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

Ödev I

Problem 1

İngiliz alfabesi kullanılarak oluşturulan

a) Kaydırmalı, Atlamalı ve Afin şifreleme sistemlerindeki geçerli anahtar sayılarını bulunuz.

b) "Kriptografik" açık metnini,

i) Playfair şifreleme sistemini ve "matematik" anahtarını kullanarak şifreleyiniz.

ii) Vigenere şifreleme sistemini ve "mat" anahtarını kullanarak şifreleyiniz.

Problem 2

$p(x) = x^4 + x^3 + 1$ ve $q(x) = x^4 + x^3 + x^2 + x + 1$ polinomlarını kullanarak $2^4 = 16$ elemanlı cisimleri bulunuz. Bu cisimlerin neden izomorfik olduğunu açıklayınız.

Problem 3

a) $\mathbb{F}_2$ sonlu cismi üzerinde $x^5 + x + 1$ polinomu indirgenebilir midir? Neden?

b) $\mathbb{F}_2$ sonlu cismi üzerinde $x^5 + x^2 + 1$ polinomu indirgenebilir midir? Neden?

c) 32 elemanlı bir cisim bulunuz ve elemanlarını yazınız.

Problem 4

Euclid algoritmasını kullanarak aşağıdaki işlemleri yapınız.

a) $obeb(x^4 + x^2 + 1, x^2 + 1) = ?$

b) $obeb(x^4 - 4x^3 + 6x^2 - 4x + 1, x^3 - x^2 + x - 1) = ?$

Problem 5

Aşağıdaki denklem sistemlerinin çözümünü bulunuz. (En küçük negatif olmayan x tamsayısını bulun).

a) $\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \\ x \equiv 4 \mod 11 \\ x \equiv 5 \mod 16 \end{cases}$ b) $\begin{cases} x \equiv 12 \mod 31 \\ x \equiv 87 \mod 127 \\ x \equiv 91 \mod 255 \end{cases}$ c) $\begin{cases} 19x \equiv 103 \mod 900 \\ 10x \equiv 511 \mod 841 \end{cases}$

Problem 6

$\phi(n) \leq 18$ olan bütün n sayılarını bulunuz.

Problem 7

Mert ve Kadri gizli mesaj alışverişinde bulunmak için 3×3 şifreleme matrislerini kullanmak üzere anlaşmaya varıyorlar.

a) Kadri, Mert'in nerede bulunduğunu öğrenmek istiyor. Mert cevap olarak CANAKKALE açık metnini UAMOIXFGT anahtarını kullanarak şifreliyor ve kapalı metni gönderiyor. Kadri'ye ulaşan metni bulunuz.

b) Kadri LUBRAFRSH mesajını alıyor ve metni deşifre ederken tereddüte düşüyor. Neden? Kadri mesajı nasıl çözebilir? Açık metin nedir?

Not: Anahtar 123456789 $\left(K = \begin{bmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{bmatrix} \right)$ ve açık metin 987654321 $\left(P = \begin{bmatrix} 9 & 6 & 3 \\ 8 & 5 & 2 \\ 7 & 4 & 1 \end{bmatrix} \right)$ ise kapalı metin $C = KP \pmod{26}$ dan elde edilir.

Problem 8

26 harfli İngiliz alfabesi ve şifreleme fonksiyonu olarak $F_k(x) = kx^k + k \pmod{26^3}$ kullanılarak üç harfi üç harfe götüren bir şifre sistemi tasarlanmıştır.

a) Geçerli anahtarların sayısını bulunuz.

b) Deşifre işlemini açıklayınız.

c) Uygun bir anahtar seçerek adlarınızı (Ad1+Ad2+Ad3) şifreleyiniz. Deşifre fonksiyonunu belirtiniz.

Problem 9

Aşağıdaki kapalı metnin Vigenere şifreleme sistemi kullanılarak elde edildiği bilinmektedir.

APGNU YFLPS WBVTL ZLHIT FLLSP VVCSW JLQLJ WBWWO EWAPA GUFSA WXVZR WOWVZ SSMBO ZMGFK LAMID CGLAS GRVOB QHFSE RHVVU SXYUP ALQIY MBOAW CCAPW KSNCY MEBGK YRMKT BUDYC KMFRR PWFTZ FLNBZ XKRWO WVZSY YKIUE SRPCQ KBCEJ PSWTB PYYBA LHCMV SAGUR RYIOF OKCYQ SEGZL DPSMV VAVCD WOTAV UHEWJ FOMOT GRLHB MWIIL ZXAMQ YCYAN TGVQH VVCIX QPBAL VRPKB GBARE PVWAC UELWF EMUMP VYMVZ QMWJT TVUFM SKGTM STWVH FPZKG FSWPV UEBZV QHKJH GJQAI LXGKM WCJVV RQLBZ XIEGX CWECF IVNZH RXCZE GKYYG ZXGII CYYAA ZBRRB ZWLHP JLBZX TRALR MZGRP LVGPY EMDVT XMFLK PALJR JLPGF SNFLV ZXIEJ LIKAS UFPAU KSRRP DAMMW YJMKP CLJKN GKAKF VAWHT RLPUS EGGCV XDXOE BTICX PVJPM NXGWG LVVBG YDHKW LKZRO LWOWC FVZFL QYGUI HEOKC AMWMV NGAPK XFGCU BKPFR NWMVT FFSUL KICLR ZVGKS CGNQG NGDCZ ASZSY CYMBN GKYMI UXOJG UIUHA ZAZBJ BDKFH BZTGS CJWEX CECVN ZHRXC ZBJTR VKHZC LVZQK MKBUE QMZGF VZQOC EUZVQ ACVBC RPLAU THKCY MVTFF S

Bu durumda

a) Anahtar uzunluğunu bulunuz.

b) Anahtarı bulunuz.

c) Metni deşifre ediniz.

Problem 10

Trivium ve RC4 akan şifre algoritmalarının detaylarını açıklayınız.

Problem 11

Boyu 10 ve bağlantı polinomu $f(x) = x_1 + x_2 + x_5 + x_8 + x_{10}$ olan bir LFSR, bir öğrenci numarasının son iki rakamının 2-lik gösterimi anahtar olarak kullanılarak dolduruluyor. Adlarınızı (Ad1+Ad2+Ad3) bu LFSR yi kullanarak şifreleyiniz.

Problem 12

Boyları 2, 3, 5 ve bağlantı polinomları $f_1(x) = x_1 + x_2$, $f_2(x) = x_1 + x_3$ ve $f_3(x) = x_1 + x_3 + x_5$ olan üç LFSR, $g(x) = x_1 + x_3 + x_2x_3$ fonksiyonu ile kombine ediliyor. Bir öğrenci numarasının son iki rakamını anahtar olarak kullanarak adlarınızı (Ad1+Ad2+Ad3) bu sistemle şifreleyiniz.