



Final Sınavı
19/1/2021
Sonbahar 2020

BIL 008

Adı-Soyadı: _____

Time Limit: 60 dakika

Öğrenci ID: _____

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

Lütfen soruları dikkatlice okuyun ve cevaplarınızı yazmaya başlamadan önce düşününüz.

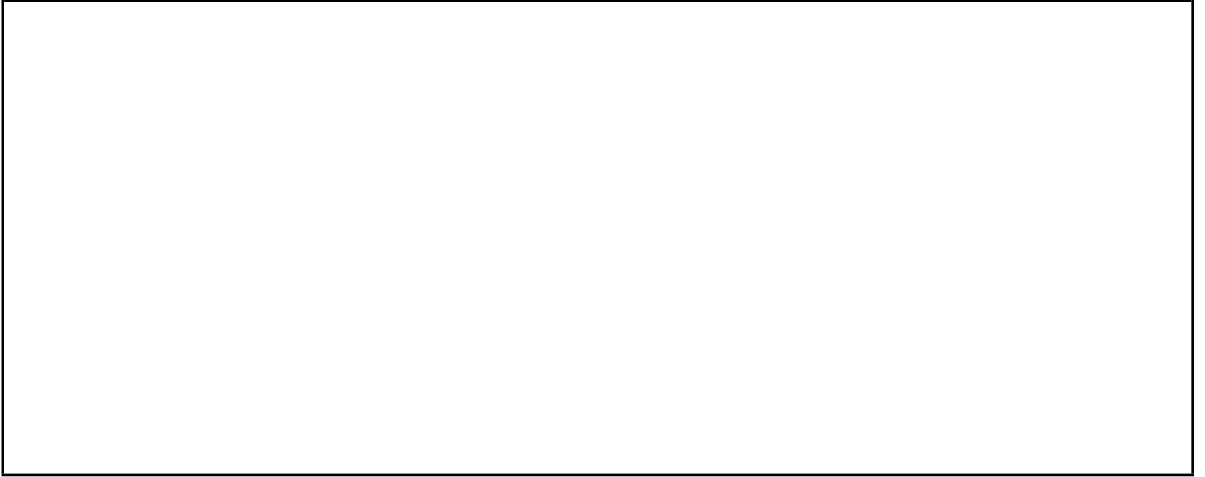
Cevaplarınızı diğer öğrencilerle paylaşmanız kesinlikle yasaktır.

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.



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



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



4. Lütfen aşağıdaki ifadelerden hangilerinin doğru hangilerinin olmadığını belirtin.

1. DES algoritması standartlaştırıldı (**Doğru|Yanlış**)
2. AES algoritması standartlaştırıldı (**Doğru|Yanlış**)
3. 3DES algoritması standartlaştırılmadı (**Doğru|Yanlış**)
4. AES algoritması asimetrik bir anahtar şifreleme algoritmasıdır (**Doğru|Yanlış**)
5. MD5 algoritması simetrik bir anahtar şifreleme algoritmasıdır (**Doğru|Yanlış**)

5. Uyguladığınız 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.

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. İkinci 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