MAT 421 - Şifreleme Bilimine Giriş *Teslim tarihi: 18 Mart, 2015*

Ödev II

Problem 1

a) RSA açık anahtarı $(67, 2047)$ yi kullanarak, gruptaki tüm öğrenci isimlerini şifreleyiniz. (blok uzunluğuna dikkat ediniz).

b) RIZA kapalı metnini deşifre ediniz.

c) mod 2047 ye göre kendisinin tersi olan anahtarları bulunuz. $((x^e)^e \equiv x \bmod 2047)$

Problem 2

Semih ve İlhami Elgamal şifre sistemini kullanmak istemektedirler. ElGamal şifre sisteminin parametreleri $(p = 1153, \alpha = 5)$ olarak seçilmiştir. Semih'in gizli anahtarı $a = 129$ ve İlhami'nin gizli anahtarı ise "i" olarak belirlenmiştir. İlhami açık anahtarının $(1153, 5, 205)$ olduğunu beyan etmiştir.

a) Semih'in açık anahtarını bulunuz.

b) Açık metinlerdeki ve kapalı metinlerdeki blokların uzunluğu nedir?

c) Semih, İlhami'ye NO mesajını şifreli olarak göndermek istiyor. Şifreli metin nedir?

d) İlhami'nin gizli anahtarını bulunuz.

Problem 3

Aşağıdaki süper artan diziyi kullanarak bir knapsack şifreleme sistemi tasarlayınız.

$$3, 7, 11, 24, 49, 96, 200, 391, 784, 1575.$$

26 harfli İngiliz alfabesini kullanarak gruptaki tüm öğrenci isimlerini şifreleyiniz.

Problem 4

n pozitif bir tek sayı olsun.

a) n nin "$\sqrt{n}$ ye eşit ve daha büyük bütün bölenleri" ile "$n = s^2 - t^2$ denklemini sağlayan (s,t) ikilileri" arasında $1-1$ bir ilişki olduğunu ispatlayınız.

b) 945 sayısını, iki tamsayının karelerinin farkı olarak kaç değişik şekilde yazabiliriz?

Problem 5

Grubunuzdaki öğrenci numaralarından en büyük olan numaranın son rakamına göre a sayısını aşağıdaki gibi seçin:

(0) 38321	(1) 38449	(2) 38609	(3) 38737	(4) 38833
(5) 38993	(6) 39089	(7) 39817	(8) 39313	(9) 39409

Aynı öğrenci numarasının 7. rakamına göre n sayısını aşağıdaki gibi seçin:

(0) 356371021	(1) 379212941	(2) 379663597	(3) 379320649	(4) 379658737
(5) 379859189	(6) 380141329	(7) 380197757	(8) 380310613	(9) 390550933

mod n ye göre $x > a$ şartını sağlayan en küçük x tam karesini bulunuz. $x \equiv b^2 \bmod n$ olan bütün b sayılarını bulunuz.

Problem 6

$S(n)$ hipotezi aşağıdaki gibi tanımlansın:

$S(n)$: "OBEB$(b,n) = 1$ olmak üzere verilen b sayısı için eğer $b^{\phi(n)/2} \equiv 1 \bmod n$ ise b mod n ye göre quadratik residü olur. "

a) $S(n)$ hipotezini sağlamayan bir n sayısı bulunuz.

b) $S(18)$ in doğru olduğunu gösteriniz.

c) $S(n)$ doğrudur ancak ve ancak $\phi(n) \equiv 2 \bmod 4$ ifadesini ispatlayınız veya aksine bir örnek bulunuz.

Problem 7

SHA-1 veya MD-5 özet (hash) fonksiyonlarından birinin detaylarını yazınız.