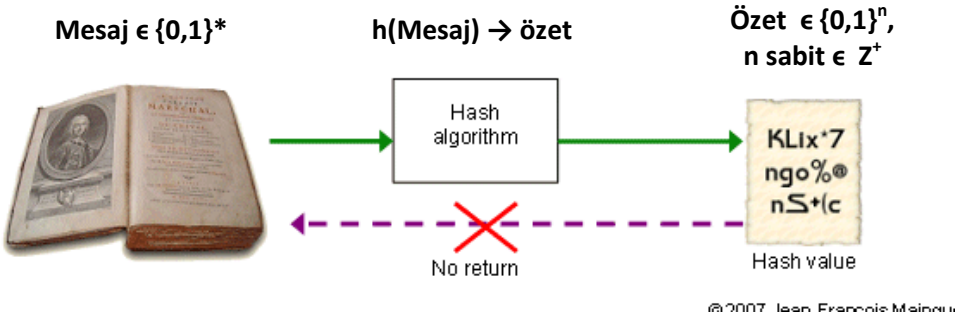
AMAÇ : Bu uygulamanın amacı kişiye kişiye özet fonksiyonların çalışma yapısını göstermek, özet fonksiyon hesaplama araçları yardımıyla aynı dokümana ait farklı özet fonksiyon değerlerinin karşılaştırmasını yapmak. Özet değer fonksiyonlarının güçlü ve zayıf yanlarını anlamasına katkıda bulunmaktır.

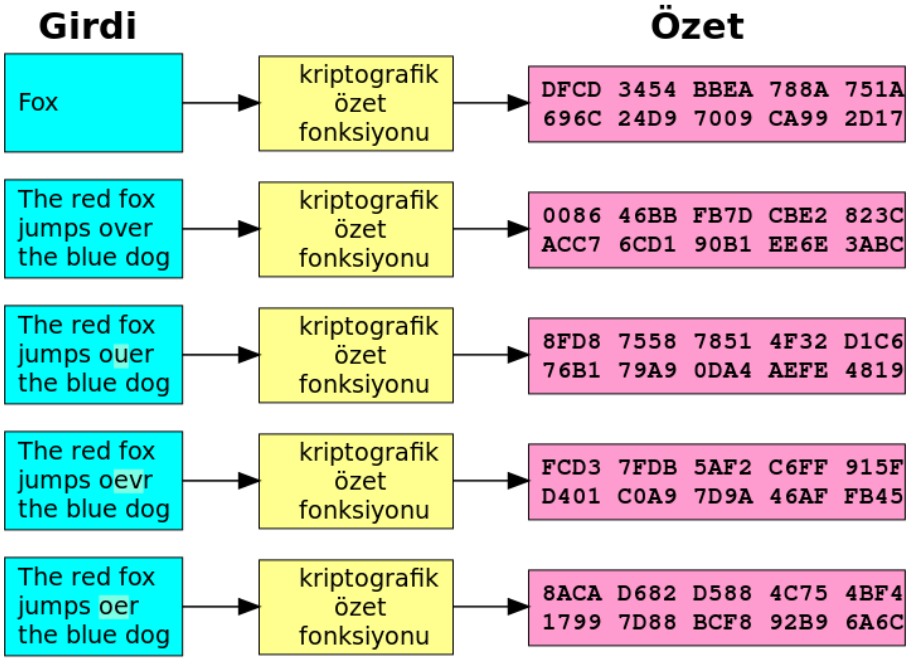
ÖNBİLGİ :

Özet (Hash)Fonksiyonlar : Değişik uzunluktaki bit dizilerini sabit uzunluklu bit dizilerine taşıyan polinomsal zamanda kolay hesaplanabilen fonksiyona "Özetleme Fonksiyonu" denir. Görüntü kümesinde oluşa sabit uzunluklu bit dizisine "Özet değer (Hash value)" denir. Kriptografide özetleme fonksiyonları değişken m uzunluklu mesajları sabit n uzunluklu mesajlara indirgemek amacıyla kullanılır. Mesajların bir bitindeki değişiklik hash kodunda değişmesine neden olur. Özet fonksiyonlar tersinir (tersine çevrilebilir değildir) özellikte değildir.



Şekil 1 Özet Fonksiyonlar Çalışma Şeması

Özetleme fonksiyonlarının amacı bir dosya, mesaj veya diğer veri bloğunun parmak izini üretmektir. Özet fonksiyonların gücü girdi olarak verilen mesajda yapılan en küçük değişikliğin özet kodda önemli değişikliğe neden olmasında (çığ etkisi) gelir.



Şekil 2 SHA1 Özet Fonksiyon Algoritması Örneği

UYGULAMA :

A. Uygulama öncesi yapılacaklar :

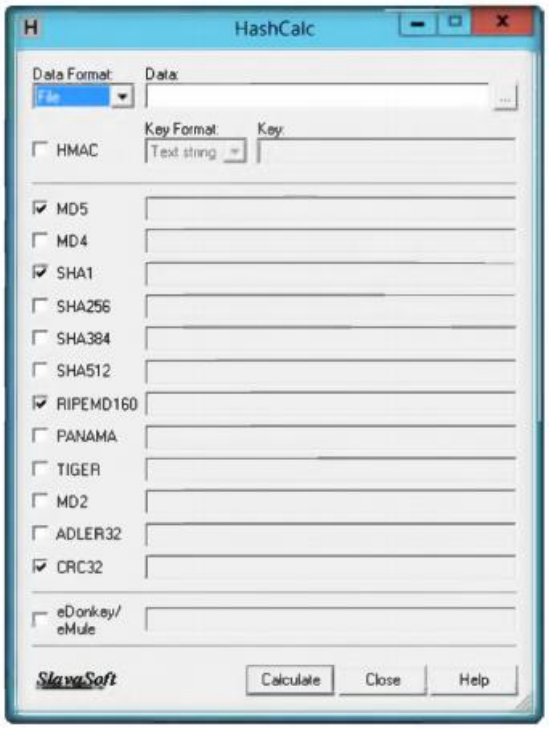
a) HashCalc programını (http://www.slavasoft.com/hashcalc/) adresinden indirip kurun.

b) Aynı_Özet_Koda_Sahip_Dosyaları_Bul(Klasör) → Dosya Listesi

Parametre olarak klasör adı alan ve bu klasör içerisinde aynı md5 özet değerine sahip dosyaları listeleyen fonksiyon yazın.

B. Uygulamanın Yapılışı:

a) HashCalc programını kullanarak bu dokumana ait özet değerleri çıkarın.



Şekil 3 HashCalc Özet Fonksiyon Programı Arayüz Görüntüsü

b) Boş bir text dokümanı oluşturun, içine ayrı ayrı "Hello World" ve "HELLO WORLD" yazarak özet değerlerini kontrol edin. Metinlerin sonuna boşluk ekleyerek özet değer değişimini gözlemleyin.

c) Size verilen resim dosyalarından hangilerinin aynı özet fonksiyona sahip olduğuna dair fikir yürütün.

d) Aynı_Özet_Koda_Sahip_Dosyaları_Bul(Klasör) fonksiyonunu kullanarak adresinde bulunan resim dosyalarından aynı md5 değerine sahip olanları bulunuz.

ANALİZ :

- Özet fonksiyonlar arasındaki farkları ve güvenlik değerini tartışın.
- Veri şifreleme için özet fonksiyonların güvenlik seviyesini tartışın.
- Aynı özet değere sahip iki farklı doküman olabilir mi ?