**UBI523 Kriptosistemler ve Kriptografik Protokoller**

**ARASINAV**

**12 Kasım 2018**

**Bir A4 yardım kağıdı. Dilediğiniz 5 soruyu yanıtlayınız.**

**Süre 120 dakika**

**1.** Elimizde aşağıdaki çözme (*decryption*) denklemine sahip bir “*affine-cipher*” var.

E-1(*y*) = *x* = 11 (y – 8) mod 26 (*y* şifrelimetin, *x* açıkmetin)

1. (10 p) Bu şifreleme sistemi için şifreleme (*encryption*) fonksiyonunu yazınız.
2. (15 p) Bu “affine-cipher” ı kullanarak aşağıdaki mesajı şifreleyiniz.

HAPPINESS IS WITHIN YOU

**2.** Bir dosya şifreleme programı 56-bit anahtarlı DES kullanmakta ve bu programda kullanıcıların DES anahtarları 8 karakterden oluşan parola (*password*) lardan üretilmektedir. Yani anahtar ardarda sıralanmış 8 x 8 = 64 bit uzunluğunda 8 ASCII karakterden oluşmaktadır. DES’in anahtar izlencelemesinde (*key scheduling*) her karakterin en az anlamlı (LSB) bit’i atılarak 56 bit anahtar elde edilmektedir. Elimizde saniyede 109 DES şifreleme/çözme işlemi yapabilen bir PC olsun. Aşağıdaki durumların her biri için, anahtar uzayı büyüklüğünü ve bir DES anahtarını bulmak için ortalama arama süresini hesaplayınız. Arama süresi sonuçlarını saniye cinsinden veriniz.

**a)** Sekiz karakterin hepsi rastgele seçilen ASCII karakterlerdir.

**b)** Sekiz karakterin hepsi rastgele seçilen büyük veya küçük harf ASCII karakterlerdir.

**c)** Sekiz karakterin hepsi rastgele seçilen 7-bit ASCII (en anlamlı bit (MSB) daima sıfır) karakterlerdir.

**3. (AES) a)** Ekte verilen Tablo 4.2’yi kullanarak onaltılı (*hexadecimal*) notasyondaki 57 ve 0B değerlerinin terslerini bulunuz.

**b)** (0B)’yı GF(28) ‘de bulduğunuz tersi ile çarparak sonucunuzu doğrulayınız. GF(28)’de çarpma yapmak için önce sayıları polinomlara çeviriniz. Her sayının MSB’si x7 katsayısını temsil eder.

**4.** Aşağıdaki soruları kısaca yanıtlayınız.

**a)** Kriptografide *Kerckhoff‘s Principle* nedir?

**b)** “*Non-deterministic encryption*” nedir? Tek kullanımlık şifreleme (*one time pad*) non-deterministic şifreleme midir?

**c)** DES-Xnedir? Blok diyagramını çiziniz; blok büyüklüğü ve anahtar büyüklüklerini diyagram üzerinde işaretleyiniz.

**d)** “Akış şifreleme (*stream ciphers*)” ile “blok şifreleme (*block ciphers*)” arasındaki farklar nelerdir?

**5.** PCBC (*Propagating Cipher Block Chaining*) standart DES modlarından CBC nin bir varyasyonudur. Burada şifreleme fonksiyonu aşağıda verilmiştir:

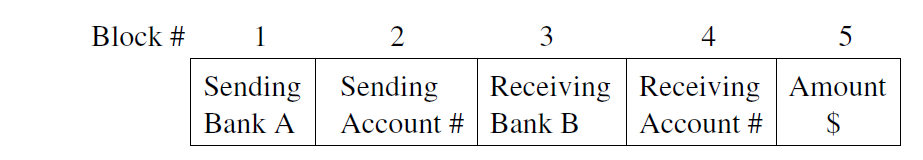
 birinci blok için (IV: initial vector)

 ikinci ve sonraki bloklar için

**a)** PCBC için deşifreleme fonksiyonunu yazınız.

**b)** İletim sırasında Ci’nci bloğun bozulduğunu varsayalım. Bu hata alıcı tarafta (deşifreleme sırasında) hangi plaintext bloklarını etkiler? Açıklayınız.

**6.** ECB modu ikame saldırısına (ing. *substitution attack*) açıktır. Bankalar arasında para transferinin aşağıdaki sahalara sahip elektronik mesajlar ve ECB modunda AES şifreleme aracılığıyla yapıldığını ve her bir sahanın bir blok (128 bit) uzunluğunda olduğunu varsayalım. Bankalar arasındaki şifreleme anahtarlarının haftada bir değiştiğini varsayalım.



Saldırının başlangıç adımları aşağıdadır.

1. Saldırgan, Oscar, A ve B bankalarında birer hesap açar.
2. Oscar bankalararası şifrelenmiş iletişim ağını dinlemenin bir yolunu bulur.
3. Oscar A bankasındaki hesabından B bankasındaki hesabına 1$’lık transferler yapar ve yeterince gözlem yaparak kendi transferlerini diğer para transferlerinden ayırabilecek noktaya gelir. Oscar aşağıdaki şifreli mesajın kendisinin gönderdiği bir transfere ait olduğunu belirlemiş olsun.

Blok #1 0C4CF34D219E55FA5D6622EA6708DC2A

Blok #2 92DE4A528FF35D1ECC08843E80BFBB31

Blok #3 135E60B532A706E2FA481B3067AA18C4

Blok #4 B402A56E071C924B31D18FC02A67E3D1

Blok #5 D0F3A21A7DE66C00B45A1D8F35619F02

Oscar daha sonra aşağıda verilen ve başkasına ait bir transfer üzerinde nasıl bir değişiklik yaparak bu transferrin kendi hesabına aktarılmasını sağlar? Değiştirilmiş transferin 5 bloğunu da yanıtınızda açık olarak gösteriniz.

Blok #1 0C4CF34D219E55FA5D6622EA6708DC2A

Blok #2 F03496255DAE1904A5B280A27F63F380

Blok #3 135E60B532A706E2FA481B3067AA18C4

Blok #4 1ECC08843E80BFBB31B402A56E071C92

Blok #5 BE31D18F8C02A67E3D18D01F3A21CA7D

