**UBI523 Kriptosistemler ve Kriptografik Protokoller**

**FİNAL SINAVI**

**7 Ocak 2019**

**İki A4 yardım kağıdı. Süre 2 saat.**

**Dilediğiniz 5 soruyu yanıtlayınız. Yanıtlamadığınız soruyu açık olarak işaretleyiniz.**

**1**. Bir firma ağ üzerinden gönderdiği tüm dosyaları 128 bitlik AES algoritması ile CBC modunda şifrelemektedir. AES için sabit bir 128 bit anahtar kullanılmakta, IV değeri ise her gün değiştirilmektedir. Şifreleme dosya tabanlı olup, her dosya için o günkü IV değeri CBC modunda kullanılmaktadır.

Varsayalımki bu sabah 128 bitlik sabit AES anahtarını ele geçirdiniz; fakat geçerli IV değerini bilmiyorsunuz. Gün içinde iki şifreli dosyayı ağ üzerinde iletim sırasında kopyalayabildiniz. İlkinin içeriği hakkında bilginiz yok, fakat ikincisinin şifrelenmeden önceki içeriği baştan sona 0xFF olan otomatik olarak üretilmiş geçici bir dosya olduğunu biliyorsunuz. Bugünün IV değerini ve ilk dosyanın içeriğini nasıl bulursunuz? Açıklayınız.

**2.** RSA parametreleri *p=11*, *q=5* ve *e=3* (*encryption exponent*) verilmiş olsun.

1. *d = ?* (*decryption exponent*)
2. Açıkmetin (*plaintext*) *M = 1234* için şifrelimetin (*ciphertext*) *C = ?*

**3.** Aşağıdaki mesajların gizlilik (*confidentiality*), bütünlük (*integrity*), doğruluk (*authentication*) ve inkar edilemezlik (*nonrepudiation*) özelliklerini sağlayıp sağlamadığını (kısa gerekçelerle) açıklayınız.

**a)** A to B : EKs[M] **b)** A to B : EKpB[M]

**c)** A to B : EKrA[M] **d)** A to B : EKpB[EKrA(M)]

Not: *E* şifreleme (*encryption*), *Ks* A ve B’nin ortak anahtarı, *KpB*B’nin açık (*public*) anahtarı, *KrA*A’nın özel (*private*) anahtarı ve *M* mesaj/açıkmetin

**4. a)** Diffie-Hellman Anahtar Değişim (DHKE) Protokolünü tüm adımlarıyla yazınız.

**b)** DHKE Protokolüne karşı yapılan Ortadaki adam (*man-in-the-middle*) saldırısını anlatınız. Bu saldırı günümüzde nasıl engellenmektedir?

**5. a)** Bu problemde simetrik ve asimetrik kripto-sistem algoritmalarının işlemsel (*computational*) performanslarını karşılaştırmak istiyoruz. ElGamal algoritmasının modern bir PC’de 1500 Kbit/sn hızında çözme (*decryption*) işlemi yapabildiğini varsayalım. Aynı makinada, AES algoritması ise 64 Mbit/sn hızında çözme yapabilir. Bilgisayarda depolanmış 1 GByte’lık bir DVD’nin çözme işlemi her bir algoritma ile ne kadar zaman alır? Simetrik algoritma mı yoksa asimetrik algoritma mı daha hızlıdır? Kaç kat?

**b)** Yaklaşık 450 çalışanı olan bir firmada Simetrik şifreleme kullanılan bir güvenlik politikası uygulanmaya karar veriliyor. Her çalışanın potansiyel olarak tüm çalışanlarla güvenli iletişim kurma ihtiyacı olacağı düşünüldüğünde sistemde toplam kaç anahtar çiftine ihtiyaç olacaktır? Her bir çalışanın kaç anahtar tutması gerekecektir?

**6.** MAC’ler mesaj asıllama için kullanılabilirler. Bu problem ile biri MAC diğeri sayısal imza kullanan iki protokol arasındaki farkı görmek istiyoruz. Aşağıda her iki protokol için gönderici tarafın yaptığı işlem verilmiştir.

***Protokol 1:***

 C = Ek1 [ m || H(k2 || m) ]

(m mesaj, H hash örneğin SHA-1, E bir ortak anahtar şifreleme algoritması, || ekleme/concatenation, k1 ve k2 sadece gönderici ve alıcının bildiği ortak anahtarlar)

***Protokol 2:***

 C = Ek [ m || SA (H(m) ) ]

(m mesaj, H hash örneğin SHA-1, E bir ortak anahtar şifreleme algoritması, || ekleme/concatenation, SA göndericinin özel imza (*private*) anahtarı ile imzalama işlemi, k sadece gönderici ve alıcının bildiği ortak anahtar)

Şifrelenmiş mesaj C’yi aldığında alıcı tarafın yapması gereken işlemleri, her iki protokol için, adım adım açıklayınız.