Muhammed Ramadan
90290605

) Bilgi güvenliği, bilginin gizlilik, bütünlük ve erişilebilirlik korunmasını sağlamak için uygulanan stratejiler, politikalar ve prosedürler bütündür. Bilgi güvenliği, bir organizasyonun veya bireyindeğerli bilgilerinin korunmasını sağlar.

1- Gizlilik: Bilginin yetksiz erişimden, ifşadan, yayımlanmasından. Gizlilik özel bilgilerin sadece yetkili kişilere açık olmasını sağlar.

2- Kimlik Denetimi: Bir sistem veya ağa erişim denemesi yapan kişinin yada hizmetin kimliğinin doğrunması işlemidir. Bu genellikle bir kullanıcı adı ve şifre kombinasyonu ile gerçekleştirilir, ancak daha gelişmiş sistemler, sistemler biyomtrik veriler veya çokfaktörlü kimlik doğulama kullanbilir.

3- Erişim kontrolü: Yetikli kullanıcıların belirli bilgilere veya kaynaklara ne zaman ve nasıl temelinde yapılır yani belirlidi bir rodeki bir kullanıcı belirli bir bilgiye veya kaynağa erişme yeteneğine sahip olabilir. Erişim kontrolünü önemli bir parçası

Muhammed Ramadan
19029060 5

Kullanıcıların yanızca işlerini yapmak için ihtiyaç duydukları bilgilere erişbilmelerini sağlamaktır.

Muhammed Rama

19029 0605

2)

ymj jsnlrf rfhmnsj nx fhumiw ijanhj ijajqtwji

fsi Zxji uwtyjhy htvrjwhnfq, inuqtrfynh

, fsi rngnyfwd htrrzsmhfynts

Muhammed Ramadan
19029605

3)

1- Anahtar Genişletme: ilk olarak, orijinal anahtar genişletilir. böylece her tur için benzersiz bir anahtar oluşturulur.
Bu genişletilmiş anahtar, şifrelemenin her bir turunda kullanılacak

2- ilk Anahtar Ekleme (AddRoundKey): Bu her bir byte'ın (veri bloğundaki) belirli bir anahtarın karışık gelen byte'ı ile XOR işlemine tabi tutulmasıdır. Bu işlem, şifreleme işlemine başlamadan önce gerçekleştirilir.

3- Byte Substitüsyonu (subBytes): Bu, S-Box adı verilen önceden belirlenmiş bir tabloyu kullanarak her byte'ı yeni bir byte ile değiştirir. Bu, şifelemenin her bir turunda gerçekleştirilir.

4- Satır Kaydırma (shiftRows): Bu, her satırın belirli bir sayıda byte'a kaydırılmasını içerir.
Birinci satır sabit kalırken, ikinci satır bir byte'a, üçüncü satır iki byte'a ve dördüncü satır üç byte'a kaydırılır. Bu işlem, veri üzerindeki düşey desenleri karıştırmaya yardımcı olur.

ammed Ramadan

290605

Sütün Karıştırma (Mix Colums): Bu, matris çarpma ve XoR işlemlerini kullanarak her sütunu dönüştürmeyi içerir. Bu işlem, veri üzerindeki yatay desenleri karıştırmaya yardımcı olur.

Tur Anahtar Ekleme (AddRoundKey): Bu, karıştırılmış verinin tur anahtarıyla XoR'lanmasını içerir.