**UTI523 Kriptosistemler ve Kriptografik Protokoller**

**ARASINAV**

**18 Kasım 2014**

**Kapalı Kitap/Notlar. Dilediğiniz 5 soruyu yanıtlayınız.**

**Süre 150 dakika**

**1.** Yukardaki şifreli mesaj kaydırmalı şifreleme (ing. *shift cipher*) ile üretilmiş olup açık metin İngilizcedir.

IQZAI UZFDA PGOQM ZAFTQ DTUEF ADUOM XOUBT QDFTQ ETURF OUBTQ DUFUE MOFGM XXKME BQOUM XOMEQ ARFTQ EGNEF UFGFU AZOUB TQDMZ PTMEM HQDKQ XQSMZ FYMFT QYMFU OMXPQ EODUB FUAZF TQETU RFOUB TQDUF EQXRU EQJFD QYQXK EUYBX QIQET URFQH QDKBX MUZFQ JFXQF FQDNK MRUJQ PZGYN QDARB AEUFU AZEUZ FTQMX BTMNQ F

1. Kaydırmalı şifrelemede anahtarı (kaydırma miktarı) nasıl bulursunuz? Açıklayınız.
2. Yukardaki şifreli metin için anahtarı bulunuz.
3. Açık metnin ilk 30 karakterini bulunuz.

**İpucu**: Yukardaki şifreli metinde en fazla geçen harf Q’dur.

**2**. P={a,b}, C={1,2,3} ve K={k1, k2, k3 } olan ve şifreleme fonksiyonu aşağıdaki şifreleme matrisi tarafından tanımlanan bir kriptosistem düşünelim.

|  |  |  |
| --- | --- | --- |
|  | a | b |
| k1 | 3 | 1 |
| k2 | 2 | 3 |
| k3 | ? | 2 |

 p(a) = 2/3

 p(b) = 1/3

 p(k1) = p(k2) = p(k3)

1. ? = 1 için bu kriptosistemi *perfect secrecy* açısından değerlendiriniz.
2. ? = 3 için bu kriptosistemi *perfect secrecy* açısından değerlendiriniz.

**3.** 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.

**4.** 192 bit anahtar kullanılan AES için saniyede 108 anahtarı test edebilecek bir ASIC yonga olsun.

**a)** Bu türden 100.000 yongayı anahtar araması için parallel olarak kullanabildiğimizi varsayalım. Bu arama ortalama kaç yıl surer?

**b)** Moore yasası her 18 ayda bir aynı paraya 2 kat hızlı hesaplama yapabilen cihazlarımızın olacağını söyler. Buna göre 192 bit anahtarlı AES için anahtar aramasını 2 saatte tamamlayabilmek için kaç yıl geçmesi gerekir? Açıklayınız.

**5.** İki farklı anahtar kullanan 2-DES’i, k=56 olmak üzere, yaklaşık 2k şifreleme ve 2k bellek hücresi kullanarak kıran bir saldırı mevcuttur.

1. Bu saldırıyı tüm adımlarıyla açıklayınız.
2. Bu saldırıda bulunacak (k1,k2) anahtar ikilisinin yanlış anahtar olma olasılığını yeterince küçültmek için kaç adet (x,y) açıkmetin – şifrelimetin çiftine ihtiyaç vardır?

**6.** Aşağıdaki sorularda sonucu ve yaptığınız işlemleri gösteriniz.

**a)** obeb (268, 901) = ?

**b)** 19-1 mod 178?

**c)** $∅\left(242\right)= ?$

**d)** 178 $≡ ?mod 20$ (İpucu: $∅\left(20\right)=8$**)**