**UBI523 Kriptosistemler ve Kriptoprotokoller**

**FİNAL SINAVI**

**15 Ocak 2015**

**Kapalı kitap/notlar. Her soru 20 puan. Dilediğiniz 5 soruyu yanıtlayınız.**

**Süre 120 dakika.**

**1.** Aşağıdaki terimleri/standartları ve kullanım alanlarını açıklayınız.

 **a)** Feistel Network **b)** CBC mode

 **c)** PKI, X.509 **d)** DSS, DSA

**2.** RSA kripto-sisteminin dikkatsiz kullanımı ile protokol hataları doğabilir. İşte bir örnek:  olacak şekilde her bir karakter bir sayı ile ifade edilip, sonrada bu sayıların her birisi kendi başına RSA ile şifrelenip alıcıya gönderilmektedir.

 **a)** Bu mesajlara erişimi olan bir üçüncü kişi RSA anahtarını bilmeden bu mesajları nasıl kolaylıkla çözebilir? Açıklayınız.

 **b)** N =18721, e=25 ve şifreli mesaj 6400, 1375, 1759, 1759, 17173, 17173

 ise açık mesajı bulunuz.

 *İpucu*: mod 18721`de (5^5)^5=1759, 14^25=1375, 2^50=17173

**3. a)** Bu problemde simetrik ve asimetrik kripto-sistem algoritmalarının işlemsel (*computational*) performanslarını karşılaştırmak istiyoruz. ElGamal algoritmasının modern bir PC’de 500 Kbit/sn hızında çözme (*decryption*) işlemi yapabildiğini varsayalım. Aynı makinada, AES algoritması ise 16 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 250 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?

**4. a)** Diffie-Hellman Anahtar Değişim (DHKE) Protokolünü bir şema üzerinde anlatınız.

**b)** Zp\*’da DHKE protokolünün 80 bit simetrik şifrelemeye eşdeğer güvenli olabilmesi için p’nin uzunluğu ne kadar olmalıdır?

**c)** b) şıkkını 128 bit simetrik şifrelemeye eşdeğer güvenlik için yeniden çözünüz.

**5. a)** Gönderici (veya mesaj) asıllama (*authentication*) daima veri bütünlüğünü sağlar mı? Açıklayınız.

**b)** Veri bütünlüğü her durumda gönderici (veya mesaj) asıllama sağlar mı? Açıklayınız.

**6.** Aşağıda **akım (stream)** şifreleme ile bütünlük koruması (*integrity*) için iki farklı yöntem önerilmektedir.

**a)** h**( )** bir hashfonksiyonu, || ekleme (concatenation) , M açık mesaj olmak üzere şifreli mesaj aşağıdaki gibi oluşturuluyor olsun.

 C = E**k**( M || h(M)) || M

Bu yöntem bilinen açık-metin (*known plaintext*) saldırısına karşı güvenli değildir. Bir saldırgan açık-metin M yerine onunla aynı uzunlukta başka bir mesaj M’ için alıcı tarafta bütünlük kontrolünden geçecek bir akım şifrelimetin C’= Ek( M’ || h(M’)) || M’ oluşturabilir. Bu saldırıyı adım adım anlatınız.

**b)** a) şıkkındaki saldırı hash fonksiyonunu aşağıdaki MAC fonksiyonu ile değiştirirsek hala geçerli (uygulanabilir) midir? Açıklayınız.

C = E**k1**( M || MAC**k2**(M)) || M