veritaban4.txt** dosyası içinde depolayacaksınız. **Not: Her bir Kimlik, şifre ve anahtar tek bir satırda ve şu biçimde saklanmalıdır: Kimlik, Digest, Salt**.

3.5 Beşinci görev:

1. Bir **Veritaban5.txt** dosyası oluşturun.
2. Her kullanıcıy 3.1 öncesindeki görevde yaptığınız gibi **BIL008-2020xxxxx** biçiminde bir kimlik atayın.
3. 20 farklı 20 basamaklı rasgele **salt** dizeler oluşturun.
4. Oluşturulan 20 **salt** birini rastgele seçin ve şifreyle 'XOR' işlemi yapınız.
5. Şimdi XORun çıktısının digesti bulunuz. **Bu görevde hashing için SHA384 algoritması kullanmanız gerekecek**.
6. Şimdi oluşturulan her bir kimliği, şifre digesti ile birlikte oluşturulan textbf Veritaban5.txt dosyasında saklayacaksınız. **Not: Kimlik, şifre ve tüm saltları tek bir satırda ve aşağıdaki formatta saklanmalıdır: Kimlik, Digest, salt1, salt2, . . . , salt19, salt20**.

4 Giriş Sistemi:

3 bölümünde oluşturduğunuz beş farklı depolama sistemini test etmek için bir oturum açma sistemi oluşturunuz. Sistem, kullanıcıdan oturum açmak istediği depolama sistemini seçmesini isteyerek başlamalıdır. Kullanıcının tercihine göre hangi **Veritabanx.txt** dosyasını yükleyeceğinize karar vereceksiniz. **Kullanıcı 1-5 arasında herhangi bir sayı girmelidir. Kullanıcı başka bir şey girerse, program bir uyarı mesajı vermeli ve kullanıcıdan doğru bir seçim girmesini istemelidir.**

Karar verildikten sonra, program kullanıcıdan şifre ve kimlik sormalıdır. Program, seçilen **Veritabanx.txt** 'ye bağlı olarak girilen şifrenin digestini hesaplayacaktır.

Son olarak, program girilen şifrenin hesaplanan özetini ve **Veritabanx.txt** 'de depolanan kimlikle ilişkili hash değerini karşılaştırmalıdır. Parola doğruysa, program kullanıcıyı parolanın doğru olduğu konusunda

bilgilendirecek ve çıkacaktır, aksi takdirde program kullanıcıyı parolanın yanlış olduğu konusunda uyarmalı ve kullanıcıdan depolama sistemini seçmekten başlayarak tüm adımı tekrarlamasını istemelidir (**Veritabanx.txt**).

Not: İlk depolama sisteminde 3.1 parolayı özetini hesaplamadan sakladığınızı unutmayın.
Not: Veritaban3-5.txt sistemleri için girilen şifre ile Saltu XOR işlem yapmayı ve Veritaban5.txt'de saklanan tüm olası saltları kontrol etmeyi unutmayınız.

5 Proje kuralları:

- 4 kişilik gruplar oluşturabilirsiniz.
- Her grup bir lider belirlemelidir. Grup lideri, proje ilişkin soruları sormaktan sorumludur.
- **Projenin son teslim tarihi 5 Ocak 10: 00'dur**.
- Tüm ekip üyeleri kodun akışını çok iyi bilmelidir çünkü aynı gün sunum olacaktır.
- Proje kodlarınızı ve tüm **Veritabnx.txt** dosyalarını .rar uzantılı sıkıştırılmış klasörler olarak göndermelisiniz.
- Proje klasörüne kodun akışını kısaca açıklayan ve grup üyelerinin adını ve soyadını belirten bir README.txt dosyası eklenmelidir.