İSÜ | İSTİNYE ÜNİVERSİTESİ
İSTANBUL

Final Sınavı
19/1/2021
Sonbahar 2020

BIL 008

Adı-Soyadı: Furkan Kaya

Time Limit: 60 dakika

Öğrenci ID: 19721600 2

Bu sınav 4 sayfa (bu kapak sayfası dahil) ve 6 sorudan oluşmaktadır.

Lütfen soruları dikkatlice okuyun ve cevaplarınızı yazmaya başlamadan önce düşününüz.

Cevaplarınızı diğer öğrencilerle paylaşmanız kesinlikle yasaktır.

1. Lütfen blok şifrelemeyle ilgili aşağıdaki soruları yanıtlayın:

   1. One time pad algoritması güvenli bir algoritma olarak kabul edilmekle birlikte, yine de pratik değildir. Neden?
   2. Neden AES şifreleme algoritması 3DES yerine yaygın olarak kullanılıyor? Her iki algoritma için anahtar uzunlukları nedir?
   3. AES algoritmasının operasyonel adımlarını listeleyin.

1.) Algoritmanın güvenliği, pedin yalnız 1kez kullanılmasına bağlıdır. Bu sebeple pratik değildir.

2-) AES çok daha hızlı ve daha güvenlidir.
AES: Algoritma 128-256 arasındaki 32 bitin herhangi bir katı uzunluğa izin vermektedir. Lakin FIPS 128 ile standart hale getirdi. 3DES: 56*3 => 168

3-) subBytes / shiftRows / mixColumn / addRoundKey

2. Derste öğretilen Stream ciphers'in ilk iki çalışma modunu listeleyin ve her birini savunmasız bırakabilecek saldırıları listeleyin.

ECB - CBC

CBC: IV Başlatma vektörü tahmin edilemez olmalı
Kayıtlar aynı anahtarla şifrelenmemeli.
Flipping attack, Bit savgısız, oracle padding
ecb: man in the middle saldırısı kullanılabilir. Şifrelide olsa aynı giriş, aynı çıkışı vereceğinden veriler manipüle edilebilir.

3. Diffie-Hellman algoritmasını tanımlayın. Onu savunmasız bırakabilecek saldırılar nelerdir?

İsmi protokolü kesfeden iki kriptografik öncülerin soy isimlerinden gelmektedir.
yanlış yönden çözülmesi çok zor olan ama doğru yönden hesaplanabilen matematik problemlerine dayanır.
güvensiz ağlarda anahtar değişimi için kullanılabilir.
man in the middle savunmasız bırakır. Aktif saldırgan sistemi kırabilir.

4. Lütfen aşağıdaki ifadelerden hangilerinin doğru hangilerinin olmadığını belirtin.

   1. DES algoritması standartlaştırıldı (**Doğru**|**Yanlış**) 1977'de
   2. AES algoritması standartlaştırıldı (**Doğru**|**Yanlış**) 128, 192, 256 bit ile sınırlı
   3. 3DES algoritması standartlaştırılmadı (**Doğru**|**Yanlış**) Des standart insanlar 3Des'i kullanıyor
   4. AES algoritması asimetrik bir anahtar şifreleme algoritmasıdır (**Doğru**|**Yanlış**)
   5. MD5 algoritması simetrik bir anahtar şifreleme algoritmasıdır (**Doğru**|**Yanlış**) Hash algo.

5. Uygulamağınız parola depolama projesiyle ilgili olarak, 5 tür depolama sistemi vardı:

   1. Parolayı olduğu gibi saklıyor.
   2. Parolayının digesti uyguladıktan sonra saklama.
   3. Parola ve verilen salt karışımını karıştırdıktan sonra parolayı saklama.
   4. Parola ve rastgele oluşturulan salt karışımını karıştırdıktan sonra parolayı saklama.
   5. Parola ve rastgele oluşturulan 20 salt un rastgele seçilen salt karışımını karıştırdıktan sonra parolayı saklama.

   Aşağıdaki cevaplayın:

   - Hangi depolama sistemleri güvenli, hangileri güvenli değildir?
   - Güvensiz olarak listelediklerinizin zayıf yönleri nelerdir?
   - Lütfen salt ve hash işleminin önemini açıklayın.

soru-1)
3, 4, 5 güvenli. 1, 2 değildir

soru 2-)
veritabanı hacklenebilir ve şifreler siteye özel olmadıklarından facia oluşur. yanlızca digest saklanması ise Rainbow tablolarına izin verir. ilerisi için tehlike yaratır.

soru-3)
salt digest'i siteye özel hale getirir ve Rainbow tablelerin önüne keser. hash ise veritabanı kırılırsa şifrelerin direkt saldırgan eline geçmesine engel olur.

6. İlk projenizde, aşağıdaki adımlardan oluşan bir şifreleme / şifre çözme algoritması uyguladınız:

   1. Bit çevirme.
   2. İlk ikili akışı karıştırma (Anahtar1 kullanılacak).
   3. XOR işlem (Anahtar2 kullanılacak. Ters çevirmeyi unutmayın).
   4. Ikinci ikili akışı karıştırma (Anahtar3 kullanılacak).

   Verilen 16 bitlik ikili sayıyı "1001101110001010" algoritmaya girdi olarak düşünün, Anahtar1 = [3,2,4,1], Anahtar2 = 10110011 ve Anahtar3 = [3,5,7,1,2,8,4,6] olduğunu bilerek dört adımın her birinin sonuçlarını yazın.
   Not: Algoritmanın 256 bit yerine 16 bit üzerinde çalıştığını düşünün

1-) 0101000111011001
2-) 1101,0001,1001,0101
1011001101001100
3.1) 10110011 → 01001100
10110011 01001100
3-) 01,10,00,10,11,01,10,01
3 5 7 1 2 8 4 6
4) 1011011010010001 //