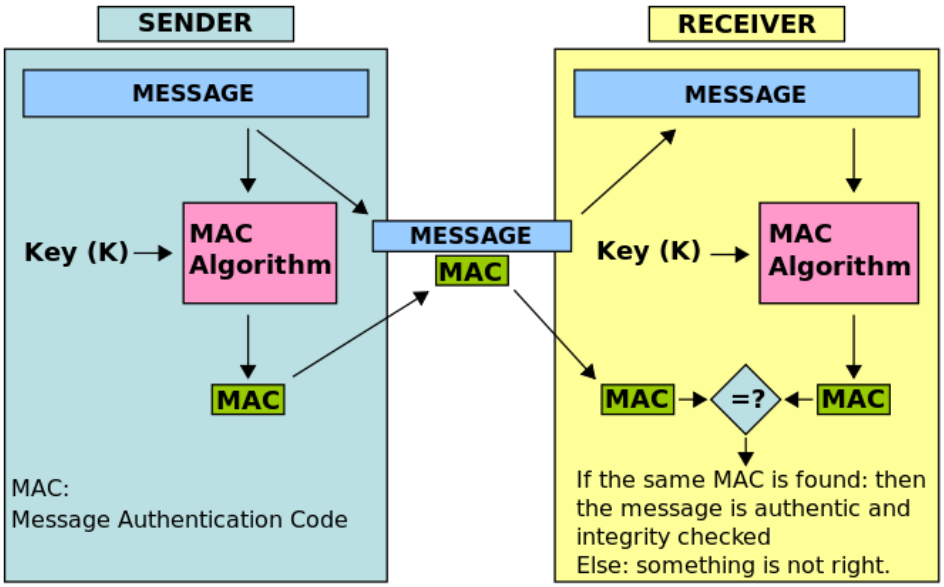
AMAÇ : Bu uygulamanın amacı kişiye mesaj doğrulama fonksiyonların çalışma yapısını göstermek. Merkle–Damgård yöntemini yöntemini kullanana mesaj doğrulama kod fonksiyonlarında bulunan hash uzunluk genişletme açılığını istismar edecek.

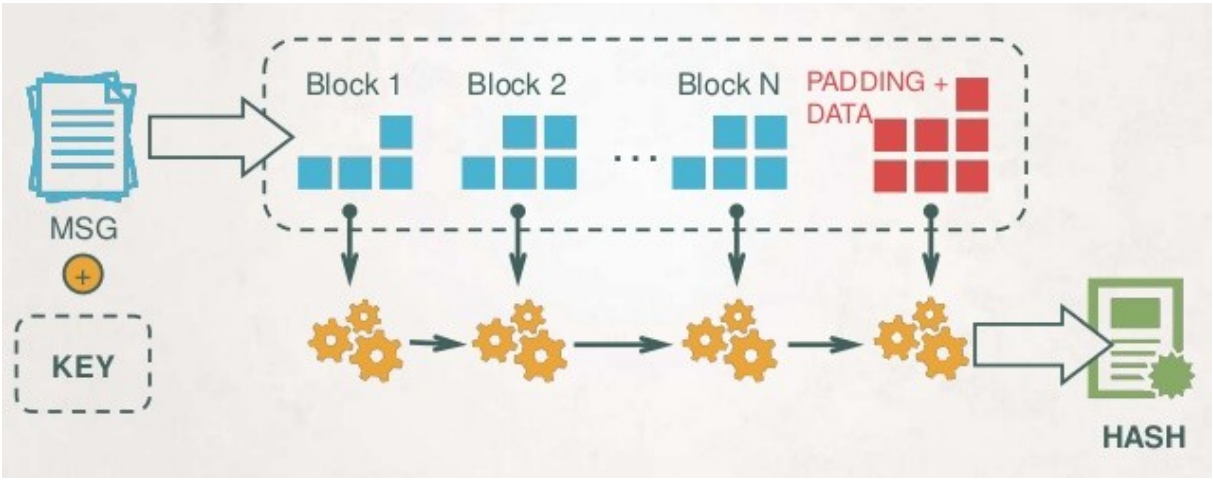
ÖNBİLGİ :

Mesaj Doğrulama Kodu MAC (Message authentication code):



Şekil 1 mesaj Doğrulama Kodu Çalışma Şeması

Hash Uzunluk Genişletme Saldırısı: Özet Fonksiyonlar (MD5, SHA-1, SHA-256, SHA-512 vb.) genelde özet değer algoritmalarında Merkle–Damgård yöntemini kullanırlar. Bu yöntemde özet değeri çıkarılacak mesaj hash fonksiyonun türüne göre bloklara ayrılır ve bloklar halinde hash değeri hesaplanır. Hesaplama işleminde Şeki2'de görüleceği üzere her bir bloğun çıktısı diğer blok için girdi olarak kullanılır. Mesaj her zaman bloklara tam bölünmez. Bu durumda bloğun kalan kısmı için doldurma (padding) işlemi uygulanır. Bu özellik hash fonksiyonları MAC (mesaj doğrulama kodu) olarak kullanıldığı durumlarda hash değerini uzunluk genişletme (length extension) saldırılarına açık hale getirmektedir. Ve bu açıklık gizli anahtar bilinmese dahi (secret key) geçerli bir MAC oluşturulmasına imkan tanımaktadır.



Şekil 2 Özet Fonksiyonlar Çalışma Şeması

UYGULAMA :

A. Uygulama öncesi yapılacaklar :

a) HashCalc programını (http:/vww.slavasott.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.