Balloon Arama motoru ilk kez 2022 yılı içerisinde Tarihten Bilimsel örnekler alınarak
Yeni nesil Web 3 arama motorudur .

Davincinin şifresi adlı kitabında bulunan Kriptex ve Da brown un ilham aldığı örneklendirmeler önemli ölçüde kod olarak yeniden tasarlanıp arama motoru ile entegre edilmiştir .

Yapısı:Kripteks, bir bisiklet kilidine benzetilebilir.
Bir silindirin üstüne sabitlenmiş 5 adet halka ve her halkanın üstünde bulunan tüm alfabenin dizili olduğu bir halka var.
Anahtar tam halkalara denk gelen yerlerde boşluklara sahip, diğer yerlerde çıkıntıları var.
Harfler doğru sıraya getirildiğinde,
en alttaki halkalar anahtarın çıkabileceği bir boşluk oluşturuyorlar ve bu sayede anahtar çıkıyor.

Balloon un ürettiği anahtarlar ,güvenli alınan ve karşıya verilen verinin kilitlenerek ulaşmasını sağlıyor
anahtarlanma başlatıldığı zaman kilitlenerek çözümleme yapıyor .
hem bilgisayar kullanıcısı hemde internet ortamı daha güvenli veri akışına sahip oluyor .

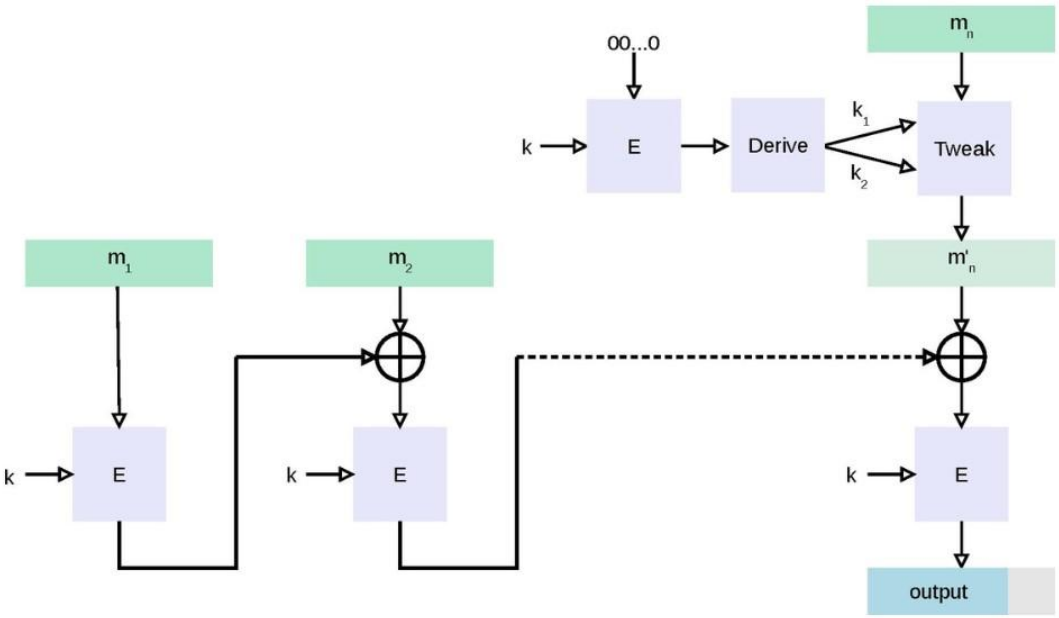
Da brown a göre :

Dan Brown'un anlattığına göre, güvenlik nedeniyle, papirüs üzerine yazılmış gizli belge bir şişe sirkeye sarılıp öyle kripteksin içine konuyor.
Bunda amaç şifreyi bilmeyen ve zorla açmaya çalışan birinin şişeyi kırıp papirüsü eritmesini sağlayabilmek.
Ayrıca her parça kendi ekseni etrafında diğer parçalardan bağımsız olarak dönebilmektedir.
Bazı özel amaçlı yapılmış kripteks lerde şifreyi girmek için bir tek hakkınız vardır.

Balloon arama motoru inşa edilirken kodlanan Şemalar .

CBC-MAC hesaplarken m CBC kipinde ilklendirme vektörü ile şifrelenir ve son blok tutulur.
Aşağıdaki şekil,

Resim:



Kriptografide, CBC-MAC , bir blok şifreleme ile mesaj kimlik doğrulama kodu oluşturmak için kullanılır.
Mesaj, her blok önceki bloğun düzgün şifrelenmesine bağlı olacak şekilde, bir blok zinciri oluşturmak için CBC kipinde bir blok şifreleme algoritmasıyla şifrelenir.
Bu bağlılık sayesinde, şifresiz metnin herhangi bir bitiminde yapılan değişikliğin, şifrelenmiş son bloğun, blok şifreleme anahtarı bilinmeden tahmin edilmesini veya etkisiz hale getirilmesini engeller.
mesajı için CBC-MAC hesaplarken m CBC kipinde ilklendirme vektörü ile şifrelenir ve son blok tutulur. Aşağıdaki şekil,
gizli anahtar k ve bir blok şifre E kullanarak CBC-MAC hesaplamasını göstermektedir.

Sabit ve değişken uzunluklu Mesajlarda güvenlik

Eğer kullanılan blok şifreleme güvenliyse (pseudorandom bir permütasyon ise),CBC-MAC sabit uzunluktaki mesajlar için güvenlidir.[1]
. Ancak, tek başına, değişken uzunluklu mesajlar için güvenli değildir. .
Nitekim, herhangi tek anahtar sadece sabit ve bilinen uzunluktaki mesajlar için kullanılmalıdır. Bunun sebebi ise, İki mesaj için doğru mesaj-etiket çiftlerini bilen saldırgan, mesajı için MAC hesaplanırken,
öncelikle m için Mac'i t deki gibi klasik şekilde hesaplanır, ama bu değer ilerideki hesaplayan bir adıma zincirlendiğini,

ilk mesajdaki mac den üretilen değer ile birlikte özel or operasyonu gerçekleştirilir. Yeni mesajda etiketin var olması,
ilk m mesajındaki şifresiz metin bloklarından üretilen mac'e etki bırakmadan iptal edileceği anlamına gelir:

Bu problem, sona mesaj boyutunda blok eklemek ile çözülemez.[2]
CBC-MAC in değişken uzunluklu mesajlar için güvenli yapabilecek şekilde değiştirildiği üç ana yöntem vardır;
1) Girdi boyutlu anahtar ayırmak; 2) başa uzunluk eklemek; 3)
son bloğu şifrelemek. Öyle bir durumda, farklı bir blok şifre çalışma kipi kullanılması önerilebilir,
örneğin, değişken boyutlu mesajın bütünlüğünü korumak için CMAC veya HMAC.

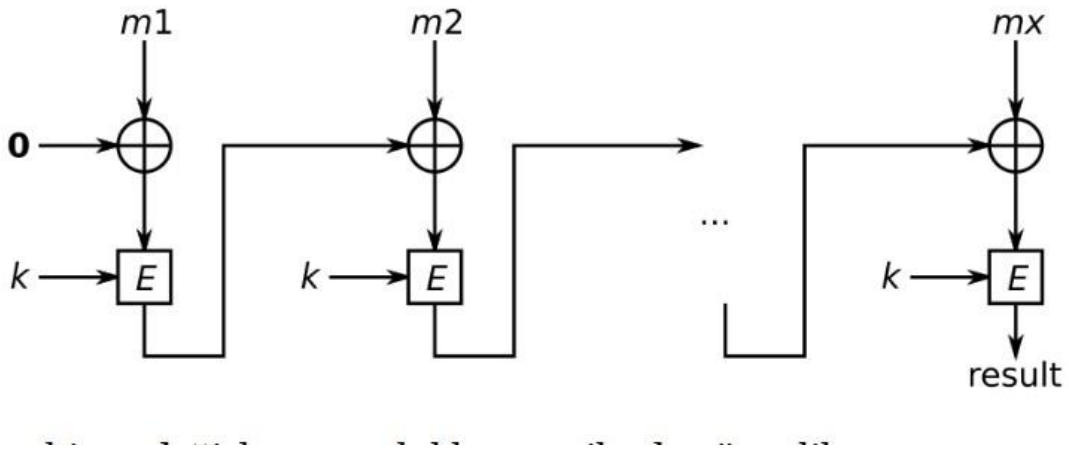
Uzunluğu Başa Eğmek :
Bir çözüm yöntemi olarak, mesaj uzunluğunu ilk blokta bulundurmaktadır.
[3]; herhangi iki birbirinin prefixi olan mesaj kullanılmadığı sürece CBC-MAC'in güvenli olduğu kanıtlanmıştır ve uzunluğu başa eklemek bunun özel bir durumudur.
[4] İşlem başladığında mesajın uzunluğu bilinmiyorsa problemler oluşabilir.

Son Blogu şifrelemek :

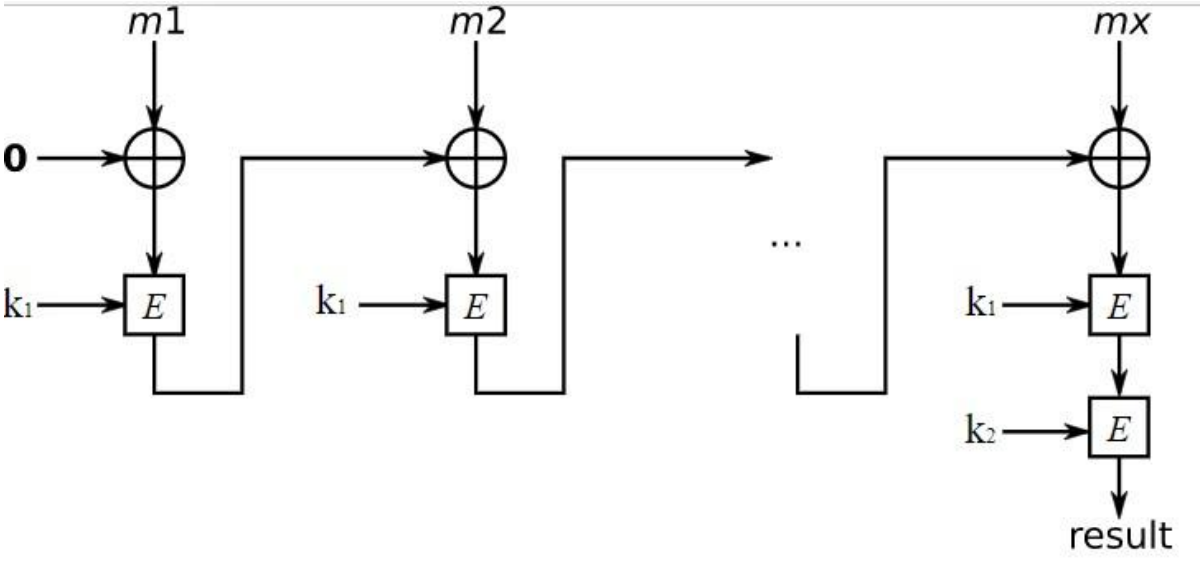
CBC-MAC te son bloğu şifrelemek (ECBC-MAC) [5], CBC-MAC-EIB (m, (k1, k2)) = E(k2, CBC-MAC(k1, m))[2] şeklinde tanımlanır
Bahsedilen diğer yöntemlerden olan CBC-MAC i değişken uzunluklu mesajlar için uzatmaya göre, son bloğu şifrelemenin avantajı hesaplama bitene kadar mesaj uzunluğunun bilinmesinin gerek memesidir.

Saldırı Yöntemleri:
Birçok kriptografik şemada olduğu gibi,
şifrelerin ve protokollerin naif kullanımı,
kriptografik korumanın etkenliğini düşürüp (hatta işe yaramaz hale getirip) saldırıları mümkün kılabilir.
CBC-MAC'in yanlış kullanımından kaynaklanan saldırılardan bahsedeceğiz.[6]

Resim



Şifreleme ve Kimlik doğrulama için aynı anahtarı kullanma:



Başlangıç Vektörünün değerinin Değişmesine izin verme :

Şifreleme bloğu zincirleme (veya bir başka) kip içinde bir blok şifreleyici kullanarak verileri şifrelerken,
şifreleme işleminin ilk aşamasına bir başlatma vektörü eklemek yaygındır.
Tipik olarak bu vektörün rastgele seçilmesi (tek seferlik anahtar) ve blok şifresinin çalıştığı herhangi bir gizli anahtar için tekrar edilmemesi gerekir.
Bu, aynı düz metnin aynı şifre metnine şifrelenmesini sağlayarak, saldırganın bir ilişki oluşturmasına izin verir semantik güvenlik sağlar.

Bir başlatma vektörünün CBC-MAC gibi bir mesaj kimlik doğrulama kodu hesaplanırken kullanılması olası bir saldırı vektörüdür.
Bir şifre bloğu zincirleme şifresinin çalışmasında, düz metnin ilk bloğu başlatma vektörü ile özel OR kullanılarak karıştırılır P1-O-IV.
Bu işlemin sonucu, şifreleme işlemi için blok şifrelemenin girdisidir.Ancak, şifreleme ve şifre çözme işlemleri gerçekleştirilirken,
ilklendirme vektörü şifresiz metinle göndermekle yükümlüyüz-tipik olarak şifreli metnin ilk bloğundan önceki blok olarak- bu şekilde şifresiz metnin ilk bloğunun şifresi çözülebilir.
ve başarıyla kurtarılabilir. Eğer bir MAC hesaplıyorsanız, mesajdaki etiketin hesaplanan değer ile eşleştiğini doğrulayın bilmek için.
ilklendirme vektörünü diğer tarafa şifresiz metin ile iletmemiz gerekecektir.
Eğer ilklendirme vektörünün keyfi olarak seçilmesine izin verilirse, aynı mesaj etiketi oluşturulurken ilk şifresiz metin bloğu değiştirilebilir (farklı bir mesaj ileterek).
Bir mesaj düşünün M1=P1|P2. Özellikle, CBC-MAC için mesaj etiketini hesaplarken, bir IV ilklendirme vektörü seçtiğimizi varsayalım, öyle ki MAC'ın hesaplanması EK (IV 1 OP 1) ile başlasın.
Bu bir mesaj etiketi üretir . (m1-,T1)
Şimdi M2=p1|P2 mesajı üret. P1 içindeki değiştirilmiş her bit için,
ilklendirme vektöründe karşılık gelen bitler çevirilir ve IV ilklendirme vektörü üretilir.
Bu mesaj için MAC'ı hesaplarken şu işlem ile başlıyoruz:
EK (p1 O IV1). Hem şifresiz metin hem ilklendirme vektörü bitleri aynı yerde değiştirildiği için, ilk aşamada değişiklik iptal edilir,yani blok şifre girişi M1 için olan ile aynıdır.
Eğer şifresiz metinde başka değişiklik yapılmazsa, farklı bir mesaj iletiliyor olsa dahi aynı etiket üretilir.
İlklendirme vektörü seçme özgürlüğü kaldırılırsa, ve tüm CBC-MAC implementasyonları belirli bir ilklendirme vektörüne sabitlenirse.
(genelde sıfır vektörü ancak herhangi bir şey olabilir) bu saldırı devam edemez.
Özetlemek gerekirse, saldırgan MAC doğrulaması için kullanılacak IV belirleyebiliyor,
MAC'i geçersiz kılmadan ilk veri bloğunda keyfi değişiklik yapabilir.

Öngörülebilir ilklendirme vektörü kullanma:

Bazen IV, mesaj tekrar saldırılarını önlemek için bir sayaç olarak kullanılır.
Ancak, saldırgan MAC doğrulaması için hangi IV'ün kullanılacağını tahmin edebiliyor ise doğrulama için kullanılacak IV deki değişikliği telafi etmek için ilk veri bloğunu,
değiştirerek önceden gözlemlenen mesajı tekrar dinleyebilir. Örneğin saldırgan IV- 1 ile birlikte M1=P1-P2 ...
mesajını gözlemlemiş sse IV-2
M'1-= (P1 O IV1 O IV 2)P2 üretebilir .IV2 ile mac doğrulamasını geçer .

En basit karşı tedbir, IV kullanmadan önce şifrelemektir (yani IV'ü veriler için hazırlamak). Alternatif olarak CFB kipindeki MAC kullanılabilir, çünkü CFB kipinde IV verilerle XOR edilmeden önce şifrelenir.

Başka bir çözüm olarak (mesaj tekrarı saldırıları koruması gerekli değilse) her zaman sıfır vektörü IV kullanılır
Yukarıdaki formül M1 için M1 = (P1- 0 -0-0) P2 ...=P1-P2 M1 haline gelir m1 ve m1 aynı mesaj olduğu için,
tanım gereği aynı etikete sahip olurlar. Bu bir sahtecilik değildir, CBC-MAC'in amaçlanan kullanımıdır.

Algoritmayı Kullanılan Standartlar :

FIPS PUB 113 Bilgisayar Verileri Kimlik Doğrulaması,
CBC-MAC algoritmasını blok şifre olarak DES kullanarak belirleyen bir ABD hükümet standardıdır (artık kullanılmamaktadır) .
CBC-MAC algoritması ISO / IEC 9797-1 MAC 1 Algoritmasına eşdeğerdir.

Ve web 3 Arama motorunun ilk örneğidir .herhangi bir Grişimci ile ölçeklendirlemez.
Web 3 Arama motoru Kriptex kodlarıyla inşa edilmiştir .
güvenli verilerin kilitlenme yoluyla sağlıklı gelen ve giden bağlantının bilgisayar kullancısına güvenle aktarma katmanıdır.