KRİPTOLOJİ

4. sınıf
bilgisayar müh.

Number Theory - Sayılar Teorisi

25.09.2017

Bölme: a ve b tamsayı. $a \neq 0$.

$a \mid b \rightarrow a$, b'yi tam böler. $\quad b = k.a$

örnek: $3 \mid 15$, $-15 \mid 60$, $7 \nmid 18$

Teoremler:

1-) $a \mid b \wedge a \mid c \Rightarrow a \mid b+c$

Proof: $b = s.a$, $c = t.a \rightarrow b+c = (s+t).a$

2-) $a \mid b \Rightarrow \forall c \in I,\ a \mid b.c$

Proof: $b = s.a \rightarrow b.c = s.a.c$

3-) $a \mid b \wedge b \mid c \Rightarrow a \mid c$

Proof: $b = s.a$, $c = t.b \rightarrow c = a.t.a$

Asal Sayı: $p \rightarrow$ asal $\Rightarrow p > 1$, $\neg(\exists q\,(q \in [2,3,\dots,p-1] \wedge q \mid p))$

örnek: $\Pi(x) \cong \frac{x}{\ln x}$, $\Pi(x) / (x/\ln x) \rightarrow 1 \quad (x \rightarrow \infty)$

Bölme İşlemi: $a \in I$ olsun. $\exists d \in N^+ \Rightarrow a = d.q + r \wedge 0 \leq r < d$

örnek: $8 = 3.2 + 2$ ✓
$-7 = -3.3 + 2$ X
$-7 = -2.3 - 1$ ✓

OBEB: $obeb(a,b) = gcd(a,b)$

örnek: $gcd(6,4) = 2$, $gcd(5,7) = 1$, $gcd(1728, 135) = 9$
$1728 = 2^6 \cdot 3^3$ $135 = 3^3 \cdot 5$

Bilgi: Bir sayının modüler aritmetikte tersinin olması için işleme alınan uzayla aralarında asal olmak.

$3^{-1} \bmod 5 \rightarrow$ ✓ $\qquad 3^{-1} \bmod 6 \rightarrow$ X

Öklid Algoritması

$\gcd(a,b) = ?$ $\quad a = r_0 \;,\; b = r_1 \;,\; r = r_2$

$a = b \cdot q_1 + r$

$r_0 = r_1 \cdot q_1 + r_2 \quad \wedge \quad 0 \le r_2 < r_1$

$r_1 = r_2 \cdot q_2 + r_3 \quad \wedge \quad 0 \le r_3 < r_2$

$\vdots \qquad\qquad\qquad \vdots$

$r_{n-2} = r_{n-1} \cdot q_{n-1} + r_n \quad \wedge \quad 0 \le r_n < r_{n-1}$

$r_{n-1} = r_n \cdot q_n + 0$

$\gcd(a,b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \dots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n$

örnek: $\gcd(482, 1180) = ?$

$1180 = 482 \cdot 2 + 216$

$482 = 216 \cdot 2 + 50$

$216 = 50 \cdot 4 + 16$

$50 = 16 \cdot 3 + 2$

$16 = 8 \cdot 2 + 0 \quad \rightarrow \quad \gcd(482, 1180) = \gcd(2, 0) = 2.$

Modüler Aritmetik: $m \in \mathbb{N}^+,\; a, b \in \mathbb{I}\;,\; a = r \bmod m \iff a = q \cdot m + r\;,\; 0 \le r < m$

Modül Denkliği: $a = b \bmod m\;,\; c = d \bmod m$

i) $(a+c) = (b+d) \bmod m$

ii) $(a \cdot c) = (b \cdot d) \bmod m$

$a \bmod m = b \bmod m = r$

örnek: $\gcd(252, 198) = ?$

$252 = 198.1 + 54$

$198 = 54.3 + 36$

$54 = 36.1 + 18$

$36 = 18.2 + 0 \rightarrow \gcd(252, 198) = \gcd(18, 0) = 18.$

teorem: $\gcd(I_1, I_2) = t.I_1 + s.I_2$, $18 = t.252 + s.198$

$18 = 54 - 1.36$

$36 = 198 - 3.54$

$54 = 252 - 1.198$

$\rightarrow$

$18 = 54 - 1.(198 - 3.54)$

$= 4.54 - 1.198$

$= 4.(252 - 1.198) - 1.198$

$= 4.252 - 5.198$

$t = 4 \quad s = -5$

Eğer iki sayının gcd'si 1 olsaydı önündeki katsayılar birbirlerine göre ters olacaktı

$1 = t.a + s.b$

$a^{-1} \bmod b = t$

$b^{-1} \bmod a = s$

örnek: $\gcd(3, 5) = ?$

$5 = 3.1 + 2$

$3 = 2.1 + 1$

$2 = 2.1 + 0 \rightarrow \gcd(3, 5) = 1$

$1 = 3 - 1.2$

$= 3 - 1.(5 - 1.3)$

$= 2.3 - 1.5$

$\hookrightarrow 3^{-1} \bmod 5 = 2$

teorem: $m \in N^+ \wedge a,b,c \in I$

$(a.c) = (b.c) \bmod m \wedge \gcd(m,c) = 1 \Rightarrow a = b \bmod m$

örnek: $40 = 25 \bmod 3$

$8.5 = 5.5 \bmod 3 \wedge \gcd(5,3) = 1 \Rightarrow 8 = 5 \bmod 3$

örnek: $14 = 8 \bmod 6$

$7.2 = 4.2 \bmod 6 \wedge \gcd(6,2) \neq 1 \Rightarrow 7 \neq 4 \bmod 6$

teorem: $m \in N^+ \wedge a,b,c \in I$

$(a.c) = (b.c) \bmod m \wedge \gcd(m,c) = i \Rightarrow k = \frac{m}{i} \wedge a = b \bmod k$

örnek: $14 = 8 \bmod 6$

$7.2 = 4.2 \bmod 6 \wedge \gcd(6,2) = 2 \Rightarrow k = \frac{6}{2} = 3 \wedge 7 = 4 \bmod 3$

Doğrusal Denklem Çözümü

$a.x = b \bmod m \quad , \quad m \in N^+ \wedge a,b,x \in I$

$x = b.a^{-1} \bmod m \Leftrightarrow \gcd(a,m) = 1$

$\downarrow$

$1 = t.m + s.a$

$\downarrow$

$a^{-1} = s \bmod m$

örnek: $3x = 4 \bmod 7$

$x = 4.3^{-1} \bmod 7 \wedge \gcd(3,7) = 1$

$\downarrow$

$1 = t.7 + s.3$

$7 = 2.3 + 1 \rightarrow 1 = 7 - 2.3$

$\downarrow$

$3^{-1} \bmod 7 = -2 = 5$

Teoremler

1-) $a.c = b.c \mod m \;\wedge\; \gcd(c,m) = 1 \Rightarrow a = b \mod m$

2-) $a.c = b.c \mod m \;\wedge\; \gcd(c,m) = i \Rightarrow k = \frac{m}{i} \;\wedge\; a = b \mod k$

3-) $\gcd(a,m) = 1 \Rightarrow \exists a^{-1},\ a.a^{-1} = 1 \mod m$

4-) $a.x = b \mod m \;\wedge\; \gcd(a,m) = 1 \Rightarrow x = b.a^{-1} \mod m$

5-) $a.x = b \mod m \;\wedge\; \gcd(a,m) = d \;\wedge\; d \mid b \Rightarrow x = b'.a'^{-1} \mod m'$

$a' = a/d,\ b' = b/d,\ m' = m/d$

örnek: $28x = 14 \mod 21$

$4.7x = 2.7 \mod 21$ (2. kural) $\quad 4x = 2 \mod 3$

$2.2x = 2.1 \mod 3$ (1. kural) $\quad 2x = 1 \mod 3$

$x = 1.2^{-1} \mod 3$ (4. kural) $\quad x = 2 \mod 3 = 2$

Euclid pseudo code: gcd(n,m)

```
if m=0 then gcd=n
else gcd(m, n mod m)
```

Extended Euclid Algorithm

$\gcd(n,m) = t.m + s.n = g$

```
gcdext(n,m,g,t,s)
  if m=0 then g:=n, t:=1, s:=0
  else gcdext(m, n mod m, g, t, s)
  u:=s
  s:=t - L n/m J .s
  t:=u
  end {gcdext}
```

örnek: $gcd(87, 55) = ?$

gcdext(87, 55, g, t, s)	g=1	t=-12	s=19
gcdext(55, 32, g, t, s)	g=1	t=7	s=-12
gcdext(32, 23, g, t, s)	g=1	t=-5	s=7
gcdext(23, 9, g, t, s)	g=1	t=2	s=-5
gcdext(9, 5, g, t, s)	g=1	t=-1	s=2
gcdext(5, 4, g, t, s)	g=1	t=1	s=0-⌊5/4⌋.1=-1
gcdext(4, 1, g, t, s)	g=1	t=0	s=t-⌊4/1⌋.s=1-⌊4/1⌋.0=1
gcdext(1, 0, g, t, s)	g=1	t=1	s=0

$$gcdext(87, 55) = 1 = -12.87 + 19.55$$

Ödev 1: Extended euclid algorithm'i gerçekleyen program.

Ödev 2: 4. ve 5. kuralı içeren program. ($ax = b \bmod m$)

örneklerle deneyip word'de kod, bilgi vs dönmek.

02.10.2017

Chinese Remaining Theorem

$x \equiv a_1 \bmod m_1$
$x \equiv a_2 \bmod m_2$
$\vdots$
$x \equiv a_n \bmod m_n$

$x = ?$

$m_1 \perp m_2 \perp \dots \perp m_n$

$m = m_1 \cdot m_2 \cdots m_n$

$x \in [0, m-1]$

$$x = (a_1 \cdot M_1 \cdot y_1 + a_2 \cdot M_2 \cdot y_2 + \dots + a_n \cdot M_n \cdot y_n) \bmod m = \left(\sum a_i \cdot M_i \cdot y_i\right) \bmod m$$

$M_i = \frac{m}{m_i}$, $\gcd(M_i, m_i) = 1$ (olmalı)

$M_i \cdot y_i = 1 \bmod m_i \rightarrow y_i$, M_i'nin tersini hesaplayıp bulmuş.

örnek: $x = 9 \bmod 13$
$x = 8 \bmod 11$
$x = 1 \bmod 7$
$x = ?$

$13 \perp 11 \perp 7 \rightarrow m = 13 \cdot 11 \cdot 7 = 1001$

$x = (a_1 \cdot M_1 \cdot y_1 + \dots + a_n \cdot M_n \cdot y_n) \bmod m = (9 \cdot M_1 \cdot y_1 + 8 \cdot M_2 \cdot y_2 + 1 \cdot M_3 \cdot y_3) \bmod 1001$

$M_1 = m_2 \cdot m_3 = 11 \cdot 7 = 77$ $M_2 = m_1 \cdot m_3 = 13 \cdot 7 = 91$ $M_3 = m_1 \cdot m_2 = 13 \cdot 11 = 143$

$77 \cdot y_1 = 1 \bmod 13$
$12 \cdot y_1 = 1 \bmod 13$
$y_1 = 12^{-1} \bmod 13$
$y_1 = 12$

$91 \cdot y_2 = 1 \bmod 11$
$3 \cdot y_2 = 1 \bmod 11$
$y_2 = 3^{-1} \bmod 11$
$y_2 = 4$

$143 \cdot y_3 = 1 \bmod 7$
$3 \cdot y_3 = 1 \bmod 7$
$y_3 = 3^{-1} \bmod 7$
$y_3 = 5$

$x = (9 \cdot 77 \cdot 12 + 8 \cdot 91 \cdot 4 + 1 \cdot 143 \cdot 5) \bmod 1001 = 11943 \bmod 1001$

$x = 932$.

örnek: $y_2 = 3^{-1} \bmod 11$

$11 = 3 \cdot 3 + 2$
$3 = 2 \cdot 1 + 1$
$2 = 2 \cdot 1 + 0$

$\gcd(3, 11) = 1$

$1 = s \cdot 3 + t \cdot 11$

$1 = 3 - 1 \cdot 2$
$2 = 11 - 3 \cdot 3$

$1 = 3 - 1 \cdot (11 - 3 \cdot 3)$
$1 = 4 \cdot 3 - 1 \cdot 11$
↳ $3^{-1} = 4 \bmod 11$

örnek: $15x = 21 \mod 48$
$x = 5 \mod 13$ $\quad x=?$
$166x = 46 \mod 22$

$15x = 21 \mod 48 \rightarrow 5x = 7 \mod 16 \rightarrow x = 7.5^{-1} \mod 16$

$x = 5 \mod 13 \qquad x = 5 \mod 13$

$166x = 46 \mod 22 \rightarrow 12x = 2 \mod 22 \rightarrow x = 6^{-1} \mod 11$

$5^{-1} \mod 16 \Rightarrow 16 = 5.3 + 1$
$1 = 1.16 - 3.5 \Rightarrow 5^{-1} \mod 16 = -3 = 13 \Rightarrow x = 7.13 \mod 16$
$x = 11 \mod 16$

$6^{-1} \mod 11 \Rightarrow 11 = 6.1 + 5$
$6 = 5.1 + 1$
$1 = 6 - 5.1$
$1 = 6 - 1.(11 - 6.1)$
$1 = 2.6 - 1.11 \Rightarrow 6^{-1} \mod 11 = 2$

$x = 11 \mod 16$
$x = 5 \mod 13$
$x = 2 \mod 11$

$m = 16.13.11 = 2288$

$M_1 = 143$, $M_2 = 176$, $M_3 = 208$

$x = (a_1.M_1.y_1 + a_2.M_2.y_2 + a_3.M_3.y_3) \mod m$

$y_1 = 143^{-1} \mod 16 = 15^{-1} \mod 16 \qquad y_2 = 176^{-1} \mod 13 = 7^{-1} \mod 13 \qquad y_3 = 208^{-1} \mod 11 = 10^{-1} \mod 11$

$y_1 = 15 \quad y_2 = 2 \quad y_3 = 10$

$$x = (11.143.15 + 5.176.2 + 2.208.10) \mod 2288 = 2059$$

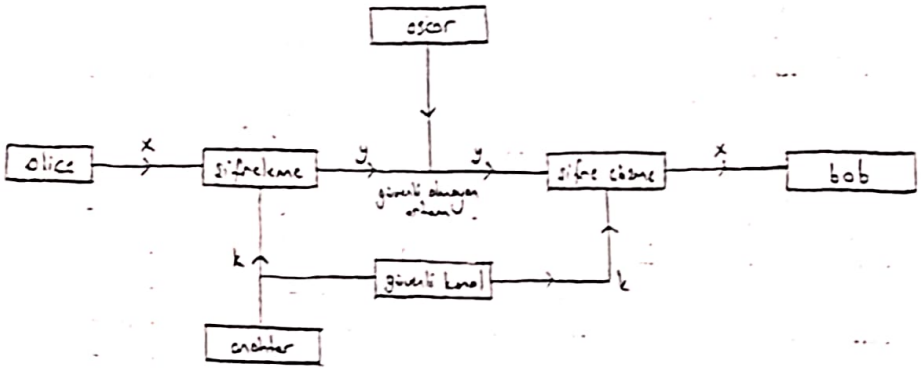
Çıkmış soru: $x^2 = 1 \mod 35$

$x = \pm 1 \mod 5 \qquad x = \pm 1 \mod 7$

$x = 1 \mod 5$ ⇄ $x = 1 \mod 7$ → $x = 1 \mod 5$ $\quad x = 1 \mod 5$ $\quad x = 4 \mod 5$ $\quad x = 4 \mod 5$
$x = 4 \mod 5$ ⇄ $x = 6 \mod 7$ $\quad x = 1 \mod 7$ $\quad x = 6 \mod 7$ $\quad x = 1 \mod 7$ $\quad x = 6 \mod 7$

işlemler yapılıp, 4 değer bulunur. Sadece a.k. elemen sayısı sorulabilir. Aralarında asal değillerse (7,5) a.k. yok.

Ödev 3: Çinli kalanlar teoreminin genelleşmiş halinin çözüm kümesini bulan program.



5 parametre vardır.

1. Plain Text, P → şifrelenecek mesajların sonlu kümesi , $x \in P$
2. Cipher Text, C → şifreli mesajların sonlu kümesi , $y \in C$
3. Keyspace , K → anahtarların sonlu kümesi , $k \in K$
4. Encryption , E → şifreleme kuralı , $e_k \in E$, $e_k : P \to C$
5. Decryption, D → şifre çözme kuralı , $d_k \in D$, $d_k : C \to P$

Sözde Asallar

teorem: $2^{n-1} \equiv 1 \bmod n \Rightarrow n \to$ asal! (asal olmayan bazı sayılarda olabilir)

t1: $\alpha \equiv 1 \bmod p \Rightarrow \alpha^n \equiv 1 \bmod p$

proof: $\alpha \equiv 1 \bmod p \Rightarrow p \mid (\alpha - 1)$

$\alpha^n - 1 = (\alpha - 1).(\alpha^{n-1} + \dots + 1)$

$p \mid (\alpha - 1) \Rightarrow p \mid (\alpha^n - 1)$

t2: $p_1 \mid \alpha$, $p_2 \mid \alpha$ ^ $p_1 \perp p_2 \Rightarrow p_1 . p_2 \mid \alpha$

proof: $\alpha = k . p_1$, $p_2 \mid \alpha \Rightarrow p_2 \mid k . p_1 \Rightarrow p_2 \mid k$

$\alpha = p_1 . p_2 . t$, $p_2 . t = k$

örnek: $2^{340} = 1 \bmod 341$

proof: $2^{340} = (2^{10})^{34}$ $\quad 2^{340} = (2^5)^{68}$ $\quad [11 \mid 2^{340}-1] \wedge [31 \mid 2^{340}-1]$

$2^{10} = 93.11 + 1$ $\quad 2^5 = 1.31 + 1$ $\quad 11 \perp 31$

$2^{10} = 1 \bmod 11$ $\quad 2^5 = 1 \bmod 31$ $\quad 11.31 = 341 \mid 2^{340}-1$

$(2^{10})^{34} = 1 \bmod 11$ $\quad (2^5)^{68} = 1 \bmod 31$ $\quad 2^{340} = 1 \bmod 341$

Fermat Teoremi

$p \rightarrow$ asal. $\wedge$ $\gcd(p,a) = 1 \Rightarrow a^{p-1} = 1 \bmod p$

örnek: $a.x = b \bmod p$ ise $x = ?$

$x = a^{-1}.b \bmod p$

$a.a^{-1} = 1 \bmod p \rightarrow x = a^{p-2}.b \bmod p$

a^{p-2}

örnek: $29^{1000} \bmod 37 = ?$

$29^{36.27+28} \bmod 37 = \underbrace{(29^{36})^{27}}_{1}.\ 29^{28} \bmod 37 = 29^{28} \bmod 37$

$= (-8)^{28} \bmod 37$

$= (2^3)^{28} \bmod 37 = 2^{84} \bmod 37 = 2^{36.2+12} \bmod 37$

$= \underbrace{(2^{36})^2}_{1}.2^{12} \bmod 37$

$= 2^{12} \bmod 37$

$= 2^4.2^8$

$= 16.256$

$= 16.(-3)$

Euler Fonksiyonu

$\forall m \in \mathbb{N}$, $\varphi(m)$: m'ye göre asal olan m'den küçük tüm doğal sayıların sayısını verir.

örnek: $m=10 \Rightarrow \overline{\mathbb{Z}}(10) = \{1,3,7,9\}$

$\varphi(10) = 4$

$p \rightarrow$ prime $\quad \varphi(p) = p-1$

$p \rightarrow$ prime $\quad \varphi(p^2) = p^2 - p$

a,b aralarında asal $\quad \varphi(a.b) = \varphi(a).\varphi(b)$

örnek: $\varphi(45) = \varphi(3.5) = \varphi(9).\varphi(5) = 6.4 = 24$.

teorem: $\forall n \in \mathbb{N}$, $\varphi(n) = n.\prod(1-1/p_i)$, $p_i \rightarrow$ asal

örnek: $\varphi(45) = 45.(1-1/3).(1-1/5) = 24$

Euler-Fermat Teorem: $\gcd(a,m)=1 \Rightarrow a^{\varphi(m)} \equiv 1 \bmod m$

örnek: $331^{51} \bmod 49 = ?$

$\gcd(331,49) = 1 \qquad \varphi(49) = \varphi(7^2) = 7^2 - 7 = 42$

$331^{51} = 331^{42+9} = \underbrace{331^{42}}_{1} \cdot 331^9 = 331^9 \bmod 49$

Hızlı Modüler Üs Alma Algoritması

09.10.2017

$a^b \bmod m = ?$ $\quad b = (b_k \cdot 2^k + b_{k-1} \cdot 2^{k-1} + \dots + b_1 \cdot 2 + b_0 \cdot 2^0)$ → binary form

1. $c \leftarrow 0$ (c, sonuda bize eşit olur)
2. $d \leftarrow 1$ (d, sonuçtur)
3. $b_k b_{k-1} b_{k-2} \dots b_1 b_0$ S.170. kodu var bilgiye.
4. i, k'dan 0'a kadar
5. $\quad c \leftarrow 2c$
6. $\quad d \leftarrow (d \cdot d) \bmod m$
7. $\quad$ Eğer $b_i = 1$ ise
8. $\quad\quad c \leftarrow c + 1$
9. $\quad\quad d \leftarrow (d \cdot a) \bmod m$
10. d ← sonuç

örnek: $7^{560} \bmod 561 = ?$

$560 = (1000110000)_2$

i	9	8	7	6	5	4	3	2	1	0	
c	1	2	4	8	17	35	70	140	280	560	$c = b = 560$
d	7	49	157	526	160	241	298	166	67	1	$d = a^b \bmod m = 1$

Klasik Şifreleme Algoritmaları

Shift Cipher

A	B	C	D	.....	W	X	Y	Z
0	1	2	3		22	23	24	25

$P = C = K = \mathbb{Z}_{26} \quad (0 \le K \le 25)$

$y = e_k(x) = (x + k) \pmod{26}$

$x = d_k(y) = (y - k) \pmod{26}$

örnek: P: "ABCDZ" $\quad K = 3$

$y_1 = e_k(A) = (0+3) \bmod 26 = 3 \rightarrow D$

$y_2 = e_k(B) = (1+3) \bmod 26 = 4 \rightarrow E$

$y_3 = e_k(C) = (2+3) \bmod 26 = 5 \rightarrow F$

$y_4 = e_k(D) = (3+3) \bmod 26 = 6 \rightarrow G$

$y_5 = e_k(Z) = (25+3) \bmod 26 = 2 \rightarrow C$

C: "DEFGC"

Substitution Cipher

$P = C = \mathbb{Z}_{26}$

K: 26 sembolün olası permütasyonlarından oluşur. ($\pi \in K$)

π :	a	b	c	d	e	.....	w	x	y	z
	X	N	Y	A	H		K	J	D	I

π^{-1} :	A	B	C	D	E	.....	W	X	Y	Z
	d	l	r	g			m	o	c	i

$y = e_\pi(x) = \pi(x)$

$x = d_\pi(y) = \pi^{-1}(y)$

örnek: P: "ABC"

$e_\pi(A) = X$ $\quad d_{\pi^{-1}}(X) = A$

$e_\pi(B) = N$ $\rightarrow$ C: "XNY" $\quad d_{\pi^{-1}}(N) = B$

$e_\pi(C) = Y$ $\quad d_{\pi^{-1}}(Y) = C$

Affine Cipher

$P = C = \mathbb{Z}_{26}$

$K = \{(a,b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \gcd(a,26) = 1\}$ $\quad a,b \in K$ $\quad$ uzay: $12 \cdot 26 = 312$

$y = e_k(x) = (ax+b) \pmod{26}$ $\quad y \in C$

$x = d_k(y) = a^{-1}(y-b) \pmod{26}$ $\quad x \in P$

örnek: $K = (7,3)$

$y = e_k(x) = (7x+3) \bmod 26$

$x = d_k(y) = 7^{-1}(y-3) \bmod 26 = 15(y-3) \bmod 26$

P: "hot"

$y_1 = e_k(h) = (7 \cdot 7 + 3) \bmod 26 = 52 \bmod 26 = 0 \rightarrow A$

$y_2 = e_k(o) = (7 \cdot 14 + 3) \bmod 26 = 101 \bmod 26 = 23 \rightarrow X$

$y_3 = e_k(t) = (7 \cdot 19 + 3) \bmod 26 = 136 \bmod 26 = 6 \rightarrow G$ $\quad$ C: "AXG"

Not: Affine, harflerin kullanma sıklığı, frekans analizi.

A → 0,082
B → 0,015
X → 0,001
Y → 0,02
Z → 0,001

* 1. E → 0.12
2. T, A, O, I, N, S, H, R → (0,06 - 0,09)
3. D, L → 0,04
4. C, U, M, W, F, G, Y, P, B → (0,015 - 0,028)
5. V, K, J, Q, X, Z < 0,01

** TH, HE, IN

*** THE, ING, AND, HER

örnek: C: "FMXVED ....." 57 karakter

R → 8
D → 7
E, H, K → 5
F, S, V → 4

$e_k(e) \to R \quad = (4.a+b) \bmod 26 = 17 \bmod 26$

$e_k(t) \to D \quad = (19.a+b) \bmod 26 = 3 \bmod 26$

$y = e_k(x) = (ax+b) \bmod m$

$$\begin{array}{l} 4a+b = 17 \\ -\,19a+b = 3 \\ \hline -15a = 14 \bmod 26 \end{array}$$

a=6 b=19 → gcd(6,26) ≠ 1 old. için seçim doğru değil. (cevap a=3 b=5)

Yukarıdaki soruda izlenilen yol, normalde en sık kullanılan harf e, şifremizdeki R ve normalde e'den sonra en sık kullanılan harf T olduğu için deneyerek cevap bulunmaya çalışır. Bir sonraki adım:

$e_k(e) \to R$; $e_k(a) \to D$ olacaktır.

Ödev 4: Hızlı modüler üs alma algoritmasının programı.

Ödev 5: Affine cipher kırıp analizi.

Ödev 6: Shift, substution, affine ve vigenere cipher'ın programı.

Vigenere Cipher

$P = C = K = (\mathbb{Z}_{26})^m$

$K = (k_1, k_2, \dots, k_m)$

$e_k(x_1, x_2, \dots, x_m) = (x_1 + k_1, x_2 - k_2, \dots, x_m + k_m) \bmod 26$

$d_k(y_1, y_2, \dots, y_m) = (y_1 - k_1, y_2 - k_2, \dots, y_m - k_m) \bmod 26$

örnek: $m = 6$, keyword → "CIPHER"

$k = (2, 8, 15, 7, 4, 17)$

P: "t h i s c r y p t o s y s t e m i s n o t s e c u r e"
19 7 8 18 2 17 24 15 19 14 18 .....
+ 2 8 15 7 4 17 2 8 15 7 4 .....

21 15 22 25 6 8 0 23 8 21 22 .....
C: V P X Z G I A .....

Hill Cipher

16.10.2017

$P = C = (\mathbb{Z}_{26})^m$, $m \geq 2$, int

$K =$ [m x m, $\mathbb{Z}_{26}$ üzerinde tersi alınabilir matris.]

$y = e_k(x) = x \cdot K$

$x = d_k(y) = y \cdot K^{-1}$ $\quad K^{-1} = (\det K)^{-1} \cdot K^*$ $\quad \det K = \sum_{j=1}^{m} (-1)^{i+j} \cdot k_{ij} \cdot \det K_{ij}$

$K = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $K^* = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, $K \cdot K^{-1} = I$

örnek: $K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$, $P =$ "july" , $C = ?$

P: "j u l y"
9 20 11 24

$\Rightarrow (j,u) \cdot K = (9, 20) \cdot \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (159, 212) \bmod 26 = (3, 4) \rightarrow D, E$

$(l,y) \cdot K = (11, 24) \cdot \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (193, 256) \bmod 26 = (11, 22) \rightarrow L, W$

C: "D E L W"

örnek: $K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$, $K^{-1} = ?$

$K^{-1} = \frac{1}{\det K} \cdot K^*$

$\det K = 7 \cdot 11 - 3 \cdot 8 = 53 \bmod 26 = 1$ $\qquad K^* = \begin{pmatrix} 11 & -8 \\ -3 & 7 \end{pmatrix} \bmod 26 = \begin{pmatrix} 11 & 18 \\ 23 & 7 \end{pmatrix}$

$$K^{-1} = \frac{1}{1} \cdot \begin{pmatrix} 11 & 18 \\ 23 & 7 \end{pmatrix} = \begin{pmatrix} 11 & 18 \\ 23 & 7 \end{pmatrix}$$

örnek: $m = 2$, P: "friday", C: "PQCFKU", $K = ?$ (hill cipher)

P: " f r i d a y "
  5 17 8 3 0 24

C: " P Q C F K U "
  15 16 2 5 10 20

$e_k(f,r) = (P,Q)$

$e_k(i,d) = (C,F)$

$e_k(a,y) = (K,U)$

$e_k(5,17) = (15,16)$

$e_k(8,3) = (2,5)$

$e_k(0,24) = (10,20)$

$y = x \cdot K \Rightarrow \begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix} \cdot K \rightarrow K = \begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix} \cdot \begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix}^{-1}$

$$\begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix}^{-1} = \frac{1}{\det} \cdot \begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix}^* = \begin{pmatrix} 9 & 1 \\ 2 & 15 \end{pmatrix}$$

$$K = \begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix} \cdot \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix} = \begin{pmatrix} 7 & 19 \\ 8 & 3 \end{pmatrix}$$

örnek: $K = \begin{pmatrix} 10 & 5 & 12 \\ 3 & 14 & 21 \\ 8 & 9 & 11 \end{pmatrix}$, $K^{-1} = ?$

$K^{-1} = (\det K)^{-1} \cdot K^*$

$\det K = -695 \bmod 26 = 7$

$\begin{vmatrix} 14 & 21 \\ 9 & 11 \end{vmatrix}$ K^*

Permutation Cipher

$P = C = (\mathbb{Z}_{26})^m$. $m \rightarrow$ pozitif int.

$K = \{1, 2, 3, \ldots, m\}$ ye bağlı olarak oluşan permütasyonların değerleri. (π)

$y = e_\pi(x_1, x_2, \ldots, x_m) = (x_{\pi(1)}, \ldots, x_{\pi(m)})$

$x = d_{\pi^{-1}}(y_1, y_2, \ldots, y_m) = (y_{\pi^{-1}(1)}, \ldots, y_{\pi^{-1}(m)})$

örnek: $m = 6$, P: "shesellsseashellsbytheseashare", C = ?

x	1	2	3	4	5	6
$\pi(x)$	3	5	1	6	4	2

y	1	2	3	4	5	6
$\pi^{-1}(y)$	3	6	1	5	2	4

P: "	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6	"
	s	h	e	s	e	l	l	s	s	e	a	s	h	e	l	l	s	b	y	t	h	e	s	e	a	s	h	a	r	e	
	3	5	1	6	4	2	3	5	1	6	4	2	.....																		
C: "	e	e	s	l	s	h	e	e	s	l	s	h	.....																		"

$K_\pi = k_{ij} = \begin{cases} 1 & \text{if } i = \pi(j) \\ 0 & \text{diğer durumlar} \end{cases} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$

Stream Cipher

$y = y_1 y_2 \ldots = e_k(x_1)\, e_k(x_2) \ldots$

$z = z_1 z_2 \ldots$

$y = y_1 y_2 \ldots = e_{z_1}(x_1)\, e_{z_2}(x_2) \ldots$

$z_i \in L$, $e_{z_i} \in E$; $P \rightarrow C$

$d_{z_i} \in D$; $C \rightarrow P$

(P, C, K, L, E, D)

L: keystream (anahtar akımı) alfabesi

g: keystream generator

Autokey Cipher

$P = C = K = L = \mathbb{Z}_{26}$

$$z_i = \begin{cases} z_1 = K \\ z_i = x_{i-1}, & i \geq 2 \end{cases} \quad (0 \leq z \leq 25)$$

$y = e_z(x) = (x+z) \bmod 26$

$x = d_z(y) = (y-z) \bmod 26$ $\quad x, y \in \mathbb{Z}_{26}$

örnek: $K = 8$, P: "rendezvous", C = ?

P: " r e n d e z v o u s "
17 4 13 3 4 25 21 14 20 18
z: 8 17 4 13 3 4 25 21 14 20
+
25 21 17 16 7 3 20 9 8 12

C: " Z V R Q H D U J I M "

One-Time Pad

$n \geq 1$, int (exor)

$P = C = K = (\mathbb{Z}_2)^n$

$y = e_k(x) = (x_1+K_1, x_2+K_2, \ldots, x_n+K_n) \bmod 2$

$x = d_k(y) = (y_1+K_1, y_2+K_2, \ldots, y_n+K_n) \bmod 2$

Substation-Permutation Networks

$\Pi_S : \{0,1\}^L$

$\Pi_P : \{1, 2, \ldots, L.m\} \to \{1, 2, \ldots, L.m\}$

L, m ve N_r → pozitif int.

$P = C = \{0,1\}^{L.m}$, $K \subseteq (\{0,1\}^{(L.m)})^{N_r+1}$

$K^1, K^2, \ldots, K^{N_r+1}$

$w^0 \leftarrow x$
for $r \leftarrow 1$ to $N_r - 1$
  $u^r \leftarrow w^{r-1} \oplus K^r$
  for $i \leftarrow 1$ to m
    do $v^r_{(i)} \leftarrow \Pi_S(u^r_{(i)})$
  $w^r \leftarrow (v^r_{\Pi_P(1)}, \ldots, v^r_{\Pi_P(L.m)})$
$u^{N_r} \leftarrow w^{N_r-1} \oplus K^{N_r}$
for $i \leftarrow 1$ to m
  do $v^{N_r}_{(i)} \leftarrow \Pi_S(v^{N_r}_{(i)})$
$y \leftarrow v^{N_r} \oplus K^{N_r+1}$
output (y)

Örnek: $\ell = m = N_r = 4$

$\ell = 16$

z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi_S(z)$	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

z	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\pi_P(z)$	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

$K =$ 0011 1010 1001 0100 1101 0110 0011 1111

K^1, K^2, K^3, K^4, K^5

$x =$ 0010 0110 1011 0111 → Şifrelenecek

$K^1 =$ 0011 1010 1001 0100

⊕

$u^1 =$ 0001 1100 0010 0011

$v^1 =$ 0100 0101 1101 0001

$w^1 =$ 0010 ....

Ödev 7: SPN permutation, substitution cipher'ın kodu.

Ödev 8: xor işleminin tersini bulan program

Ödev 9: SPN'i gerçekleyen program, key'lerini biz belirleriz

Data Encryption Standard - DES

23.10.2017

64 bitlik sifreleme algoritması.

$\begin{cases} x \rightarrow 64\ bit \\ +K \rightarrow 64\ bit \\ \searrow y \rightarrow 64\ bit \end{cases}$

1-) $x_0 = IP(x)$

$$IP = \begin{pmatrix} 58 & 50 & 42 & \cdots \\ 60 & \cdots & \cdots & \\ 62 & \cdots & \cdots & \\ \vdots & \cdots & \cdots & \end{pmatrix}_{8\times 8} \qquad IP(x) = \frac{x_{57}}{1}\ \frac{x_{49}}{2}\ \frac{x_{41}}{3}\ \cdots\ \frac{x_{32}}{9}\ \cdots = L_0 R_0$$

$\overline{32\ bit}\ \overline{32\ bit}$

2-) $1 \le i \le 16$, $L_i R_i$

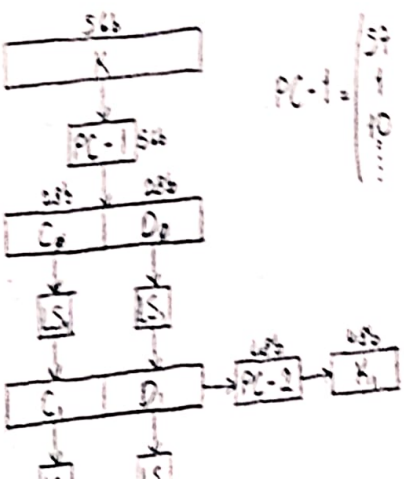
$L_i = R_{i-1}$
$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

$R_0 = 32\ bit$, $K_i = 48\ bit$, $f(R_{i-1}, K_i) = 32\ bit$

Ki, Dizgi anahtarlarının oluşturulması

$K \rightarrow 64\ bit$

$8, 16, 24, 32, 40, 48, 56 \Rightarrow$ 64 bitten, kontrol bitleridir.

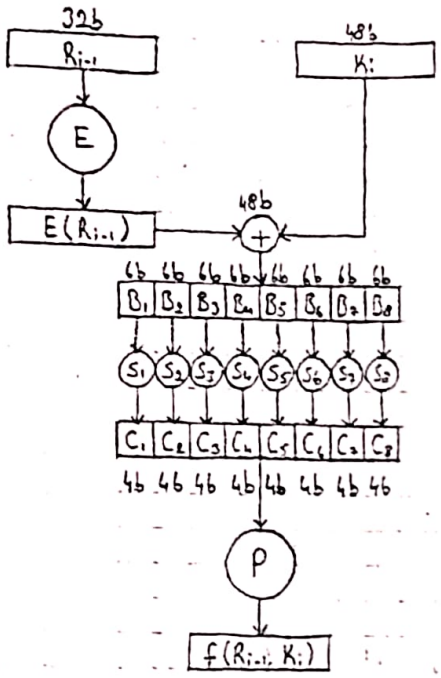


$$PC\text{-}1 = \begin{pmatrix} 57 & 49 & 33 & \cdots \\ 1 & \cdots & \cdots & \\ 10 & \cdots & \cdots & \\ \vdots & \cdots & \cdots & \end{pmatrix}_{8\times 7} \qquad PC\text{-}1(K) = C_0 D_0 = \frac{K_{57}}{1}\ \frac{K_{49}}{2}\ \cdots\cdots\cdots$$

C_0 D_0
28 bit 28 bit

$C_i = LS_i(C_{i-1})$
$D_i = LS_i(D_{i-1})$
$i = 1, 2, 3, 4, \ldots$

- $f(R_{i-1}, K_i)$



$$E = \begin{pmatrix} 32 & 1 & 2 & \cdots \\ 10 & 11 & \cdots & \\ 18 & \cdots & & \\ \vdots & & & \end{pmatrix}_{8\times 6} \qquad S_i = \begin{pmatrix} 14 & 4 & 13 & \cdots \\ 0 & 15 & \cdots & \\ 5 & \cdots & & \\ 7 & \cdots & & \end{pmatrix}_{4\times 16}$$

$C_j = S_j(B_j)$

$B_j = b_1 b_2 b_3 b_4 b_5 b_6$ örnek: $B_1 = 100001$

$b_1 b_6$ → satır no
$b_2 b_3 b_4 b_5$ → sütun no

$b_1 b_6 = 11 \rightarrow 3.$ satır
$b_2 b_3 b_4 b_5 = 0000 \rightarrow 0.$ sütun

$C_1 = S_1(B_1) = (7)_2 = 0111$

$$P = \begin{pmatrix} 16 & 7 & 20 & 5 \\ 3 & \cdots & & \\ 2 & \cdots & & \\ \vdots & & & \end{pmatrix}_{8\times 4}$$

3-) $y = IP^{-1}(R_{16} L_{16})$, $y = 64b$

Ödev 10: Triple DES nedir, araştır. Vize de sorumluyuz.

DES İşlem Kipleri

ECB, OFB, CFB, CBC

ECB - Electronic Code Book

$y_1 = e_k(x_1)$, $y_2 = e_k(x_2)$, ...

Output Feedback Mode - OFB

$y_i = x_i \oplus z_i$, $i \geq 1$

$z_i = e_k(z_{i-1})$, $i \geq 1$

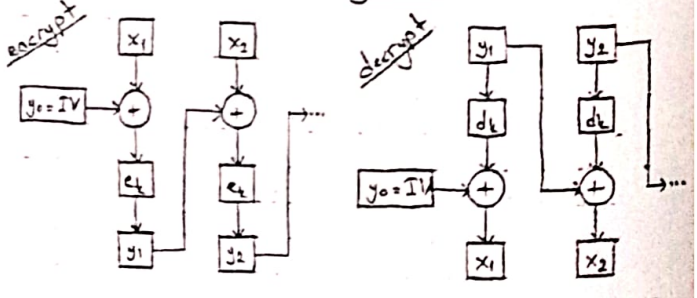
$z_0 = IV \rightarrow$ 64 bitlik fix değer.

Cipher Feedback Mode - CFB

$y_i = x_i \oplus z_i$, $i \geq 1$

$z_i = e_k(y_{i-1})$, $i \geq 1$, $y_0 = IV$

Cipher Block Chaining - CBC



Ödevler hakkında bilgi

Ödevlere numara, ad, soyad yaz.

Verilen ödevlerin kod, çıktı ve algoritma hakkında bilgi ver.

Vize hakkında bilgi

%70 kolay, %30 özel soru.

Obeb, modüler ters alma, üs alma ; klasik şifreleme algoritmaları ; affine, hill cipher gibi kripto analiz sayısal soru ; matrisin tersini alma ; des işlem kipllerinin mantığını bil.

Sınav Hazırlık

ECB: Verilen mesaj bloklara bölünür, bölünmüş mesaj ayrı ayrı parçalar olarak şifrelenir. Şifrelenen bloklar arasında bir ilişki yoktur. Her blok tek başına şifrelenir.

OFB: Bir bloğun şifreleme algoritmasından çıktısı ile bir sonraki bloğu beslemeye yarar. Algoritmaya giren değer başlangıç vektörü olmaktadır. Şifreleme sonucunda elde edilen değer bir sonraki bloğun başlangıç vektörü olarak kullanılmaktadır. Şifreli mesaj blokları ise, açık blokların, şifreleme algoritması çıktıları ile xor'lanması halidir.

CFB: ECB aksine her şifrelenen blok, bir sonraki şifre için bir girdi olmaktadır.

CBC: ECB aksine, şifrelenen mesajın bir önceki mesajla xor işlemine sokulması sonucunda çıkan mesaj şifrelenir.

Soru: $x^2 = 16 \bmod 105$ eşitliğini sağlayan x'lerin Ç.K'ni CRT ile bulun

$105 = 3.5.7$

$x = \pm 4 \bmod 3 = \mp 1 \bmod 3$ $\quad x = \pm 4 \bmod 5 = \mp 1 \bmod 5$ $\quad x = \pm 4 \bmod 7 = \mp 2 \bmod 7$

$x = 1 \bmod 3$ $\quad x = 1 \bmod 5$ $\quad x = 3 \bmod 7$

$x = 2 \bmod 3$ $\quad x = 4 \bmod 5$ $\quad x = 4 \bmod 7$

$x = 1 \bmod 3$ $\quad x = 1 \bmod 3$ $\quad x = 1 \bmod 3$ $\quad x = 1 \bmod 3$ $\quad x = 2 \bmod 3$ $\quad x = 2 \bmod 3$ $\quad x = 2 \bmod 3$ $\quad x = 2 \bmod 3$

Soru: Euler fonksiyonu nedir, $\phi(56) = ?$

$\phi(m)$, m'ye göre asal olan m'den küçük tüm doğal sayıların kümesine

$\phi(56) = 1, 3, 5, 9, 11, \ldots, 55$

$\phi(56) = 24$ tane

Soru: $(28^{-1} \pmod{75})$'i Extended Euclid Algoritmasına göre bulun.

gcd(75, 28, g, t, s)	g=1	t=3	$s = -2 - \lfloor 25/28 \rfloor \cdot -2 = -8$
gcd(28, 19, g, t, s)	g=1	t=-2	$s = 1 - \lfloor 28/19 \rfloor \cdot -2 = 3$
gcd(19, 9, g, t, s)	g=1	t=1	$s = 0 - \lfloor 19/9 \rfloor \cdot 1 = -2$
gcd(9, 1, g, t, s)	g=1	t=0	$s = t - \lfloor 9/1 \rfloor \cdot s = 1 - 0 \cdot 1$
gcd(1, 0, g, t, s)	g=1	t=1	s=0

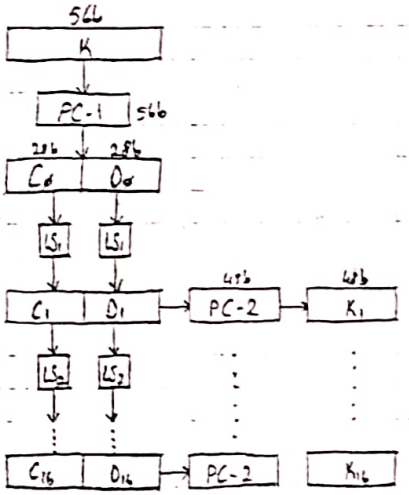
$$gcd(m, n) = g = t \cdot m + s \cdot n$$

$$gcd(75, 28) = 1 = 3 \cdot 75 - 8 \cdot 28$$

$$28^{-1} \bmod 75 = -8 = 67$$

Soru: DES şifreleme işleminde anahtar nasıl belirlenir? Şekil çizerek belirtiniz.

K = 64 bit, 8, 16, 24, 32, 40, 48, 56, 64. bitler kontrol bitidir. Kalan 56 bit algo'ya girilir.



$C_i = LS_i(C_{i-1})$
$D_i = LS_i(D_{i-1})$
if i=1, 2, 9, 16
  sola 1 adım ötele
else
  sola 2 adım ötele

mod n, shift cipher, involutory key?

$$e_k(x) = e_k^{-1}(x)$$

$$x + a = x - a \bmod n$$

$$2a = 0 \bmod n$$

$a = 0$ ve $a = \frac{n}{2}$

Soru: Bir plaintext Hill Cipher ile $\begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$ matrisi kullanılarak şifreleniyor. Ciphertext "OKYUQPKB" ise plaintext nedir? $x = y \cdot K^{-1}$

$K = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$ $K^{-1} = (\det K)^{-1} \cdot K^*$ $\det K = 4 - 3 = 1$ $1^{-1} \bmod 26 = 1$

$$K^* = \begin{pmatrix} + \begin{vmatrix} 2 & 3 \\ 1 & 2 \end{vmatrix} & - \begin{vmatrix} 2 & 3 \\ 1 & 2 \end{vmatrix} \\ - \begin{vmatrix} 2 & 3 \\ 1 & 2 \end{vmatrix} & + \begin{vmatrix} 2 & 3 \\ 1 & 2 \end{vmatrix} \end{pmatrix}^* = \begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix}^* = \begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix} \bmod 26 = \begin{pmatrix} 2 & 23 \\ 25 & 2 \end{pmatrix}$$

$$K^{-1} = 1 \cdot K^* = \begin{pmatrix} 2 & 23 \\ 25 & 2 \end{pmatrix}$$

$x = y \cdot K^{-1} \Rightarrow$

$(O, K) \cdot K^{-1} = (14, 10) \cdot \begin{pmatrix} 2 & 23 \\ 25 & 2 \end{pmatrix} = (18, 4) =$ "SE"

$(Y, U) \cdot K^{-1} = (24, 20) \cdot \begin{pmatrix} 2 & 23 \\ 25 & 2 \end{pmatrix} = (2, 20) =$ "CU"

$(Q, P) \cdot K^{-1} = (16, 15) \cdot \begin{pmatrix} 2 & 23 \\ 25 & 2 \end{pmatrix} = (17, 8) =$ "RI"

$(K, B) \cdot K^{-1} = (10, 1) \cdot \begin{pmatrix} 2 & 23 \\ 25 & 2 \end{pmatrix} = (19, 24) =$ "TY"

C = "SECURITY"

Soru:

a. mod 20'de yapılan bir Affine Cipher yönteminde a hangi değerleri alabilir?

$\gcd(a, 20) = 1 \rightarrow$ $a: \{1, 3, 7, 9, 11, 13, 17, 19\}$

b. b hangi değerleri alabilir?

$0 \leq b < 20$

c. Hill Cipher yönteminde anahtar olarak her matris kullanılabilir mi? Neden?

Her matris kullanılamaz. Matrisler kare matris ve tersi alınabilir yani $\det \neq 0$ olması gerekir. Çünkü $K^{-1} = \frac{1}{\det K} \cdot K^*$ olduğundan det 0 olamaz.