MAT 421 - Şifreleme Bilimine Giriş *Teslim tarihi: 18 Şubat, 2014*

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.

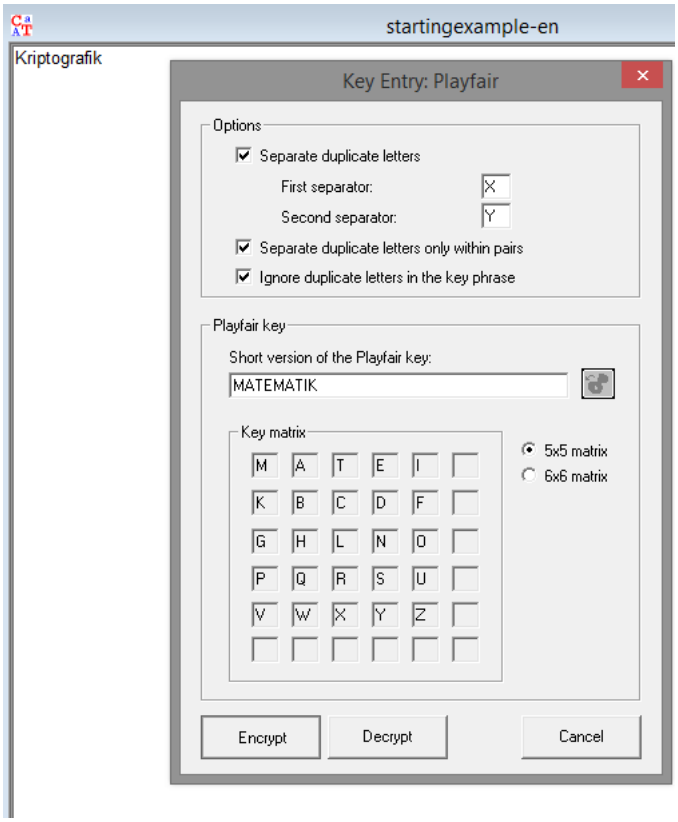
Çözüm:

a) i) Kaydırmalı sistemde çözerken sadece çıkarma işlemi yaptığımız için bütün olabilecek anahtarlar geçerlidir. ($P \equiv C - K \mod 26$) Dolayısıyla anahtar sayısı 26 dır. (Dejenere durum olan $K = 0$ durumunu da saydık).

   ii) Atlamalı sistemde ise $P \equiv C \cdot K^{-1} \mod 26$ şeklinde deşifre edildiğinden K anahtarınının $\mod 26$ da tersi söz konusu olup bu durumda anahtarlar 26 ile aralarında asal olan sayılar olabilir. Yani istenilen sayı $\phi(26) = (2-1)(13-1) = 12$ dir.

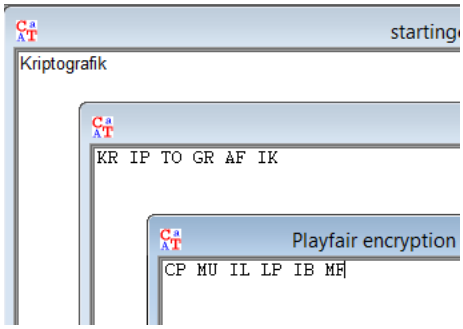
   iii) Afin şifreleme sistemi ise kaydırmalı ve atlamalı sistemlerin birleşimi olduğundan $(P \equiv (C - K_1)K_2^{-1} \mod 26)$ cevap $12 \cdot 26 = 312$ dir.

b) i) Playfair kripto sisteminde bir anahtar matrisi oluşturuyoruz. Bu matrisi oluştururken anahtarımızın her bir harfini yanlız bir kere kullanarak, geri kalan harfleri a,b,c,.... sırası ile yerleştiriyoruz. Matriste dikkat edilmesi gereken nokta harfler yanlız birkere kullanılmalıdır. Aşağıda cryptool ile, matematik anahtarı için oluşturulmuş anahtar matrisi yer almaktadır. (Şekil: 1)



Şekil 1: Playfair ile Şifreleme

Encrypt dediğimiz zaman sistem ilk olarak açık metni ikili gruplar haline getiriyor ve matris üzerinde playfair algoritmasını uygulayarak, metni şifreliyor. (Şekil 2)



Şekil 2: Şifreli Metin CP MU IL LP IB MF

olup şifreli metin CPMUILLPIBMF bulunur.

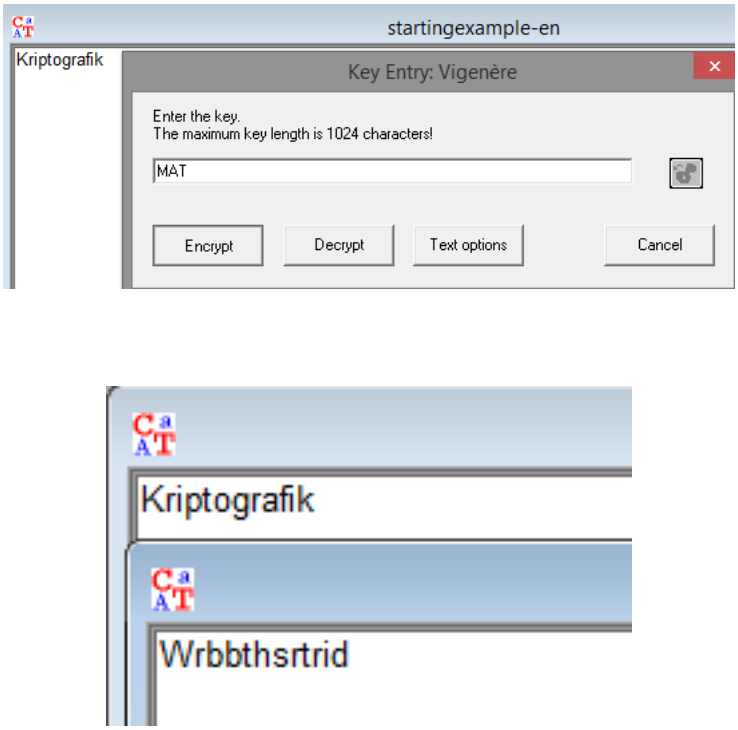
ii) Vigenere sisteminde açık metinin uzunluğu kadar anahtar arka arkaya yazılır.

Ardından düz metin ile toplanır. (İlgili mod'da toplanır. Bizim durumda mod 26'da) (Şekil 3)

K	R	I	P	T	O	G	R	A	F	I	K
M	A	T	M	A	T	M	A	T	M	A	T
W	R	B	B	T	H	S	R	T	R	I	D

Şekil 3: Vigere İşlem Tablosu

Bu işlemleri Cryptoolda yaptıracak olursak aşağıdaki gibi elde ederiz (Şekil: (4)):



Şekil 4: Vigenere İle Şifreleme

olup şifreli metin WRBBTHSRTRID bulunur.

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.

Çözüm: $p(x)$ polinomunun bir kökü x olmak üzere x in kuvvetlerine bakacak olursak $\{x^i \mid i = 0, 1, \ldots, 14\} = \{1, x+1, x^2+1, x^3+x^2+x+1, x^3+x^2+x, x^3+x^2+1, x^3, x^2+x+1, x^3+1, x^2, x^3+x^2, x^3+x+1, x, x^2+x, x^3+x\}$ elde ederiz. Görüldüğü gibi x in sadece 0. ve 15. kuvvetleri 1 vermektedir. Dolaısıyla x elemanının mertebesi 15 olup, $\mathbb{F}_{2^4}^*$ kümesinin bir üretecidir veya $\mathbb{F}_{2^4}$ cisminin bir ilkel(primitive) elemanıdır.

$q(x)$ polinomunun bir kökü y olmak üzere y nin kuvvetlerine bakacak olursak $\{y^i \mid i = 0, 1, \ldots, 14\} = \{1, y, y^2, y^3, y^3+y^2+y+1, 1, y, y^2, y^3, y^3+y^2+y+1, 1, y, y^2, y^3, y^3+y^2+y+1\}$ olup y nin 1 verdiği ilk kuvvet 5 olup, y nin mertebesi 5 tir, yani y bir üreteç değildir. Benzer şekilde $y+1$ elemanının kuvvetine bakacak olursak: $\{(y+1)^i \mid i = 0, 1, \ldots, 14\} = \{1, y+1, y^2+1, y^3+y^2+y+1, y^3+y^2+y, y^3+y^2+1, y^3, y^2+y+1, y^3+1, y^2, y^3+y^2, y^3+y+1, y, y^2+y, y^3+y\}$ olup $y+1$ elemanının bir üreteç olduğunu görebiliriz. Bu durumda x elemanını $y+1$ elemanına ve kuvvetlerini de kuvvetlerine götürecek şekilde işlem tanımlarsak $p(x)$ ve $q(x)$ polinomları ile elde edilen cisimlerin izomorfik olduğunu görebiliriz. Aşağıda iki cismin çarpmaya göre işlemleri verilmiştir. (Sayfa 5 ve 6)

İkinci bir çözüm olarak verilen bir sayı kadar elemana sahip cismin tek olduğu teoremin ispatı verilebilir.

Çarpmaya Göre İşlem Tablosu ($p(x)$ polinomu):

$*$	0	1	x	x^2	x^3	x^3+1	x^3+x+1	x^3+x^2+x+1	x^2+x+1	x^3+x^2+x	x^2+1	x^3+x	x^3+x^2+1	$x+1$	x^2+x	x^3+x^2
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	x	x^2	x^3	x^3+1	x^3+x+1	x^3+x^2+x+1	x^2+x+1	x^3+x^2+x	x^2+1	x^3+x	x^3+x^2+1	$x+1$	x^2+x	x^3+x^2
x	0	x	x^2	x^3	x^3+1	x^3+x+1	x^3+x^2+x+1	x^2+x+1	x^3+x^2+x	x^2+1	x^3+x	x^3+x^2+1	$x+1$	x^2+x	x^3+x^2	1
x^2	0	x^2	x^3	x^3+1	x^3+x+1	x^3+x^2+x+1	x^2+x+1	x^3+x^2+x	x^2+1	x^3+x	x^3+x^2+1	$x+1$	x^2+x	x^3+x^2	1	x
x^3	0	x^3	x^3+1	x^3+x+1	x^3+x^2+x+1	x^2+x+1	x^3+x^2+x	x^2+1	x^3+x	x^3+x^2+1	$x+1$	x^2+x	x^3+x^2	1	x	x^2
x^3+1	0	x^3+1	x^3+x+1	x^3+x^2+x+1	x^2+x+1	x^3+x^2+x	x^2+1	x^3+x	x^3+x^2+1	$x+1$	x^2+x	x^3+x^2	1	x	x^2	x^3
x^3+1	0	x^3+1	x^3+x+1	x^3+x^2+x+1	x^2+x+1	x^3+x^2+x	x^2+1	x^3+x	x^3+x^2+1	$x+1$	x^2+x	x^3+x^2	1	x	x^2	x^3
x^3+x^2+x+1	0	x^3+x^2+x+1	x^2+x+1	x^3+x^2+x	x^2+1	x^3+x	x^3+x^2+1	$x+1$	x^2+x	x^3+x^2	1	x	x^2	x^3	x^3+1	x^3+x+1
x^2+x+1	0	x^2+x+1	x^3+x^2+x	x^2+1	x^3+x	x^3+x^2+1	$x+1$	x^2+x	x^3+x^2	1	x	x^2	x^3	x^3+1	x^3+x+1	x^3+x^2+x+1
x^3+x^2+x	0	x^3+x^2+x	x^2+1	x^3+x	x^3+x^2+1	$x+1$	x^2+x	x^3+x^2	1	x	x^2	x^3	x^3+1	x^3+x+1	x^3+x^2+x+1	x^2+x+1
x^2+1	0	x^2+1	x^3+x	x^3+x^2+1	$x+1$	x^2+x	x^3+x^2	1	x	x^2	x^3	x^3+1	x^3+x+1	x^3+x^2+x+1	x^2+x+1	x^3+x^2+x
x^3+x	0	x^3+x	x^3+x^2+1	$x+1$	x^2+x	x^3+x^2	1	x	x^2	x^3	x^3+1	x^3+x+1	x^3+x^2+x+1	x^2+x+1	x^3+x^2+x	x^2+1
x^3+x^2+1	0	x^3+x^2+1	$x+1$	x^2+x	x^3+x^2	1	x	x^2	x^3	x^3+1	x^3+x+1	x^3+x^2+x+1	x^2+x+1	x^3+x^2+x	x^2+1	x^3+x
$x+1$	0	$x+1$	x^2+x	x^3+x^2	1	x	x^2	x^3	x^3+1	x^3+x+1	x^3+x^2+x+1	x^2+x+1	x^3+x^2+x	x^2+1	x^3+x	x^3+x^2+1
x^2+x	0	x^2+x	x^3+x^2	1	x	x^2	x^3	x^3+1	x^3+x+1	x^3+x^2+x+1	x^2+x+1	x^3+x^2+x	x^2+1	x^3+x	x^3+x^2+1	$x+1$
x^3+x^2	0	x^3+x^2	1	x	x^2	x^3	x^3+1	x^3+x+1	x^3+x^2+x+1	x^2+x+1	x^3+x^2+x	x^2+1	x^3+x	x^3+x^2+1	$x+1$	x^2+x

Çarpmaya Göre İşlem Tablosu ($q(x)$ polinomu):

$*$	0	1	$y+1$	y^2+1	y^3+y^2+y+1	y^3+y^2+y	y^3+y^2+1	y^3	y^2+y+1	y^3+1	y^2	y^3+y^2	y^3+y+1	y	y^2+y	y^3+y
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	$y+1$	y^2+1	y^3+y^2+y+1	y^3+y^2+y	y^3+y^2+1	y^3	y^2+y+1	y^3+1	y^2	y^3+y^2	y^3+y+1	y	y^2+y	y^3+y
$y+1$	0	$y+1$	y^2+1	y^3+y^2+y+1	y^3+y^2+y	y^3+y^2+1	y^3	y^2+y+1	y^3+1	y^2	y^3+y^2	y^3+y+1	y	y^2+y	y^3+y	1
y^2+1	0	y^2+1	y^3+y^2+y+1	y^3+y^2+y	y^3+y^2+1	y^3	y^2+y+1	y^3+1	y^2	y^3+y^2	y^3+y+1	y	y^2+y	y^3+y	1	$y+1$
y^3+y^2+y+1	0	y^3+y^2+y+1	y^3+y^2+y	y^3+y^2+1	y^3	y^2+y+1	y^3+1	y^2	y^3+y^2	y^3+y+1	y	y^2+y	y^3+y	1	$y+1$	y^2+1
y^3+y^2+y	0	y^3+y^2+y	y^3+y^2+1	y^3	y^2+y+1	y^3+1	y^2	y^3+y^2	y^3+y+1	y	y^2+y	y^3+y	1	$y+1$	y^2+1	y^3+y^2+y+1
y^3+y^2+1	0	y^3+y^2+1	y^3	y^2+y+1	y^3+1	y^2	y^3+y^2	y^3+y+1	y	y^2+y	y^3+y	1	$y+1$	y^2+1	y^3+y^2+y+1	y^3+y^2+y
y^3	0	y^3	y^2+y+1	y^3+1	y^2	y^3+y^2	y^3+y+1	y	y^2+y	y^3+y	1	$y+1$	y^2+1	y^3+y^2+y+1	y^3+y^2+y	y^3+y^2+1
y^2+y+1	0	y^2+y+1	y^3+1	y^2	y^3+y^2	y^3+y+1	y	y^2+y	y^3+y	1	$y+1$	y^2+1	y^3+y^2+y+1	y^3+y^2+y	y^3+y^2+1	y^3
y^3+1	0	y^3+1	y^2	y^3+y^2	y^3+y+1	y	y^2+y	y^3+y	1	$y+1$	y^2+1	y^3+y^2+y+1	y^3+y^2+y	y^3+y^2+1	y^3	y^2+y+1
y^2	0	y^2	y^3+y^2	y^3+y+1	y	y^2+y	y^3+y	1	$y+1$	y^2+1	y^3+y^2+y+1	y^3+y^2+y	y^3+y^2+1	y^3	y^2+y+1	y^3+1
y^3+y^2	0	y^3+y^2	y^3+y+1	y	y^2+y	y^3+y	1	$y+1$	y^2+1	y^3+y^2+y+1	y^3+y^2+y	y^3+y^2+1	y^3	y^2+y+1	y^3+1	y^2
y^3+y+1	0	y^3+y+1	y	y^2+y	y^3+y	1	$y+1$	y^2+1	y^3+y^2+y+1	y^3+y^2+y	y^3+y^2+1	y^3	y^2+y+1	y^3+1	y^2	y^3+y^2
y	0	y	y^2+y	y^3+y	1	$y+1$	y^2+1	y^3+y^2+y+1	y^3+y^2+y	y^3+y^2+1	y^3	y^2+y+1	y^3+1	y^2	y^3+y^2	y^3+y+1
y^2+y	0	y^2+y	y^3+y	1	$y+1$	y^2+1	y^3+y^2+y+1	y^3+y^2+y	y^3+y^2+1	y^3	y^2+y+1	y^3+1	y^2	y^3+y^2	y^3+y+1	y
y^3+y	0	y^3+y	1	$y+1$	y^2+1	y^3+y^2+y+1	y^3+y^2+y	y^3+y^2+1	y^3	y^2+y+1	y^3+1	y^2	y^3+y^2	y^3+y+1	y	y^2+y

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.

Çözüm:

a) $p(x) = x^5 + x + 1$ polinomunun $\mathbb{F}_2$ de kökleri olmadığından bu polinomun lineer bir çarpanı yoktur. Dolayısıyla ikinci ve üçüncü dereceden indirgenemez polinomların çarpımları şeklinde olabilir. Diğer taraftan $\mathbb{F}_2$ de ikinci dereceden tek indirgenemez polinom $x^2 + x + 1$ olduğundan $p(x)$ polinomu indirgenebilir ise $p(x) = (x^3 + ax^2 + bx + 1)(x^2 + x + 1)$ şeklindedir. Son eşitlikte çarpma işlemi yaparak polinom eşitlemesi yaparsak $a = 1$ ve $b = 0$ elde ederiz. Demek ki $p(x)$ polinomu indirgenebilirdir.

b) $q(x) = x^5 + x^2 + 1$ polinomu için de a) şıkkındaki yorumları yaparak $q(x) = (x^3 + ax^2 + bx + 1)(x^2 + x + 1)$ şeklinde yazabiliriz. Bu son eşitlikte çarpma işlemini yaparak polinom eşitlemesi yaparsak $a + b = 0$ ve $a + b = 1$ olup çelişki elde ederiz. Dolayısıyla $q(x)$ polinomu indirgenemezdir.

c) $q(x) = x^5 + x^2 + 1$ polinomu $\mathbb{F}_2[x]$ de indirgenemez olup $\langle x^5 + x^2 + 1 \rangle$ ideali $\mathbb{F}_2[x]$ halkasında maximaldir, dolayısıyla $\mathbb{F}_2[x]/\langle x^5 + x^2 + 1 \rangle$ bölüm halkası bir cisim oluşturur. Bu cisim $\{ax^4 + bx^3 + cx^2 + dx + e \mid a, b, c, d, e \in \mathbb{F}_2\}$ şeklinde olup 32 elemanlıdır.

Problem 4

Euclid algoritmasını kullanarak aşağıdaki işlemleri yapınız.

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

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

Çözüm:

a) $x^4 + x^2 + 1 = x^2(x^2 + 1) + 1$ olup bu iki polinom aralarında asaldır. Yani $obeb(x^4 + x^2 + 1, x^2 + 1) = 1$ dir.

b)

$$x^4 - 4x^3 + 6x^2 - 4x + 1 = (x - 3)(x^3 - x^2 + x - 1) + 2x^2 - 2$$
$$2(x^3 - x^2 + x - 1) = (x - 1)(2x^2 - 2) + 4x - 4$$
$$2(2x^2 - 2) = (x + 1)(4x - 4) + 0$$

olup bu iki polinomun *obeb*'i $4x-4$ veya $x-1$ dir. Not: burada işlemleri $\mathbb{Q}$ kümesinde yaptık.

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) $\begin{cases} 19x \equiv 103 \mod 900 \\ 10x \equiv 511 \mod 841 \end{cases}$

Çözüm:

a) $\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \\ x \equiv 4 \mod 11 \\ x \equiv 5 \mod 16 \end{cases}$ sisteminin çözümü $x = 3\cdot 5\cdot 11x_{16} + 3\cdot 5\cdot 16x_{11} + 3\cdot 11\cdot 16x_5 + 5\cdot 11\cdot 16x_3$ şeklindedir. Yani $x = 165x_{16} + 240x_{11} + 528x_5 + 880x_3$ olup geriye $\begin{cases} 880x_3 \equiv 2 \mod 3 \\ 528x_5 \equiv 3 \mod 5 \\ 240x_{11} \equiv 4 \mod 11 \\ 165x_{16} \equiv 5 \mod 16 \end{cases}$ sistemini çözmemiz gerekmektedir. Dolayısıyla $\begin{cases} x_3 \equiv 2 \mod 3 \\ x_5 \equiv 1 \mod 5 \\ x_{11} \equiv 9 \mod 11 \\ x_{16} \equiv 1 \mod 16 \end{cases}$ bulunur ve $x = 165\cdot 1 + 240\cdot 9 + 528\cdot 1 + 880\cdot 2 = 4613 \equiv 1973 \mod 3\cdot 5\cdot 11\cdot 16$ elde ederiz. Cevap 1973 tür.

b) $\begin{cases} x \equiv 12 \mod 31 \\ x \equiv 87 \mod 127 \\ x \equiv 91 \mod 255 \end{cases}$ sisteminin çözümü $x = 31\cdot 127x_{255} + 31\cdot 255x_{127} + 127\cdot 255x_{31}$ şeklindedir. Yani $x = 3937x_{255}+7905x_{127}+32385x_{31}$ olup geriye $\begin{cases} 3937x_{255} \equiv 91 \mod 255 \\ 7905x_{127} \equiv 87 \mod 127 \\ 32385x_{31} \equiv 12 \mod 31 \end{cases}$ sistemini çözmemiz gerekmektedir. Dolayısıyla $\begin{cases} x_{255} \equiv 208 \mod 255 \\ x_{127} \equiv 11 \mod 127 \\ x_{31} \equiv 5 \mod 31 \end{cases}$ bulunur ve $x = 3937\cdot 208+7905\cdot 11+32385\cdot 5 \equiv 63841 \mod 1003935$ elde ederiz. Cevap 63841 dir.

c) $\begin{cases} 19x \equiv 103 \mod 900 \\ 10x \equiv 511 \mod 841 \end{cases}$ sistemi ile $\begin{cases} x \equiv 103\cdot 379 \equiv 337 \mod 900 \\ x \equiv 511\cdot 757 \equiv 808 \mod 841 \end{cases}$ sistemi denktir. Son sistemin çözümü de $x = 841x_{900}+900x_{841}$ şeklinde olup geriye $\begin{cases} 841x_{900} \equiv 337 \mod 900 \\ 900x_{841} \equiv 808 \mod 841 \end{cases}$

sistemini çözmemiz gerekmektedir. Dolayısıyla $\begin{cases} x_{900} \equiv 757 \mod 900 \\ x_{841} \equiv 199 \mod 841 \end{cases}$ bulunur ve $x = 841 \cdot 757 + 900 \cdot 199 \equiv 58837 \mod 900 \cdot 841$ elde ederiz. Cevap 58837 dir.

Problem 6

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

Çözüm: ϕ fonksiyonunun formülünü hatırlayalım: $\phi(n) = \phi(p_1^{\alpha_1} p_2^{\alpha_2} \dots) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \dots$ dır. Burada p_i ler farklı asal sayılardır.

Soru iki farklı şekilde ele alınabilir. Birincisi $\phi(n)$ fonksiyonunu sırayla 18 tane sayıya eşitleyerek n leri bulabiliriz. İkincisi n sayısının farklı asal çarpanlarına göre $\phi(n)$ fonksiyonu hangi değerleri aldığını inceleyebiliriz. Bu çözümde ikinci yaklaşımı ele alacağız.

Birinci durum: n sayısı bir asalın kuvveti olsun

i) $p = 2$ ise n nin alabileceği değerler (ve $\phi(n)$ nin alabileceği değerler parantez içinde olmak üzere) aşağıdaki gibidir:
$2^1(2 - 1 = 1), 2^2(2^2 - 2^1 = 2), 2^3(2^3 - 2^2 = 4), 2^4(2^4 - 2^3 = 8), 2^5(2^5 - 2^4 = 16)$

ii) $p = 3$ ise $3^1(3 - 1 = 2), 3^2(3^2 - 3^1 = 6), 3^3(3^3 - 3^2 = 18)$

iii) $p = 5$ ise $5^1(5 - 1 = 4)$

iv) $p = 7$ ise $7^1(7 - 1 = 6)$

v) $p = 11$ ise $11^1(11 - 1 = 10)$

vi) $p = 13$ ise $13^1(13 - 1 = 12)$

vii) $p = 17$ ise $17^1(17 - 1 = 16)$

viii) $p = 19$ ise $19^1(19 - 1 = 18)$

İkinci durum: n sayısı iki tane asal sayı ile bölünebiliyor olsun. Bu durumda n nin alabileceği değerler aşağıdaki gibidir

i) n çift sayı ise
$2.3, 2^2.3, 2^3.3, 2^4.3, 2.3^2, 2^2.3^2, 2.3^3, 2.5, 2^2.5, 2^3.5, 2.7, 2^2.7, 2.11, 2.13, 2.17, 2.19$

ii) n tek sayı ise
$3.5, 3.7$

Üçüncü durum: n sayısı üç tane asal sayı ile bölünebiliyor olsun. Bu durumda n nin alabileceği değerler aşağıdaki gibidir

$2.3.5, 2.3.7, 2^2.3.5$

O halde n nin alabileceği sayıların kümesi { 1, 2, 4, 8, 16, 32, 3, 9, 27, 5, 7, 11, 13, 17, 19, 6, 12, 24, 48, 18, 36, 54, 10, 20, 40, 14, 28, 22, 26, 34, 38, 15, 21, 30, 42, 60 } dir.

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 $C = KP \ (\mod 26)$ dan elde edilir.

Çözüm: Harflere karşılık gelen sayılarımız aşağıdaki gibi olsun:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

V	W	X	Y	Z																
21	22	23	24	25																

a) Anahtarımız ve metnimizi sayılarla ifade edecek olursak $K = \begin{bmatrix} U & O & F \\ A & I & G \\ M & X & T \end{bmatrix} = \begin{bmatrix} 20 & 14 & 5 \\ 0 & 8 & 6 \\ 12 & 23 & 19 \end{bmatrix}$ ve $P = \begin{bmatrix} C & A & A \\ A & K & L \\ N & K & E \end{bmatrix} = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 10 & 11 \\ 13 & 10 & 4 \end{bmatrix}$ olup $C = KP = \begin{bmatrix} 1 & 8 & 18 \\ 0 & 10 & 8 \\ 11 & 4 & 17 \end{bmatrix} = \begin{bmatrix} B & I & S \\ A & K & I \\ L & E & R \end{bmatrix}$ veya şifreli metnimiz BALIKESIR bulunur.

b) Anahtarımız $K = \begin{bmatrix} 20 & 14 & 5 \\ 0 & 8 & 6 \\ 12 & 23 & 19 \end{bmatrix}$ ve Kadrinin aldığı mesaj LUBRAFRSH veya $C = \begin{bmatrix} L & R & R \\ U & A & S \\ B & F & H \end{bmatrix} = \begin{bmatrix} 11 & 17 & 17 \\ 20 & 0 & 18 \\ 1 & 5 & 7 \end{bmatrix}$ olup $P = \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & i \end{bmatrix}$ açık metni çözmek için $\begin{bmatrix} 11 & 17 & 17 \\ 20 & 0 & 18 \\ 1 & 5 & 7 \end{bmatrix} = \begin{bmatrix} 20 & 14 & 5 \\ 0 & 8 & 6 \\ 12 & 23 & 19 \end{bmatrix} \times \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & i \end{bmatrix}$ denklemini mod 26 da çözeceğiz.

Son eşitliği üç farklı denklem sistemi halinde düşünebiliriz:

$\begin{bmatrix} 11 \\ 20 \\ 1 \end{bmatrix} = \begin{bmatrix} 20 & 14 & 5 \\ 0 & 8 & 6 \\ 12 & 23 & 19 \end{bmatrix} \times \begin{bmatrix} a \\ b \\ c \end{bmatrix}$, $\begin{bmatrix} 17 \\ 0 \\ 5 \end{bmatrix} = \begin{bmatrix} 20 & 14 & 5 \\ 0 & 8 & 6 \\ 12 & 23 & 19 \end{bmatrix} \times \begin{bmatrix} d \\ e \\ f \end{bmatrix}$ ve $\begin{bmatrix} 17 \\ 18 \\ 7 \end{bmatrix} = \begin{bmatrix} 20 & 14 & 5 \\ 0 & 8 & 6 \\ 12 & 23 & 19 \end{bmatrix} \times \begin{bmatrix} g \\ h \\ i \end{bmatrix}$ şeklinde. Bunların ilkini detaylı ele alalım:

$$\begin{bmatrix} 11 \\ 20 \\ 1 \end{bmatrix} = \begin{bmatrix} 20 & 14 & 5 \\ 0 & 8 & 6 \\ 12 & 23 & 19 \end{bmatrix} \times \begin{bmatrix} a \\ b \\ c \end{bmatrix}$$

yada

$$\left[\begin{array}{ccc|c} 20 & 14 & 5 & 11 \\ 0 & 8 & 6 & 20 \\ 12 & 23 & 19 & 1 \end{array}\right]$$

sistemini satır işlemleri ile sadeleştirip çözeceğiz:

$$\text{1.satırı } -\frac{3}{5} = 15 \text{ ile çarp ve 3.satır ile topla} \rightarrow \left[\begin{array}{ccc|c} 20 & 14 & 5 & 11 \\ 0 & 8 & 6 & 20 \\ 0 & 25 & 16 & 10 \end{array}\right]$$

$$\text{1.satırı } \frac{1}{5} = -5 \text{ ile ve 3.satır } \frac{8}{25} = -8 \text{ ile çarp} \rightarrow \left[\begin{array}{ccc|c} 4 & 8 & 1 & 23 \\ 0 & 8 & 6 & 20 \\ 0 & 8 & 2 & 24 \end{array}\right]$$

$$\text{3.satırdan 2.satırı çıkar} \rightarrow \left[\begin{array}{ccc|c} 4 & 8 & 1 & 23 \\ 0 & 8 & 6 & 20 \\ 0 & 0 & 22 & 4 \end{array}\right]$$

$$\text{3.satırı 19 ile çarp} \rightarrow \left[\begin{array}{ccc|c} 4 & 8 & 1 & 23 \\ 0 & 8 & 6 & 20 \\ 0 & 0 & 2 & 24 \end{array}\right]$$

$$\text{2.satırdan 3.satırın 3 katını çıkar } \rightarrow \left[\begin{array}{ccc|c} 4 & 8 & 1 & 23 \\ 0 & 8 & 0 & 0 \\ 0 & 0 & 2 & 24 \end{array}\right]$$

$$\text{1.satırdan 2.satırı çıkar } \rightarrow \left[\begin{array}{ccc|c} 4 & 0 & 1 & 23 \\ 0 & 8 & 0 & 0 \\ 0 & 0 & 2 & 24 \end{array}\right]$$

elde ederiz. Yani

$$\left\{\begin{array}{l} 2c = 24(26) \\ 8b = 0(26) \\ 4a + c = 23(26) \end{array}\right. \rightarrow \; c = 12(13) \; \rightarrow \left\{\begin{array}{l} c = 12(26) \text{ veya} \\ c = 25(26) \end{array}\right.$$

$$8b = 0(26) \;\rightarrow\; 4b = 0(13) \;\rightarrow \left\{\begin{array}{l} b = 0(26) \text{ veya} \\ b = 13(26) \end{array}\right.$$

$c = 12$ (26) durumunda a için çözüm yoktur. $c = 25$ durumunda ise

$$4a + 25 = 23(26) \;\rightarrow\; 2a = -1(13) \;\rightarrow\; a = 6(13) \;\rightarrow \left\{\begin{array}{l} a = 6(26) \text{ veya} \\ a = 19(26) \end{array}\right.$$

bulunur. Şu halde

$$\left(\begin{array}{c} a \\ b \\ c \end{array}\right) = \left(\begin{array}{c} 6 \text{ veya } 19 \\ 0 \text{ veya } 13 \\ 25 \end{array}\right)$$

olup 4 tane çözüm vardır. Bunlardan $b = 13$ çözümüne bakarsak denklemi sağlamadığından

$$\left(\begin{array}{c} a \\ b \\ c \end{array}\right) = \left(\begin{array}{c} 6 \\ 0 \\ 25 \end{array}\right) \text{ veya } \left(\begin{array}{c} a \\ b \\ c \end{array}\right) = \left(\begin{array}{c} 19 \\ 0 \\ 25 \end{array}\right)$$

çözümlerini elde ederiz. Benzer şekilde

$$\left(\begin{array}{c} d \\ e \\ f \end{array}\right) \text{ ve } \left(\begin{array}{c} g \\ h \\ i \end{array}\right)$$

için çözümlere bakacak olursak

$$\left(\begin{array}{c} d \\ e \\ f \end{array}\right) = \left(\begin{array}{c} 8 \\ 0 \\ 13 \end{array}\right) \text{ veya } \left(\begin{array}{c} d \\ e \\ f \end{array}\right) = \left(\begin{array}{c} 21 \\ 0 \\ 13 \end{array}\right)$$

ve

$$\left(\begin{array}{c} g \\ h \\ i \end{array}\right) = \left(\begin{array}{c} 6 \\ 4 \\ 15 \end{array}\right) \text{ veya } \left(\begin{array}{c} g \\ h \\ i \end{array}\right) = \left(\begin{array}{c} 19 \\ 4 \\ 15 \end{array}\right)$$

çözümleri elde edilir. Toplamda bakacak olursa 8 farklı çözüm bulunmuştur. Bunlara karşılık gelen kelimeler şunlardır:

GAZIANGEP, GAZIANTEP, GAZVANGEP, GAZVANTEP, TAZIANGEP, TAZIANTEP, TAZVANGEP, TAZVANTEP.

Kadri 8 farklı çözüm elde ettiği için tereddüte düşüyor ancak sadece bir tanesi anlamlı mesaj olduğundan cevabı doğru buluyor. Cevap GAZIANTEP tir.

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.

Çözüm:

a) $F_k(x) = k(x^k + 1)$ olduğundan geçerli anahtarlar 26^3 ve $\phi(26^3) = 2^4 \cdot 3 \cdot 13^2$ ile aralarından asal olması gerekmektedir. Yani $\frac{2}{3}\phi\left(26^3\right) = 2^5 \cdot 13^2 = 5408$ tane geçerli anahtarlar bulunmaktadır.

b) Deşifre etmek için elimize gelen C şifreli mesajı üzerinde $(k^{-1}C - 1)^e$ şeklinde bir işlem yaparız. Burada k^{-1} sayısı k nın mod 26^3 sayısına göre tersi ve e sayısı da k'nın mod $\phi(26^3)$ sayısına göre tersidir.

c) Üç harfi üç harfe götürdüğümüz için {AAA, AAB, AAC, ... , ZZZ} kümesini {AAA, AAB, AAC, ..., ZZZ} kümesine götüren bir fonksiyon tasarlıyormuşuz gibi düşünebiliriz. Yani toplamda $26^3 - 1 = 17575$ tane elemanı yine o kadar tane elemana götüren bir fonksiyon tasarlıyoruz. Bu kümenin elemanlarına bakacak olursak üç basamaklıdır, yani 26 tabanında çalışıyormuşuz gibi düşünebiliriz. Mesela elimizde CAN kelimesi varsa bu $2 \cdot 26^2 + 0 \cdot 26 + 13 = 1365$ sayısına karşılık gelir çünkü C= 2, A= 0 ve N= 13 tür. Diğer taraftan elimizde 17576 dan küçük bir sayı varsa, mesela 15490 olsun, onu üçlü harfe şu şekilde dönüştürüyoruz: $15490 \equiv 20 (\text{mod } 26)$ olup birinci rakamı U(= 20) dur. İkinci rakamı $\dfrac{15490 - 20}{26} = 595 \equiv 23 (\text{mod } 26)$ olup X(= 23) tir. Üçüncü rakamı ise $\dfrac{595 - 23}{26} = 22$ olup W(= 22) dur. Dolayısıyla 15490 sayısı UXW olarak şifrelenir.

Şimdi adlarımızı şifreleyecek olursak

Anil+Ernist+Kivanc=ANI LER NIS TKI VAN CXX olup bunu sayılarla ifade edersek:

P = $(0 \cdot 26^2 + 13 \cdot 26 + 8)$ $(11 \cdot 26^2 + 4 \cdot 26 + 17)$ $(13 \cdot 26^2 + 8 \cdot 26 + 18)$ $(19 \cdot 26^2 + 10 \cdot 26 + 8)$ $(21 \cdot 26^2 + 0 \cdot 26 + 13)$ $(2 \cdot 26^2 + 23 \cdot 26 + 23) =$

346 7557 9014 13112 14209 1973

elde edilir. Şimdi bu altı tane sayıyı $k = 5$ seçerek $F_5(x) = 5x^5 + 5$ fonksiyonu ile şifreleyelim:

$F_5(346) = 9717, F_5(7557) = 9142, F_5(9014) = 2565, F_5(13112) = 7429, F_5(14209) = 2202, F_5(1973) = 15846$ olup 9717 = OJT, 9142 = NNQ, 2565 = DUR, 7429 = KZT, 2202 = DGS, 15846 = XLM elde edilir, yani

ANILERNISTKIVANCXX kelimesinin şifreli hali OJTNNQDURKZTDGSXLM dir.

Şimdi deşifre etmek için k^{-1} ve e sayılarını bulmamız lazım. Yani $kx \equiv 1 (\text{mod } 26^3)$ ve $ky \equiv 1 (\text{mod } \phi(26^3))$ denklemlerini çözmemiz gerekiyor. $5x \equiv 1 (\text{mod } 26^3)$ denkleminin çözümü $k^{-1} = 14061$ ve $5y \equiv 1 (\text{mod } \phi(26^3))$ denkleminin çözümü ise $e = 3245$ bulunur. Dolayısıyla $G(x)$ deşifre fonksiyonu $G(x) = (14061x - 1)^{3245}$ olarak verilir.

Not: En son elde ettiğimiz $G(x)$ fonksiyonu ile 9717, 9142, 2565, 7429, 2202, 15846 şifreli metinlerimizi (sayılarımızı) deşifre edecek olursak:

$G(9717) = 13528 \neq 346, G(9142) = 7557, G(2565) = 13408 \neq 9014, G(7429) = 13112, G(2202) = 10985 \neq 14209, G(15846) = 1973$ olup, bazı metinler doğru şekilde deşifre edilmediğini görüyoruz. Bunun sebebi Euler teoreminde M (metin) ile $\phi(26^3)$ sayıları aralarında asal olması gerekiyor. Aralarında asal olmadığı durumlarda ise deşifre fonksiyonu doğru çalışmayabilir.

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

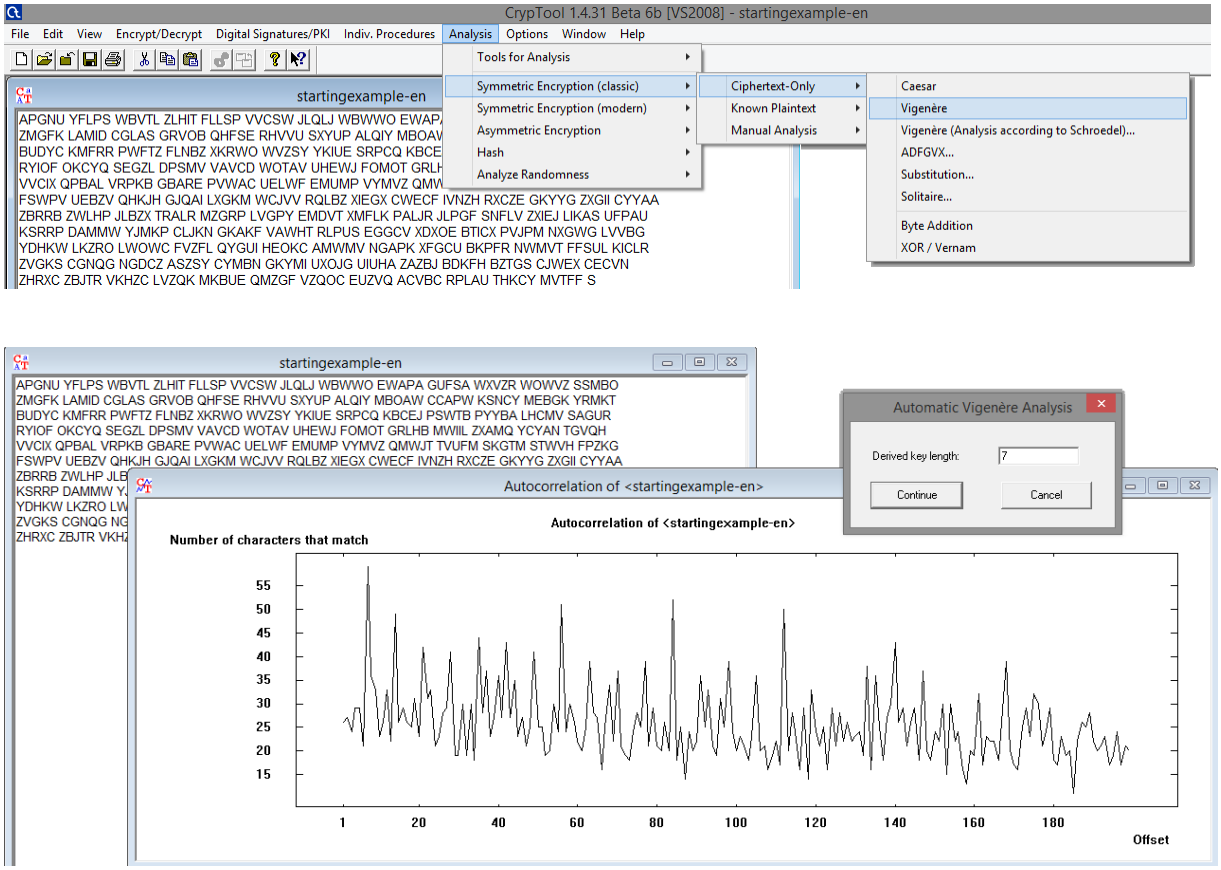
Bu durumda

a) Anahtar uzunluğunu bulunuz.

b) Anahtarı bulunuz.

c) Metni deşifre ediniz.

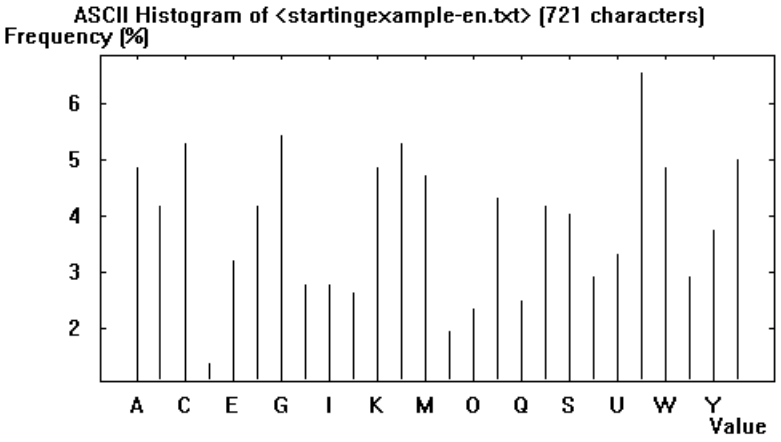
Çözüm: Bu analiz için cryptool kullanacağız. Genel olarak Vigenere sisteminin analizini yapmanın bir çok metodu var. Kasiski analizi, Friedman test, Frekans Analizi ve Anahtar eleme yöntemleri.



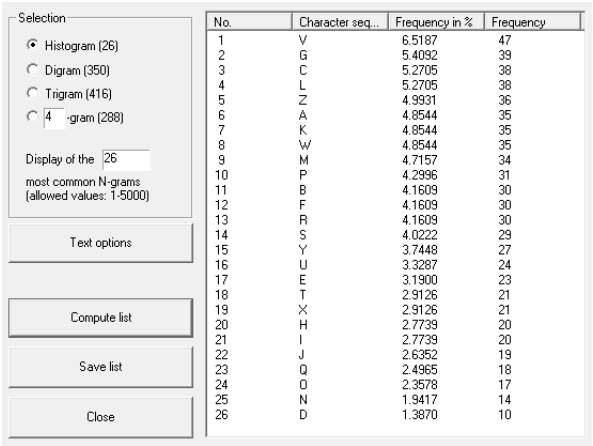
Şekil 5: Cryptool ile Vigenere

Cryptool da bunu deneyerek hem anahtar uzunluğunu, hem anahtarı, hem de şifreli metnin çözümünü bulabiliriz.

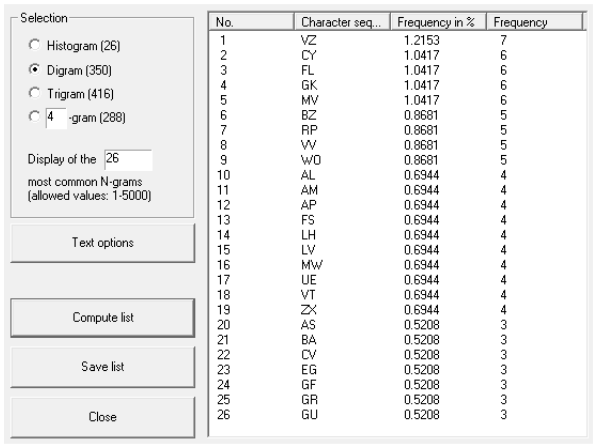
Anahtar Uzunluğu 7 olarak bulundu. Harflerin kullanım sıklığı da kriptoanalizde çok kullanılan bir yöntemdir. Anahtarın uzunluğu için etkili yöntemlerden birisi olan Frequency Anlayze yöntemine göre harflerin kullanım sıklığı şekilde gösterilmiştir.

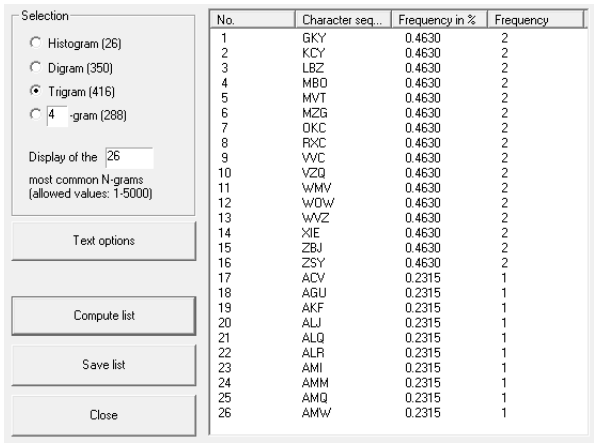


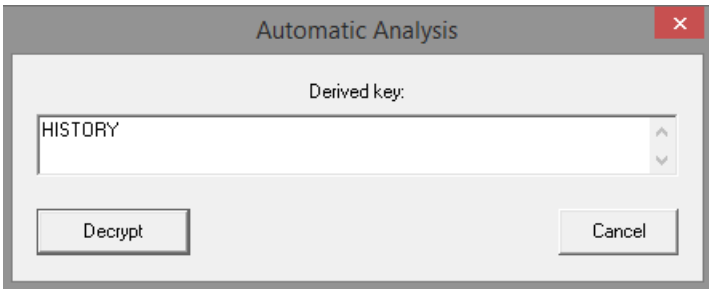
Grupların ve kelimelerin gruplandırılarak kullanım sıklığına bakarak da şifreli metin çözülebilir. Şifreli olarak verilen metnin analizi yapılırken kelime gruplarının kullanım sıklığına ve tekrar etme uzunluklarına baktığımız zaman anahtarın uzunluğunu tahmin edebiliriz.



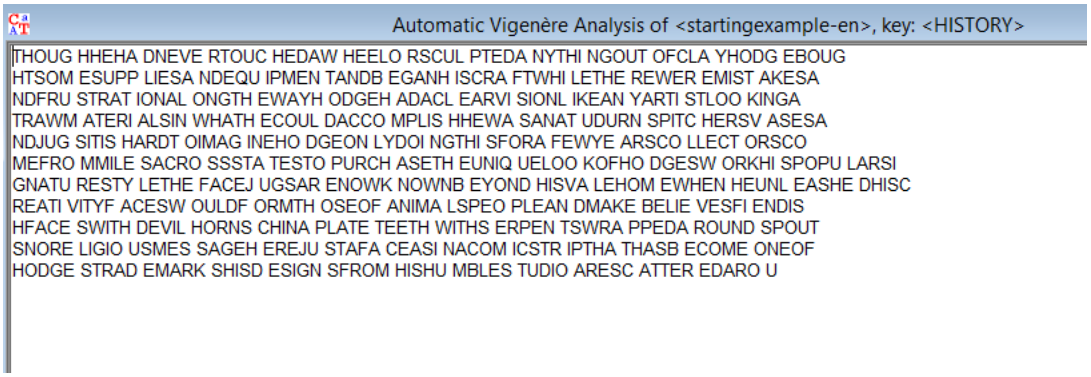
No.	Character seq...	Frequency in %	Frequency
1	V	6.5187	47
2	G	5.4092	39
3	C	5.2705	38
4	L	5.2705	38
5	Z	4.9931	36
6	A	4.8544	35
7	K	4.8544	35
8	W	4.8544	35
9	M	4.7157	34
10	P	4.2996	31
11	B	4.1609	30
12	F	4.1609	30
13	R	4.1609	30
14	S	4.0222	29
15	Y	3.7448	27
16	U	3.3287	24
17	E	3.1900	23
18	T	2.9126	21
19	X	2.9126	21
20	H	2.7739	20
21	I	2.7739	20
22	J	2.6352	19
23	Q	2.4965	18
24	O	2.3578	17
25	N	1.9417	14
26	D	1.3870	10







Şekil 6: Anahtar "HISTORY"



Şekil 7: Çözülmüş Metin

Yukarı da çözülmüş metini görebiliriz. Bu metni okuyup anlamlı haline bakarsak aşağıdaki gibi bir sonuç gelecektir.

THOUGH HE HAD NEVER TOUCHED A WHEEL OR SCULPTED ANYTHING OUT OF CLAY HODGE BOUGHT SOME SUPPLIES AND EQUIPMENT AND BEGAN HIS CRAFT WHILE THERE WERE MISTAKES AND FRUSTRATION ALONG THE WAY HODGE HAD A CLEAR VISION LIKE ANY ARTIST LOOKING A TRAW MATERIALS IN WHAT HE COULD ACCOMPLISH HE WAS AN ATUDURNSPITC HERS VASES AND JUGS IT IS HARD TO IMAGINE HODGE ONLY DOING THIS FOR A FEW YEARS COLLECTORS COME FROM MILES ACROSS STATE STOP URCH AS ETHEUNIQUE LOOK OF HODGES WORK HIS POPULAR SIGNATURE STYLE THE FACE JUGS ARE NOW KNOWN BEYOND HIS VALEHOME WHEN HE UNLEASHED HIS CREATIVITY FACES WOULD FORM THOSE OF ANIMALS PEOPLE AND MAKE BELIEVES FIENDISH FACES WITH DEVIL HORN SCHIN A PLATE TEETH WITH SERPENTS WRAPPED AROUND SPOUT SNORELIGIOUS MESSAGE HERE JUST A FACE AS IN A COMICS TRIP THAT HAS BECOME ONE OF HODGES TRADE MARKS HIS DESIGNS FROM HIS HUMBLE STUDIO ARE SCATTERED A ROU

Problem 10

Trivium ve RC4 akan şifre algoritmalarının detaylarını açıklayınız.

Çözüm: *RC4 Şifreleme algoritması:*

⋆ RC4 algoritması şifrelenecek veriyi akan bir bit dizisi olarak algılar.

⋆ RC4 belirlenen anahtar ile veriyi şifreleyen bir algoritmadır.

⋆ Genellikle hız gerektiren uygulamalarda kullanılır.

⋆ Şifreleme hızı yüksektir ve MB/sn seviyesindedir.

⋆ Güvenliği rastgele bir anahtar kullanımına bağlıdır.

⋆ Anahtar uzunluğu değişkendir.

⋆ 128 bitlik bir RC4 şifrelemesi sağlam bir şifreleme olarak kabul edilir.

⋆ Bankacılık ve Dökümantasyon (PDF) şifrelemelerinde yaygın olarak kullanılır.

RC4 rasgele olarak ürettiği anahtar akışlarını (keystream), hem şifreleme hem de açma işlemi sırasında yahut (özel veya (XOR)) işlemi ile mesaja uygulamaktadır. Bir anahtar akışı (keystream) oluşturmak için algoritma iki gizli adım icra eder:

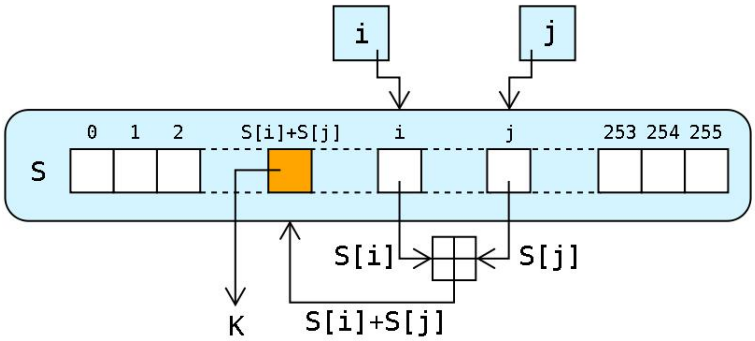
1. 1. Aşağıda S olarak da adlandırılacak olan bütün 256 ihtimali içeren bir permütasyon
2. 2. Aşağıda i ve j olarak adlandırılacak olan iki adet 8 bitlik gösterici (pointer)

Permütasyon işlemi 40 ile 256 arasında değişken bir sayıdaki anahtar ile ilklendirilir.

Anahtar algoritması:

```
byte S[256];
(Initialize S)
i = j = 0;
Loop:
i = (i + 1) % 256;
j = (j + S[i]) % 256;
swap (S[i], S[j]);
output S[ (S[i] + S[j]) % 256 ]
```

Yukarıdaki algoritmanın çalışması aşağıdaki şekilde tasvir edilmiştir:



Trivium Şifreleme Algoritması: Trivium bir akış şifreleme algoritmasıdır. Amaç, bir akış şeklinde her şifreleme birimindeki işlem bir önceki şifreleme sisteminden gelen bilgiye bağlıdır. Trivium donanım bazlı bir dizi şifreleme sistemidir. Anhatar dizisi açık metinden bağımsız üretildiği için senkron bir şifreleme sistemidir.

Trivium hız ve alan arasında esnek bir optimizasyon sağlar.

Trivium dizi şifreleme algoritması, 80-bit gizli anahtar ve 80-bit ilk değer üreterek 264 bite kadar anahtar dizisi üretebilir. Şifreleyici, ilk olarak gizli anahtar ve ilk değer kullanılarak başlangıç durumuna getirilir, daha sonra durum tekrar güncellenir ve anahtar bitlerini üretmek için kullanılır.

Temel olarak algoritmada kullanılan anahtar uzunluğu 80 bit, ilk değer uzunluğu 80 bit ve internal state 288 bittir.

Trivium Dizi Şifreleme Algoritmasında 288-bitlik iç durum (internal state) s1, s2, ..., s288 ile gösterilmiştir. Anahtar dizisi üretilme işlemi 15 özel bitin ayrılması, hepsinin 3 bitin güncellenmesinde kullanılması ve son olarak 1 bit anahtar dizisi zi' nin hesaplanması işlemlerini içerir. Daha sonra durum bitleri kaydırılarak döndürülür ve istenen N $\leq$ 264 bitlik anahtar dizisi üretilene kadar işlem tekrarlanır. Algoritmanın matematiksel tanımı aşağıdaki gibidir:

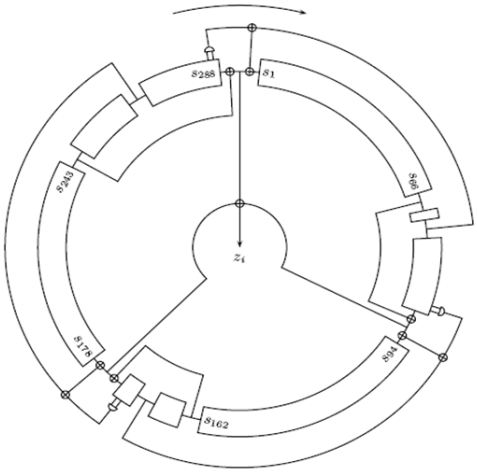
```
for
i = 1 to N do
t1 ← s66 + s93
t2 ← s162 + s177
t3 ← s243 + s288
zi ← t1 + t2 + t3
t1 ← t1 + s91.s92 + s171
t2 ← t2 + s175.s176 + s264
t3 ← t3 + s286.s287 + s69
(s1, s2, ..., s93) ← (t3, s1, ..., s92)
(s94, s95, ..., s177) ← (t1, s94 , ..., s176)
(s178, s179 ,..., s288) ← (t2, s178,..., s287)
end for
```

Modülo-2'ye göre yazılan yukarıdaki algoritmada toplama (+) işlemi XOR ve çarpma (.) işlemi AND lojik işlemlerini göstermektedir. Ayrıca s1 en düşük anlamlı biti, s288 ise en yüksek anlamlı biti göstermektedir. Anahtar üretilme işlemi Şekil (8)'de gösterildiği gibidir.

Trivium Dizi Şifreleme Algoritması'nda anahtar üretme işleminden önce durumların başlangıç durumuna getirilmesi gerekmektedir. 288-bitlik iç durum 80-bitlik gizli anahtarın, 80-bitlik ilk değerin yüklenmesi ve s286, s287 ve s288 hariç diğer bitlerin '0' atanması ile başlangıç konumuna getirilmiş olur. Daha sonra 288-bitlik iç durum 4 tam tur boyunca anahtar bitinin üretilmesi hariç yukarıda anlatıldığı gibi kaydırılarak döndürülür. Başlangıç

koşuluna getirilme ve 4 tur döndürme aşağıda matematiksel olarak anlatılmıştır.

```
(s1, s2,..., s93) ← (K1,..., K80, 0, ..., 0)
(s94, s95,..., s177) ← (IV1,..., IV80, 0,..., 0)
(s178, s179 ,..., s288) ← (0,..., 0, 1, 1, 1)
for i = 1 to 4.288 do
t1 ← s66 + s91.s92 + s93 + s171
t2 ← s162 + s175.s176 + s177 + s264
t3 ← s243 + s286.s287 + s288 + s69
(s1, s2,..., s93) ← (t3, s1,..., s92)
(s94, s95,..., s177) ← (t1, s94 ,..., s176)
(s178, s179,..., s288) ← (t2, s178,..., s287)
end for
```



Şekil 8: Trivium ve Anahtar Üretilme İşlem

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.

Çözüm: Öğrenci numaramızın son iki rakamı 10 olsun. Her bir rakam için 5 er bit kullanarak 0000100000 şeklinde yazdığımızı varsayalım. Yani LFSR başlangıç girdisi olarak bu sayıyı alacağız.

Benzer şekilde şifreleyeceğimiz metni, yani adlarımızı ikilik tabanda yazacak olursak

ERNIST = 4,17,13,8,18,19 = (00100, 10001, 01101, 01000, 10010, 10011)

KIVANC = 10,8,21,0,13,2 = (01010, 01000, 10101, 00000, 01101, 00010)

ANIL = 0,13,8,11 = (00000, 01101, 01000, 01011)
olarak bulunur. Bu üçünün toplam uzunluğu 80 bit olduğundan bize o uzunlukta anahtar lazım olacaktır. Onu elde etmek için ise LFSR yi, veya bağlantı fonksiyonumuzu bu uzunluğu elde edene kadar çalıştıracağız.

Bu durumda LFSR nın çıktısı $K =$
00001000000011101001011110111111100010110100001000000011101001011110111111100010
olarak elde edilir.

Açık metinimizle anahtarımızı mod2'ye göre toplarsak şifreli metinimizin 2'lik sistemde yazılımını elde ederiz:

00100100010111010100010010100110101001000101010000001101000100000001101010000101 1

00001000000011101001011110111111100010110100001000000011101001011110111111100010

$\oplus$

00101000010101000001111011110010110000111110101000011001100001011101101011101001

= 00101 00001 01010 00001 11101 11100 10110 00011 11101 01000 01100 11000 01011 10110 10111 01001 veya EBKBŞÖWDŞIMYLWXJ şifreli metnini elde ederiz.

Burada not edilmesi gereken, alfabede 26 karakter vardı. Fakat ikilik tabanda gösterirken her bir karakteri 5 bit kullanarak gösterdik. Dolayısıyla toplamda 32 farklı gösterim elde ettik. Arta kalan 6 gösterim için de 6 tane karakter ekledik (Ç=11010, İ=11011, Ö=11100, Ş=11101, Ü=11110, Ğ=11111)

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.

Çözüm: Öğrenci numaramızın son iki rakamı $(06)_{10} = (110)_2$ olsun. Bu durumda girdi olarak f_1 için 10, f_2 için 110 ve f_3 için 00110 kullanacağız. Adlarımız *Anil+Ernist+Kivanc* = 16 uzunluklu olduğundan $5 \cdot 16 = 80$ uzunluklu dizi üretmemiz gerekiyor.

Not: Bir önceki problemde olduğu gibi Ç=11010, İ=11011, Ö=11100, Ş=11101, Ü=11110, Ğ=11111 olarak aldık.

1.LFSR: 101 101 101 101 101 ... şeklinde devam eden çıktı verecek...periyodu 3 tür.

2.LFSR: 1101001 1101001 1101001 1101001 1101001 ... şeklinde devam eden çıktı verecek...periyodu 7 dir.

3.LFSR ise: 001101011110001 001101011110001 001101011110001 001101011110001... şeklinde devam eden çıktı verecek... Not: bu dizinin periyodu 15 çıkmıştır ancak karakteristik polinomu $x^5+x^4+x^2+1$ indirgenebilir olduğundan bu dizinin periyodu başlangıç değerlere göre değişmektedir.

Şimdi bu üç diziyi alt alta yazarak verilen kombinasyon ile bağlarsak 10010 01010 01101 10100 11001 11101 10000 11110 11100 10010 11000 01101 10110 01101 01100 10110 ile başlayan periyodu okek(3,7,15)=105 olan bir dizi elde ederiz. Ancak bize sadece ilk 80 lik kısmı lazım olduğundan 105 e kadar gitmemize gerek yok...

00000 01101 01000 01011 00100 10001 01101 01000 10010 10011 01010 01000 10101 00000 01101 00010 = P = ANILERNISTKIVANC

10010 01010 01101 10100 11001 11101 10000 11110 11100 10010 11000 01101 10110 01101 01100 10110 = K olup

10010 00111 00101 11111 11101 01100 11101 10110 01110 00001 10010 00101 00011 01101 00001 10100 = C = SHFĞŞMŞWOBSFDNBU şifreli metnini elde edeceğiz. Deşifre etmek için ise aynı diziyi bir kere daha toplarsak düz metni elde ederiz.